CHAPTER 2

Provisioning SIP Trunks

Revised: October 21, 2008, OL-5351-10

This chapter provides instructions for provisioning 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.

Provisioning Example

The following example models a local Cisco BTS 10200 subscriber making a call out from a SIP trunk to a SIP proxy serving a NPA-NXX domain.

A trunk must be created and associated with the IP address of the proxy. The dial digits associated with the trunk must be provisioned within the originators' dial plan.

Note Before provisioning, identify the following:
* The first 6 dial digits of the SIP proxy NPA-NXX domain: in this example, 469-255.
* Provisioned dial plan ID of the originator in Cisco BTS 10200: in this example, 'dp1'.
* IP address of the SIP proxy: in this example, 1.2.3.4.

Provisioning Example - CLI

```
add softsw_tg_profile id=<profile_id>; protocol_type=SIP;
add pop id=<pop_id>; state=tx; country=usa; timezone=CST;
add trunk_grp id=<trunk_id>; tg_type=SOFTSW; softsw_tsap_addr=1.2.3.4; dial_plan_id=dp1;
   tg_profile_id=<profile_id>; call_agent_id=<ca_id>; pop_id=<pop_id>;
add route id=<route_id>; tgn1-id=<trunk_id>;
add route-guide id=<route_guide_id>; policy_type=ROUTE; policy_id=<route_id>;
add destination dest-id=<dest_proxy_id>; call-type=LOCAL; route-type= ROUTE;
   route_guide_id=<route_guide_id>;
add dial-plan id=dp1; digit-string=469-255; dest-id=<dest_proxy_id>;
```

Provisioning SIP Trunk Features

The following sections describe how to provision SIP trunk features.

- General Requirements for Provisioning SIP Trunk Groups, page 2-2
- Validation of Source IP Address for Incoming SIP Messages (Release 4.5.1, Maintenance Release 1), page 2-3
- Call Redirection, page 2-3
- Locating SIP Servers Using DNS Queries, page 2-4
- Type of Service, page 2-5
- Reliable Provisional Responses, page 2-6
- Diversion Indication, page 2-7
- Carrier Identification Code over SIP, page 2-7
- Number Portability Information over SIP, page 2-8
- SIP Trunk Sub-Groups, page 2-8
- Session Timers, page 2-9
- SIP Timer Values, page 2-9
- SIP-T, ISUP Version, ISUP-Transparency, and GTD, page 2-10
- DTMF SIP Signaling, page 2-11
- Asserted Identity and User-Level Privacy, page 2-12
- ANI-Based Routing, page 2-13
- Calling Name Delivery on Terminating SIP Trunks, page 2-13
- Trunk Group Audit for the SIP Adapter, page 2-14
- T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface, page 2-14

General Requirements for Provisioning SIP Trunk Groups

The TSAP_address in the outbound SIP trunk group can be provisioned with a static IP address, but the inbound SIP trunk group must be provisioned with a domain name. This is because it needs to match the domain name in the incoming INVITE message Via header. If you do not provision the TSAP_address this way, the call is rejected with 403 Forbidden message.

To avoid a DNS lookup, to use the static IP address, we suggest using at least three SIP trunk groups: two for outbound with the IP addresses of two remote softswitches, and one for inbound with the domain name of one remote softswitch.

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 is controlled through a switch-wide parameter (applies to all SIP trunk groups on the switch). You can enable this capability using the following command.

```
add ca-config type=SIA-TG-VALIDATE-SOURCE-IP; datatype=BOOLEAN; value=Y;
```

Note By default, SIA-TG-VALIDATE-SOURCE-IP is set to N, and IP address validation is disabled.

Call Redirection

The following commands control call redirection on all trunks associated to the SIP trunk profile <profile_id>.

Step 1 Disable call redirection.

```
change softsw_tg_profile id=<profile_id>; REDIRECT_SUPPORTED=NONE;
```

Step 2 Enable call redirection.

