



Cisco BTS 10200 Softswitch SIP Trunk Group Authentication and Registration Feature Module

Revised: July 31, 2008

This document describes the SIP Trunk Group Authentication and Registration feature for Release 6.0.x of the Cisco BTS 10200 Softswitch and explains how to use it. This document includes the following topics:

- [Understanding the SIP Trunk Group Authentication and Registration Feature](#)
- [Provisioning](#)
- [Measurements](#)
- [Troubleshooting](#)

Understanding the SIP Trunk Group Authentication and Registration Feature

In addition to providing inter Cisco BTS 10200 connectivity, a SIP trunk serves a number of SIP subscribers through a SIP gateway, such as an IP-PBX. The SIP Trunk Group Authentication and Registration feature allows the service provider to

- Register the contact information of trunk groups
- Enable or disable authentication on specific trunk groups
- Set authentication parameters for those trunk groups

The service provider need not register for every user served by the IP-PBX, using different credentials for each user. If you enable the authentication of a SIP trunk group, the Cisco BTS 10200 does not attempt to authenticate the credentials of individual subscribers, instead it checks and authenticates the trunk group when an individual inbound call is placed through the SIP gateway on that trunk group. The credentials include username, password, realm, nonce, and response.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

**Note**

[Authentication for individual SIP subscribers](#) is an existing function. It is documented in the *Cisco BTS 10200 Softswitch SIP Feature and Provisioning Guide, Release 4.5.x*.

The service provider needs to register the contact information of specific SIP trunk groups on the Cisco BTS 10200 Softswitch. The Cisco BTS 10200 Softswitch identifies the trunk group based on

- Received user-name and realm
- Sip-Inbound-policy-profile table
- Top-Most Via header (TSAP address of the trunk group)

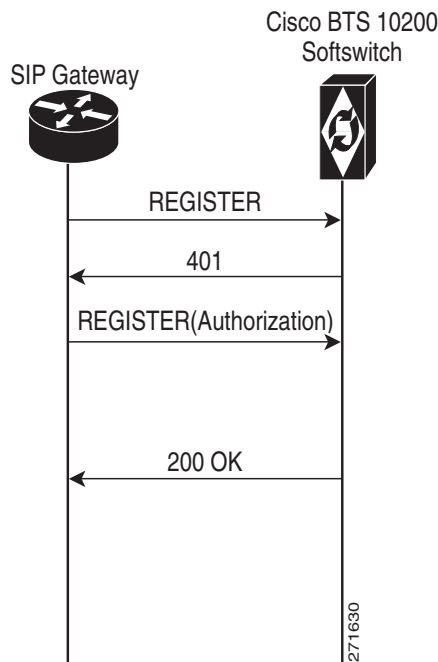
**Note**

RFC 2617 defines realm as a string that displays the username and password to a user. This string contains the name of the host that performs the authentication. In addition, the realm displays the list of users who have access.

If the Cisco BTS 10200 Softswitch does not identify the trunk group then all requests are rejected with 403 response.

[Figure 1](#) shows the registration flow.

Figure 1 Registration Flow



The following steps explain the registration flow:

1. The SIP Gateway sends the REGISTER request (without authorization header) to Cisco BTS 10200 Softswitch.
2. The Cisco BTS 10200 Softswitch challenges the REGISTER request with 401 response and requests for an authorization header. The authorization header contains the SIP trunk credentials.

