CHAPTER 6

CALEA Provisioning

Revised: July 28, 2009, OL-4366-13

The Cisco BTS 10200 Softswitch provides interfaces for transmission of data used in conjunction with the Communications Assistance for Law Enforcement Act (CALEA). This chapter explains how to provision these interfaces on the Cisco BTS 10200 Softswitch and contains the following sections:

The Cisco BTS 10200 Softswitch provides support for CALEA using two different industry-developed architectures: PacketCable, and the Cisco Service Independent Intercept (SII).

Note For a general description of the Cisco BTS 10200 Softswitch implementation for CALEA support, refer to the *Cisco BTS 10200 Softswitch System Description*.

Create a Workgroup to Manage Access to ESS Commands

Any user with a high enough command privilege level can execute electronic surveillance server (ESS) commands. However, access can be more easily controlled using a workgroup.

To set up a workgroup, execute the following commands.

Step 1 Start a session with SSH, and log in to the EMS.

Step 2 Create a workgroup for the ESS command.

```
change command-table noun=ess; verb=add; work-groups=<Workgroup Name>;
```

Step 3 Add this workgroup to the user using the following command. This permits the user to access the ESS commands.

```
change user name=<someUser>; work-groups=<Workgroup Name>;
```

Service Independent Interception Provisioning

Perform the following steps to set up CALEA on the Cisco BTS 10200 Softswitch in an SII network. Example commands are provided but may not replicate your specific network conditions.

Step 1 Enable SII using the Call Agent Profile table. User class privileges are required to perform this command.

```
add call-agent-profile id=<CAid>;es-intercept-type=service-independent-intercept;
cms-id=1234; feid=4321;
```

Note Beginning with Release 4.4.1, the es-intercept-type token is no longer valid in the Call-agent-profile table.

Note Prior to Release 4.4.1, the default value for es-intercept-type is *packet-cable-intercept*, so if your network is a PacketCable network, you do not have to set the es-intercept-type.

Note CMS-ID=xxxx, FEID=xxxx are mandatory settings for CALEA.

Step 2 Provision the Electronic Surveillance Server table. This identifies the Delivery Function (DF) server to the Cisco BTS 10200 Softswitch.

```
add ess cdc-df-address=<IPaddress>; cdc-df-port=<port#>;
```

The CALEA feature is now available for use.

Release 4.1 and 4.2 PacketCable Electronic Surveillance Provisioning

Perform the following steps to set up CALEA on the Cisco BTS 10200 Softswitch in a PacketCable network. Example commands are provided but may not replicate your specific network conditions.

Note Only the CALEA-specific tokens and values for the Call Agent Profile, Media Gateway Profile, Aggregation, and Media Gateway tables are presented here.

Note The token values shown in this section are examples.

Step 1 Verify that your system is set for PacketCable intercept in the Call Agent Profile (*call-agent-profile)* table:

a. Display the current value of **es-intercept-type** in the *Call Agent Profile* table:

```
show call-agent-profile id=<Call Agent ID>;
```

Note Beginning with Release 4.4.1, the es-intercept-type token is no longer valid in the Call-agent-profile table and Steps a. and b are not necessary.

b. Verify that the display from the show command in Step a. indicates es-intercept-type=packet-cable-intercept, which is the default value. If it does not indicate packet-cable-intercept, change the value using the following command:

```
change call-agent-profile id=<Call Agent ID>;
es-intercept-type=packet-cable-intercept;
```

c. Verify that the display from the **show** command in Step a. indicates values for cms-id and feid. If it does not indicate values for these tokens, then add this information using the following command:

```
change call-agent-profile id=<Call Agent ID>; cms-id=<CMS ID>; feid=<FEID>;
```

Caution Both **cms-id** and **feid** are mandatory settings for the CALEA feature.

Step 2 Provision the ESS table using the following example. This identifies the DF server to the Cisco BTS 10200 Softswitch.

```
add ess cdc-df-address=<DNS or IPaddress>; cdc-df-port=<port#>; encryption-key=[1 to 16
ASCII characters]; acc-req-retransmit=4; acc-rsp-timeout=3; ipsec-sa-esp-cs=[cipher suite
for ESP]; ipsec-sa-lifetime=[IPsec SA expiration time]; ipsec-sa-grace-period=[expiration
grace period]; ipsec-ulp-name=[IP | UDP | TCP]; ike-group=[1|2]; ike-sa-lifetime=[IKE SA
expiration time]; ike-cs=[cipher suite for IKE]; ike-key=[IKE pre-shared key];
description=[user-defined description]; protocol-version=I03;
```

Step 3 If an aggregation router (CMTS) supports CALEA, and CALEA is enabled on the aggregation router, provision the *Aggregation* table and *Media Gateway* table as follows:

a. Provision the Aggregation table.

```
change aggr id=<er1>; es-supp=y; es-event-supp=y;
```

b. To display the current settings in the MGW table for each MTA, enter the following command:

```
show mgw id=<mgw id for the MTA>;
```

c. Verify that the display from the **show** command in Step b. indicates that the aggregation router (CMTS) is properly identified by the *aggr-id* token in the Media Gateway table. If there is no valid value displayed for ***aggr-id***, you must enter it using the following command:

```
change mgw id=<mgw id>; aggr-id=<Aggregation router (CMTS) ID>
```

d. Repeat Steps b. and c. as necessary to verify/enter the *aggr-id* on all MTAs (MGWs) connected to the CMTS (aggregation router).