The trunk accepts redirection contacts only with host names of the Cisco BTS 10200 SIP contact, or the TSAP address of any provisioned SIP trunks.

The default is:

```
change softsw_tg_profile id=<profile_id>; REDIRECT_SUPPORTED=VALID_DOMAINS_ONLY;
```

Step 3 Enable call redirection.

The trunk accepts redirection contacts with any host name. A 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.

```
change softsw_tg_profile id=<profile_id>; REDIRECT_SUPPORTED=ALL_DOMAINS;
```

The following parameters are provisioned through the Call Agent Configuration (ca-config) table, and affect all SIP trunks on the switch. Additional details for the ca-config table are provided in the *Cisco BTS 10200 Softswitch Command Line Interface Guide*, Chapter 1, "Call Agent Provisioning," and Appendix A, "Configurable Parameters and Values."

Step 1 If necessary, change the upper limit on the number of 300 class redirection responses the Cisco BTS 10200 accepts while performing redirection on any given call attempt; the default is 1.

```
add ca-config type=MAX-3XX-COUNT; datatype=INTEGER; value=2;
```

Step 2 If necessary, change the limit on the maximum number of call redirection attempts the Cisco BTS 10200 makes on any given call attempt, after which it releases the call; the default is 5.

```
add ca-config type=MAX-REATTEMPT-COUNT; datatype=INTEGER; value=4;
```

Step 3 If necessary, set the 3XX reroute parameter for call redirection. If you want to force the system to perform fresh routing (reroute) using the dial plan of the terminating trunk, use the following command to set the 3XX reroute parameter to Y.

```
add ca-config type=SIP-3XX-REROUTE-ON-LOCAL-DOMAIN; datatype=BOOLEAN; value=Y;
```

Note By default, SIP-3XX-REROUT-ON-LOCAL-DOMAIN is set to N, and the system performs route advance when the redirection number is the same as the number in the original INVITE.

Locating SIP Servers Using DNS Queries

The system can locate SIP servers using NAPTR and SRV DNS queries, or using A-Record DNS queries.

Tip For a description of how the system uses these queries to locate SIP servers, see the DNS query description in the *Cisco BTS 10200 Softswitch SIP Protocol User Guide*.

Provisioning the System to Use NAPTR and SRV DNS Queries

Follow these steps to provision the system to use NAPTR and SRV DNS queries.

Step 1 Enable NAPTR and SRV DNS queries.

```
change softsw_tg_profile id=<profile_id>; DNS_SRV_SUPP=RFC2782_LABELS;
```

Step 2 Provision the TSAP address in the trunk group for the SIP server.

```
change trunk_grp id=<trunk group id>; softsw_tsap_addr=<see list of values below>;
```

Either of the following can be provisioned for softsw_tsap_addr:

- NAPTR name
- SRV name

Note The use of either NAPTR or SRV names requires correctly configured DNS servers.

Provisioning Recommendations for NAPTR and SRV in the DNS Servers

- When using SRV, if a host name is provisioned in the TSAP address, include a port. This allows the application to identify the address as a host name and skip NAPTR and SRV queries.
- If an SRV name is required, provision NAPTR entries to provide SRV replacement strings instead of waiting for a failure on the NAPTR query to make an SRV query.

Provisioning the System to Use A-Record DNS Queries

Follow these steps to provision the system to use A-record DNS queries.

Step 1 Disable NAPTR and SRV DNS queries.

```
change softsw_tg_profile id=<profile_id>; dns_srv_supp=NONE;
```

Note NONE is the default value for dns_srv_supp.

Step 2 Provision the transport type.

```
change softsw_tg_profile id=<profile_id>; non_srv_transport=<see list of values below>;
```

Any one of the following can be provisioned for non_srv_transport:

- 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.