**Note**

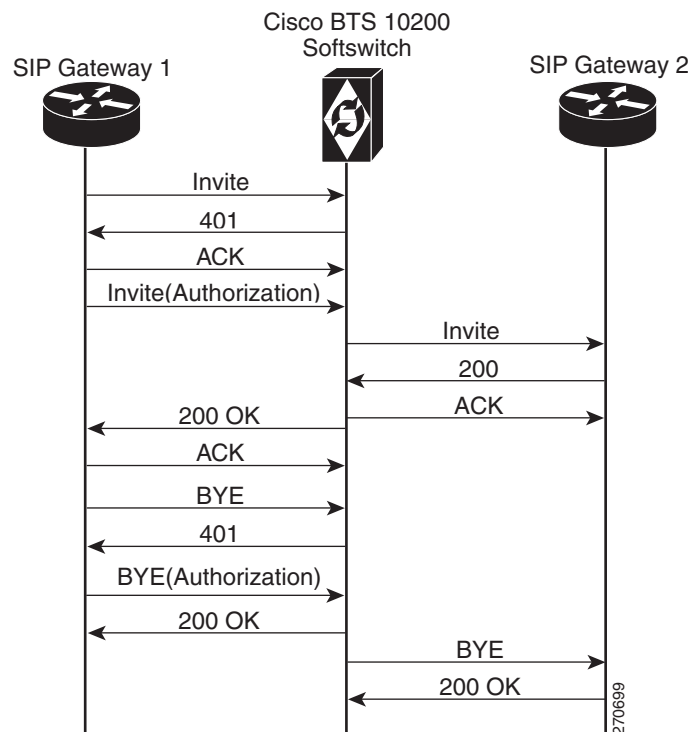
A challenge is a method to authenticate User Agent Client (UAC), here UAC is a SIP trunk. When a UAC sends a request to Cisco BTS 10200 Softswitch, the Cisco BTS 10200 Softswitch challenge the request with 401 response (requesting for credentials). The UAC resubmits the request with the credentials.

3. The SIP Gateway adds the authorization header and sends it to Cisco BTS 10200 Softswitch in response to 401 message.
4. The Cisco BTS 10200 Softswitch accepts the request and sends 200 OK message.

The Cisco BTS 10200 Softswitch allows the subscriber to place a call by authenticating the specific trunk group based on the authentication information provisioned in the sip-tg-auth-reg table. The registration information is used for routing the outbound requests towards a trunk group.

Figure 2 shows the processing of an incoming request and the messaging involved in the Cisco BTS 10200 softswitch for the SIP Trunk Group Authentication and Registration feature.

Figure 2 Processing of an Incoming Request



The following steps explain the call flow:

1. The SIP Gateway 1 sends the Invite request (without authorization header) to the Cisco BTS 10200 Softswitch when the subscriber tries to place a call.
2. The Cisco BTS 10200 Softswitch sends the 401 response requesting for authorization header.
3. The SIP Gateway 1 sends the ACK message that it has received the 401 message.
4. The SIP Gateway 1 again sends the Invite request with authorization header to the Cisco BTS 10200 Softswitch in response to 401 message.
5. After receiving the second INVITE with credentials, the Cisco BTS 10200 verifies and authenticates the credentials.

6. If the authentication is successful, then the Cisco BTS 10200 Softswitch forwards this Invite to SIP Gateway 2. The SIP Gateway 2 sends the 200 OK message to the Cisco BTS 10200 Softswitch.
7. The Cisco BTS 10200 Softswitch sends the 200 OK message to SIP Gateway 1.
8. The subscribers are in a call.
9. When the subscriber wants to terminate the call, a BYE request is sent to the Cisco BTS 10200 Softswitch.
10. The Cisco BTS 10200 Softswitch sends the 401 response requesting for authentication header.
11. The Gateway sends the BYE request with authorization header.
12. The Cisco BTS 10200 Softswitch sends the 200 OK message and the call is released.

Limitations

This section lists limitations. These are conditions for which the feature is not designed to work, or conditions that cause it to work in a limited manner.

- Authenticates only a maximum of 2000 SIP trunk groups.
- Does not challenge the unidentified requests using the default realm.
- Does not identify a trunk group based on username and realm.

Interoperability

The interoperability testing for this feature has been performed with the Cisco 2811 Integrated Services Router over SIP trunks. For the SIP-based PBX application, the Cisco 2811 router acts as a time-division multiplexing (TDM) IP gateway. To deploy other equipment or software on a trunk group with authentication and registration features, verify the interoperability with Cisco BTS 10200 Release 6.0.x.