Note CALEA must be enabled on every TGW and aggregation router used for CALEA. Consult your TGW and aggregation router vendor documentation for instructions.

Release 4.4 Electronic Surveillance Provisioning

The Cisco BTS 10200 Softswitch provides interfaces for transmission of data used in conjunction with the Communications Assistance for Law Enforcement Act (CALEA). This section explains how to provision these interfaces for Release 4.4, and later, of the Cisco BTS 10200 Softswitch.

The Cisco BTS 10200 Softswitch provides support for CALEA using two different industry-developed architectures: PacketCable, and the Cisco Service Independent Intercept (SII). When using packet-cable architecture for surveillance, if the Cisco BTS10200 does not find any packet-cable compliant call-content Intercept Access Point (IAP), the BTS 10200 automatically falls back to SII architecture. Alternatively, a service provider may choose to configure the BTS10200 to use SII architecture for all the tapped calls. The service provider should make sure that all the network elements are SII compliant to use SII architecture.

Note For a general description of the Cisco BTS 10200 Softswitch implementation for CALEA support, refer to the *Cisco BTS 10200 Softswitch System Description*.

Perform the following steps to set up CALEA on Release 4.4 of the Cisco BTS 10200 Softswitch in a PacketCable network. Example commands are provided but may not replicate your specific network conditions. Only the CALEA-specific tokens and values for the SIP Trunk-Group profile, Aggregation, and Media Gateway tables are presented here.

Step 1 Log on as Calea user to manage the Calea workgroup. The Cisco BTS10200 Softswitch has a default Calea workgroup that can only be accessed by a Calea user. This Calea workgroup manages two Calea related tables, the ESS table and the Wiretap table. The ESS table should be provisioned by authorized personnel while the Wiretap table is automatically provisioned by the DF server.

a. Start a session with SSH to the EMS as a Calea user:

```
ssh -l Calea@priemsXXX
```

b. Log into the Calea workgroup using the default password, calea01.

Note Authorized personnel must change the default password for CALEA using the following command.

c. Use the following command to reset the default password to a new password:

```
reset password name=calea; new_password=<new password>; warn=1; days_valid=1;
```

Step 2 Add a record to the Electronic Surveillance Server table using a command similar to the following example. This identifies the Delivery Function (DF) server to the Cisco BTS 10200 Softswitch.

```
add ess cdc-df-address=<DNS or IPaddress>; cdc-df-port=<port#>; encryption-key=[1 to 16
ASCII characters]; acc-req-retransmit=4; acc-rsp-timer=3; use-packetcable-iap=Y;
ipsec-sa-esp-cs=[cipher suite for ESP]; ipsec-sa-lifetime=[IPsec SA expiration time];
ipsec-sa-grace-period=[expiration grace period]; ipsec-ulp-name=[IP | UDP | TCP];
ike-group=[1|2]; ike-sa-lifetime=[IKE SA expiration time]; ike-cs=[cipher suite for IKE];
ike-key=[IKE pre-shared key]; description=[user-defined description];
protocol-version=I03;
```

Note The following steps are only necessary if PacketCable CALEA architecture is to be used in the network and PacketCable compliant aggregation routers (CMTS) are available in the network.

Step 3 Verify the ES_SUPP and ES_EVENT_SUPP tokens in the Aggregation table.

a. Verify that the ES_SUPP and ES_EVENT_SUPP tokens are set to Y in the Aggregation table if the associated CMTS supports packet cable CALEA requirements. Use the following command to display the ES_SUPP and ES_EVENT_SUPP tokens:

```
show aggr id=<er1>
```

b. Change the values of tokens ES_SUPP and ES_EVENT_SUPP to Y, if necessary:

```
change aggr id=<er1>; es-supp=y; es-event-supp=y;
```

Step 4 Verify that all PacketCable compliant MTAs are associated with the correct CMTS in the Aggregation table. To display the current settings in the MGW table for each MTA, enter the following command:

```
show mgw id=<mgw id for the MTA>;
```

Verify that the display from the show command in Step 4 indicates that the aggregation router (CMTS) is properly identified by the AGGR_ID token in the Media Gateway table.

Step 5 If no valid value is displayed for AGGR_ID, you must enter it using the following command:

```
change mgw id=<mgw id>; aggr-id=<Aggregation router (CMTS) ID>;
```

Note The following step is only necessary if PacketCable CALEA architecture is used in the network and SIP trunk groups are used to communicate from the BTS10200 to another CMS/MGC that supports CALEA extensions defined per CMSS signaling.

Step 6 Verify that the ES_SUPP token in the softswitch trunk group profile is set to an appropriate value. This token is used to indicate if the BTS 10200 Softswitch should ask the adjacent CMS/MGC to do surveillance on its behalf when the BTS 10200 Softswitch does not find any PacketCable call-content IAP to generate a duplicated stream on its behalf.

To display the current settings in the Softswitch trunk group profile table, enter the following command:

```
show softsw-tg-profile id=<softsw-tg-profile id>;
```