Step 3 Provision the TSAP address in the trunk group for the SIP server.

```
change trunk_grp id=<trunk group id>; softsw_tsap_addr=<see list of values below>;
```

Any one of the following can be provisioned for softsw_tsap_addr.

- Host name
- Host name and port
- IP address
- IP address and port

Note The use of host names requires correctly configured DNS servers.

Type of Service

This section describes the provisionable options for TOS settings on SIP trunks.

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.

Provisioning SIP Trunks on the Cisco BTS 10200

The following commands set the Type of Service (ToS) default settings for all SIP trunks on the Cisco BTS 10200.

```
add ca_config TYPE=SIA-TRUNK-GRP-LEVEL-SIG-TOS; DATATYPE=BOOLEAN; VALUE=N;

add ca_config TYPE=SIA-SIG-TOS-PRECEDENCE; DATATYPE=INTEGER; VALUE=3;

add ca_config TYPE=SIA-SIG-TOS-RELIABILITY; DATATYPE=BOOLEAN; VALUE=N;

add ca_config TYPE=SIA-SIG-TOS-THROUGHPUT; DATATYPE=BOOLEAN; VALUE=N;

add ca_config TYPE=SIA-SIG-TOS-LOWDELAY; DATATYPE=BOOLEAN; VALUE=Y;
```

Provisioning Type of Service Default Settings for SIP Trunks Associated to the SIP Trunk Profile

The following commands set the ToS default settings for SIP trunks associated to the SIP trunk profile <profile_id>:

```
add ca_config TYPE=SIA-TRUNK-GRP-LEVEL-SIG-TOS; DATATYPE=BOOLEAN; VALUE=Y;

change softsw_tg_profile id=<profile_id>; SIP_SIG_LOWDELAY=Y;

change softsw_tg_profile id=<profile_id>; SIP_SIG_THROUGHPUT=N;

change softsw_tg_profile id=<profile_id>; SIP_SIG_RELIABILITY=N;

change softsw_tg_profile id=<profile_id>; SIP_SIG_PRECEDENCE=FLASH;
```

Note Note that the 'SIA-TRUNK-GRP-LEVEL-SIG-TOS' flag in the call agent configuration is used to select between using ToS settings for all SIP trunks, or ToS settings for specific SIP trunks.

Reliable Provisional Responses

The following commands control the reliable provisional response feature for regular SIP calls on all trunks associated to the SIP trunk profile <profile_id>.

Step 1 The default for making reliable provisional responses not required for regular SIP calls sent or received over a SIP trunk is:

```
change softsw_tg_profile id=<profile_id>; PRACK_FLAG=N;
```

Step 2 To make reliable provisional responses required for regular SIP calls sent or received over a SIP trunk, use the following command:

```
change softsw_tg_profile id=<profile_id>; PRACK_FLAG=Y;
```

Note When reliable provisional responses are not required, the Cisco BTS 10200 will not make them required on remote SIP entities. However, the reliable provisional responses may still occur if a remote SIP entity requires it of Cisco BTS 10200.

This flag must applies only to SIP calls on regular SIP trunks, and regular SIP calls received on SIP-T provisioned trunks. Consult the *Cisco BTS 10200 SIP User Guide* for details on the behavior of this feature.

Diversion Indication

The following commands control the diversion feature for outgoing calls on all trunks associated to the SIP trunk profile <profile_id>.

Step 1 Disable diversion headers for calls sent out the trunk.

The default is:

```
change softsw_tg_profile id=<profile_id>; DIVERSION_HEADER_SUPP=N;
```

Step 2 Enable diversion headers for calls sent out the trunk.

```
change softsw_tg_profile id=<profile_id>; DIVERSION_HEADER_SUPP=Y;
```

Note This flag does not apply to incoming calls. If the diversion headers exists on the incoming call, the system interprets the information from the diversion header.

For a description of the diversion indication features, see the "Diversion Indication" section in the *SIP Protocol User Guide*.