Additional details are as follows:

- The Cisco 2811 IOS software tested by Cisco for interoperability is the IOS 12.4(15)T3 image.
- The SIP-to-ISDN (PRI) conversion mapping is an existing IOS function and is documented in the Cisco IOS software guide,
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter_09186a00807561f8.html#wp1047641

Provisioning

To provision the SIP Trunk Group Authentication and Registration feature, do the following:

Step 1 Provision the SIP trunk to the Cisco 2811 according to the procedures in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide (Release 4.5.x)*.

Step 2 Create an authentication realm.

```
add auth_realm id=<id>; description=<description>;
```

Example: add auth_realm id=cisco.com; description=Auth realm for SIP trunks;

Step 3 Enable the SIP trunk registration and authentication, then set the parameters in the sip_tg_auth_reg table.

```
add sip-tg-auth-reg tgn-id=<id>; authentication=[Y | N]; registration=[Y | N];
auth-realm_id=<id>; auth-user=tg_pbx_1; password=<password>;
reg-contact-routing_algo=ip_route; unregistered_calling=[Y | N];
max_registration_time=<time in seconds>; min_registration_time=<time in seconds>;
```

Example: add sip-tg-auth-reg tgn-id=4328;authentication=Y;
registration=Y;auth-realm_id=Cisco.com;auth-user=tg_pbx_1; password=abc1234;
reg-contact-routing_algo=IP_ROUTING; unregistered_calling=y; max_registration_time = 30;
min_registration_time= 20;

This sample command includes only mandatory parameters for provisioning SIP trunk registration and authentication. Before entering the command, take into account the following parameter details:

- For additional details on the sip_tg_auth_reg table, see the *Cisco BTS 10200 Softswitch CLI Database*.
- If you set authentication=Y, then enter valid nonnull values for auth_user, auth_realm_id, and password; the auth_realm table referenced by auth_realm_id must already exist.
- If you set authentication=N, then the system does not use auth_user, auth_realm_id, or a password.
- You should set registration=y only if the remote SIP gateway is configured to send registration requests to the Cisco BTS 10200. Else, set registration=n. If you set registration=n and the SIP gateway sends a registration request, the Cisco BTS 10200 fails the call with a 403 response.
- The setting of values for min_registration_time and max_registration_time (in seconds) allows you to adjust the minimum and maximum registration time (in seconds) which enables the registration of the gateway with the Cisco BTS 10200. Increase or decrease the values if you are unable to register. The default values are shown in the example.



Note

If you set the Unregistered_Calling =N in the Sip-tg-auth-reg table, the subscribers from an unregistered SIP trunk cannot place a call.

Step 4 Use the following command to change the registration and authentication parameters:

```
Change sip-tg-auth-reg tgn-id=<id>; authentication=[Y | N]; registration=[Y | N];
auth-realm_id=<id>; auth-user=tg_pbx_1; password=<password>;
reg-contact-routing_algo=ip_route; unregistered_calling=[Y | N];
max_registration_time=<time in seconds>; min_registration_time=<time in seconds>;
```

Example: change sip-tg-auth-reg tgn-id=4328;authentication=N;registration=N;
auth-realm_id=Cisco.com;auth-user=tg_pbx_1; password=abc1234;
reg-contact-routing_algo=IP_ROUTING; unregistered_calling=y; max_registration_time = 3600;
min_registration_time= 360;

- Step 5** The following **show** command displays the information set in the Sip-tg-auth-reg table (if provisioned) and also the realm id (if provisioned) for the same trunk group ID:

```
show sip-tg-auth-reg tgn-id=<id>;
```