Carrier Identification Code over SIP

A carrier identification code (CIC) received in a SIP call on an incoming SIP trunk is automatically interpreted. No provisioning control is available. For outgoing SIP calls originated by a local Cisco BTS 10200 subscriber, the CIC may be provided by the subscriber record if provisioned. See the CIC selection rules in the trunk-grp table and the send-cic-param token in the softsw-tg-profile table in Chapter 5, "Database Tables" of the *Cisco BTS 10200 Softswitch SIP Protocol User Guide*.

For additional description of the CIC options, see the Carrier Identification Code Over SIP section in the *Cisco BTS 10200 Softswitch SIP Protocol User Guide*.

Number Portability Information over SIP

The following commands control number portability information for calls sent out on the SIP trunk group <tg_id>.

Step 1 The following command allow for sending number portability information if the information is available.

The default is:

```
change trunk_grp id=<tg_id>; SIGNAL_PORTED_NUMBER=N;
```

Step 2 The following command disables the addition of number portability information to SIP calls sent out a SIP trunk group:

```
change trunk_grp id=<tg_id>; SIGNAL_PORTED_NUMBER=Y;
```

Note Note that number portability information received in a SIP call on an incoming SIP trunk is automatically interpreted. No provisioning control is available.

SIP Trunk Sub-Groups

These steps illustrate how to provide multiple trunks toward a remote SIP entity for additional network-specific or application-specific properties for calls to and from the Cisco BTS 10200. One example: the identification of which rate center the call originated.

The following information is required at the time of provisioning:

- Associate a unique trunk group identifier for each rate center. For example: ‘rc1,’ ‘rc2,’ and ‘rc3’ for three rate centers.
- Identify the fully qualified domain name (FQDN) and port of the remote SIP server used for SIP message exchange. For example: ‘sipserver:5060.’
- Create a dial plan for calls received on the SIP trunks, to route the calls based on the called party number. For example: the identifier for this dial plan is ‘dp.’

Step 1 Add a SIP trunk profile for the SIP trunks. Set the trunk sub-group type to indicate the trunk group identifier use:

```
add softsw_tg_profile ID=<profile_id>; PROTOCOL_TYPE=SIP; TRUNK_SUB_GRP_TYPE=TGID;
```

Step 2 Add a SIP trunk for each trunk group identifier. Each trunk points to the address of the voicemail sever:

```
add trunk_grp ID=<trk_grp_id1>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=sipserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=rc1;
```

and:

```
add trunk_grp ID=<trk_grp_id2>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=sipserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=rc2;
```

and:

```
add trunk_grp ID=<trk_grp_id3>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=sipserver:5060; DIAL_PLAN_ID=dp; TRUNK_SUB_GRP=rc3;
```

Routing and dial plan tables are provisioned (not shown) so that calls originating from a specific rate center are sent out the SIP trunk with the trunk group identifier representing that rate center.

Session Timers

Use the commands in this section to provision session timers on the Cisco BTS 10200 Softswitch.

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. In Release 4.5.x and later, the session timer values are provisioned through the MIN-SE and SESSION-EXPIRES-DELTA-SECS tokens in the sip-timer-profile table. The id of the sip-timer-profile table record is then specified as the Value for the ca-config record of Type=sip_timer_profile_id. The id of the sip-timer-profile table can also be associated with a softsw-tg-profile record for SIP trunks. If you provision the timer values for a specific trunk, that overrides the ca-config default.

Step 1 Adjust the session timer values in the sip-timer-profile table if necessary.

Note The session duration field value is in seconds with a range of 100 to 7200.
The minimum session duration field value is in seconds with a range of 100 to 1800.
We recommend a value of at least 1800 for each of these fields.

```
add sip_timer_profile id=<timer_profile_id>; session_expires_delta_secs=7200; min-se=1800;
```

Step 2 Enable session timers on the applicable softswitch trunk group profile, and assign the sip-timer-profile-id:

```
change softsw_tg_profile id=<profile_id>; session_timer_allowed=Y;
sip_timer_profile_id=<timer_profile_id>;
```

Step 3 For a switch-wide default for SIP trunks (if the trunk is not specifically provisioned), add a default sip-timer-profile-id to the ca-config table as follows:

```
add ca_config type=sip_timer_profile_id; datatype=string; value=<sip_timer_profile_id>;
```

SIP Timer Values

Release 4.5.x enhances support for customizing SIP timers through the new sip-timer-profile table. A record in this table can be configured to apply to one or more SIP trunks or to apply switch-wide. A sip-timer-profile record can be associated with a specific softsw-tg-profile record and/or to a ca-config record. On a fresh software installation, and after a upgrade, the system operates with default SIP protocol timer values, as specified by the SIP specification. These default values are adequate for many installations. If customization is required, then a sip-timer-profile table can be provisioned and associated with all calls, or with calls on specific trunks.

Note The session timer parameters, MIN-SE and SESSION-EXPIRES-DELTA-SECS, have been consolidated into this new table and, unlike prior releases, are no longer configurable directly on the ca-config table.

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 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. In Release 4.5.x and later, the timer values are provisioned in the sip-timer-profile table. The id of the sip-timer-profile table record is then specified as the Value for the ca-config record of Type=sip_timer_profile_id. The id of the sip-timer-profile table can also be associated with a softsw-tg-profile record for SIP trunks. If you provision the timer values for a specific trunk, that overrides the ca-config default.

Step 1 Adjust the session timer values in the sip-timer-profile table if necessary (example shown):

```
add sip_timer_profile id=<timer_profile_id>; timer-t1-milli=500;
```

Step 2 Enable session timers on the applicable softswitch trunk group profile, and assign the sip-timer-profile-id:

```
change softsw_tg_profile id=<profile_id>; session_timer_allowed=Y;
sip_timer_profile_id=<timer_profile_id>;
```

Step 3 For a switch-wide default for SIP trunks (if the trunk is not specifically provisioned), add a default sip-timer-profile-id to the ca-config table as follows:

```
add ca_config type=sip_timer_profile_id; datatype=string; value=<sip_timer_profile_id>;
```

For a complete list of these timers, see the "SIP Timer Values" section on page 1-22.

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

Note The values used in this section are examples. For a complete list of options, see the applicable table in the *Cisco BTS 10200 Softswitch Command Line Reference Guide.*

Step 1 Provision a SIP-T trunk by setting the protocol type to SIP-T in the SIP trunk profile <profile_id> as follows.

Note Setting PROTOCOL_TYPE=SIP_T enables both SIP-T and SIP-GTD protocols.

a. If you want to review the valid SIP-T ISUP versions, enter the following command:

```
show sipt-isup-ver-base
```

b. For a SIP-T version of ANSI GR-317, provision as follows:

```
add softsw_tg_profile ID=<profile_id>; PROTOCOL_TYPE=SIP_T; PRACK_FLAG=Y;
SIPT_ISUP_VER=ANSI_GR317;
```

c. For a SIP-T version of GTD, provision as follows:

```
add softsw_tg_profile ID=<profile_id>; PROTOCOL_TYPE=SIP_T; PRACK_FLAG=Y;
SIPT_ISUP_VER=GTD; gtd_mode=<COMPACT or VERBOSE>; gtd_parms=ALL;
```

Note The version field (SIPT_ISUP_VER) is a user-provisioned alphanumeric in the SIP trunk profile required for SIP-T trunk types. The label represents the version of the ISUP as it is understood by the remote SIP-T entity for interworking. It is one of the following values: GTD, ANSI_GR317, or Q761_HONGKONG. If the remote SIP entity is looking for these ISUP versions but under a different name, the SIPT-ISUP-VER-ALIAS table can be used to provide a custom version name in the SIP message.
If it is desired to omit the base parameter from the SIP message (as defined in RFC 3204) for the ISUP version provisioned, the USE_SIPT_ISUP_BASE flag can be set to FALSE. It is TRUE by default.
The flag for controlling reliable provisionable responses (PRACK_FLAG) must be enabled.

Step 2 Add a SIP trunk group associating it to the SIP trunk profile above as follows. The following example uses the dial plan identifier ‘dp,’ and the fully qualified domain name of the remote SIP-T entity ‘siptentity:5060.’

```
add trunk_grp ID=<trk_grp_id1>; TG_TYPE=SOFTSW; TG_PROFILE_ID=<profile_id>;
SOFTSW_TSAP_ADDR=siptentity:5060; DIAL_PLAN_ID=dp;
```

Step 3 If you are using GTD, perform these additional substeps.

a. verify that the gtd-supp token in the call-agent-profile is set to Y, or set it to Y if not already done:

```
show call-agent-profile id=CA-146;
change call-agent-profile id=CA146; gtd-supp=Y;
```

b. If you are using GTD, enter the GTD parameter values, for example:

```
add gtd-parm-values id=ACL; description=Automatic Congestion Level;
```

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

The following command controls the DTMF SIP signaling feature on all SIP trunks associated to the SIP trunk profile <profile_id>.

Step 1 Disable the DTMF SIP signaling feature.

The default is:

```
change softsw_tg_profile id=<profile_id>; DTMF_RELAY_METHOD=NONE;
```

Step 2 Enable the DTMF SIP signaling feature.

Use the SIP INFO method to send unsolicited notification of telephone events (DTMF) toward the remote SIP entity provisioned in the trunk group:

```
change softsw_tg_profile id=<profile_id>; DTMF_RELAY_METHOD=INFO;
```

Step 3 Enable the DTMF SIP signaling feature.

Use the SIP NOTIFY method to send solicited notification of telephone events (DTMF) toward the remote SIP entity provisioned in the trunk group. In this case, the remote SIP entity must subscribe to Cisco BTS 10200 for DTMF events:

```
change softsw_tg_profile id=<profile_id>; DTMF_RELAY_METHOD=NOTIFY;
```

Asserted Identity and User-Level Privacy

The following command controls the p-asserted-id (PAI) header used to send and receive calling party information.

Step 1 To set the system to derive calling party information exclusively from the PAI header on inbound calls, and always send for outbound calls, enter the command as follows:

```
change softsw_tg_profile id=<profile_id>; USE_PAI_HDR_FOR_ANI=Y;
```

Step 2 To set the system to send or receive calling party information in the From: header, enter the command as follows. (This is the default setting.)

```
change softsw_tg_profile id=<profile_id>; USE_PAI_HDR_FOR_ANI=N;
```

The following command controls user-level privacy in the outbound SIP INVITE message.

Step 1 To instruct the system to apply user-level privacy, enter the command as follows:

```
change softsw_tg_profile id=<profile_id>; APPLY-USER-PRIVACY=Y;
```

Note Setting this parameter to Y has the following effect—If the originator requested privacy, aspects of the calling party information (such as the calling name and number in the From: header) in the initial outbound SIP INVITE are hidden. Privacy is requested when either the calling party name or number have presentation restrictions.

Step 2 To instruct the system to not apply user-level privacy, enter the command as follows. (This is the default setting.)

```
change softsw_tg_profile id=<profile_id>; APPLY-USER-PRIVACY=N;
```

Note A description of asserted identity and user-level privacy is provided in the *Cisco BTS 10200 Softswitch SIP Protocol User Guide*.

ANI-Based Routing

The following rules apply when provisioning ANI-based routing for calls incoming on a SIP trunk:

- The softswitch trunk group on which the calls arrive must be have the "ANI_BASED_ROUTING" flag set to "Y."
- Office codes (NPA-NXX) must be provisioned for the calling party numbers.
- DN2Subscriber table must have the range of calling party numbers provisioned in it.
- A subscriber must be provisioned for a given range of DNs provisioned in DN2Subscriber. This subscriber's dial-plan and POP is then used to make call-type and routing decisions.

Example 2-1 Example of ANI-Based Routing CLI

```
add softsw-tg-profile ID=SS_PROFILE; PROTOCOL_TYPE=SIP;

add trunk-grp ID=157; CALL_AGENT_ID=CA146; TG_TYPE=SOFTSW;
SOFTSW_TSAP_ADDR=domainname.com; TG_PROFILE_ID=SS_PROFILE; POP_ID=1;
DIAL_PLAN_ID=BASIC_DPP; ANI_BASED_ROUTING=Y;

add subscriber-profile ID=sub_profile; DIAL_PLAN_ID=BASIC_DPP; POP_ID=1;

add subscriber ID=sub5; CATEGORY=INDIVIDUAL; NAME=sub5; TGN_ID=157;
SUB_PROFILE_ID=sub_profile; TERM_TYPE=TG;

add office-code DIGIT_STRING=214-555; OFFICE_CODE_INDEX=1;

add dn2subscriber FROM-DN=214-555-1231; TO-DN=214-555-1233; SUB_ID=sub5;
```

Calling Name Delivery on Terminating SIP Trunks

This section describes how to provision the Calling Name Delivery (CNAM) feature on a terminating SIP trunk on the Cisco BTS 10200. When enabled on a SIP trunk, a local subscriber originating a call out this SIP trunk will have the originator name in the SIP message.

In the following provisioning example, if subscriber 'sub1' calls 469-555-2222, it is routed out a SIP trunk. The CNAM feature is invoked and adds 'john doe' to the display name of outgoing SIP call. To associate CNAM to the trunk, CNAM is associated to a virtual subscriber, and the virtual subscriber is associated to the SIP trunk.

```
add softsw-tg-profile ID=SS_PROFILE; PROTOCOL_TYPE=SIP;

add trunk-grp ID=157; CALL_AGENT_ID=CA146; TG_TYPE=SOFTSW; SOFTSW_TSAP_ADDR=TsapAddr.com;
TG_PROFILE_ID=SS_PROFILE; POP_ID=1; DIAL_PLAN_ID=BASIC_DPP; ANI_BASED_ROUTING=Y;

add subscriber-profile ID=sub_profile; DIAL_PLAN_ID=BASIC_DPP; POP_ID=1;

add subscriber ID=subcnam; CATEGORY=INDIVIDUAL; NAME=subcnam; TGN_ID=157;
SUB_PROFILE_ID=sub_profile; TERM_TYPE=TG; DN1=469-555-2222;
```

```
add feature FNAME=CNAM; TDP1=FACILITY_SELECTED_AND_AVAILABLE;
TID1=TERMINATION_RESOURCE_AVAILABLE; TTYPE1=R; FEATURE_SERVER_ID=FSPTC235;
DESCRIPTION=Calling Name; GRP_FEATURE=N

add service ID=3; FNAME1=CNAM;

add subscriber-service-profile SUB_ID=subcnam; SERVICE_ID=3;

change subscriber id=sub1; NAME=john doe;
```

Trunk Group Audit for the SIP Adapter

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

When provisioning the Trunk Group audit mechanism, Cisco recommends provisioning only the STATUS-MONITORING flag in the Trunk Group table record.

The following fields should be left at the default settings:

In the SOFTSW_TG_PROFILE table:

- AUDIT-THRESHOLD

In the CA_CONFIG table:

- TRUNK-AUDIT-INTERVAL

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

The Cisco BTS 10200 Softswitch SIP interface always allows switching to T.38 fax when an incoming fax is detected from the SIP network. For additional guidance on interworking of SIP with other protocols for the T.38 fax features, see the T.38 fax relay information in the *Cisco BTS 10200 Softswitch SIP Protocol User Guide*.