Example: show sip-tg-auth-reg tgn-id=4328;

```
TGN_ID=4328
AUTH_REALM_ID=tb-cisco
AUTH_USER=5063866666
AUTHENTICATION=Y
MAX_REGISTRATION_TIME=30
MIN_REGISTRATION_TIME=20
REG_CONTACT_ROUTING_ALGO=IP_ROUTING
REGISTRATION=Y
UNREGISTERED_CALLING=N
```

- Step 6** The following **show** command displays the sip-tg-auth-reg columns if a corresponding entry is available for the trunk-grp:

```
show trunk-grp id=<id>;
```

Example: show trunk-grp id=4328;

```
ID=4328
CALL_AGENT_ID=CA146
TG_TYPE=SOFTSW
SOFTSW_TSAP_ADDR=sia-ari10ca146.hrndevtest.cisco.com:5210
TG_PROFILE_ID=SS_PRO_4328
STATUS=INS
DIRECTION=BOTH
SEL_POLICY=ASC
GLARE=SLAVE
ALT_ROUTE_ON_CONG=N
SIGNAL_PORTED_NUMBER=N
POP_ID=1
DIAL_PLAN_ID=BASIC_DPP
DEL_DIGITS=0
TRAFFIC_TYPE=LOCAL
ANI_BASED_ROUTING=N
MGCP_PKG_TYPE=NA
ANI_SCREENING=N
SEND_RDN_AS_CPN=N
SEND_EARLY_BKWD_MSG=N
EARLY_BKWD_MSG_TMR=5
SCRIPT_SUPP=N
VOICE_LAYER1_USERINFO=AUTO
VOICE_INFO_TRANSFER_CAP=AUTO
POI=INTER_ENDOFFICE
PERFORM_LNP_QUERY=N
IGNORE_INBOUND_LNP=N
EMERGENCY_TRUNK_GROUP=N
CUT_THRU_BEFORE_ANSWER=N
ENABLE_ROUTE_HEADER=N
ROUTE_HEADER_TRANSPORT_TYPE=UDP
OUTPULSE_CASUAL_AS_DIALED=N
OUTPULSE_PREFIX1_AS_DIALED=N
OUTPULSE_OPERATOR_AS_DIALED=N
OUTPULSE_INTL_AS_DIALED=N
OUTPULSE_INTL_OPR_AS_DIALED=N
DEFAULT_ROUTING=N
EGRESS_ROUTING=N
MDII_ENABLE=Y
```

```

SEND_CPNCHN_NONGEO=N
SEND_TNS=N
AUTH_REALM_ID=tb-cisco
AUTH_USER=5063866666
AUTHENTICATION=Y
MAX_REGISTRATION_TIME=30
MIN_REGISTRATION_TIME=20
REG_CONTACT_ROUTING_ALGO=IP_ROUTING
REGISTRATION=Y
UNREGISTERED_CALLING=N

```

Step 7 Use the following command to delete the entry in the sip-tg-auth-reg table:

```
delete sip-tg-auth-reg tgn-id=<id>;
```

Example: delete sip-tg-auth-reg tgn-id=4328;

Measurements

Measurements are the statistical data that helps the service provider to monitor and track the activity. The service provider can view the measurements for the SIP Trunk Group Authentication and Registration feature by entering the following command. In this example the measurements are shown for the trunk group 80035.

```
report measurement_tg_usage_summary; tgn_id=<id>;
```

Example: report measurement_tg_usage_summary; tgn_id=80035;

The following are the measurements applicable to this feature:

- TRKGRP_REGISTERS_RECVD—The total number of SIP REGISTER methods received for the specified trunk group.

For more information on SIP REGISTER methods, refer *RFC 3261*.

- TRKGRP_401S_SENT—The total number of SIP 401 challenge responses sent for the SIP requests received.

The **status** command displays the registration status of the trunk group with the registration information (Contact IP and port with Expiry time).

```
status trunk-grp id=<id>;
```

Example: status trunk-grp id=4328;

```

RESULT -> ADM configure result in success
REASON -> ADM executed successfully
ADMIN STATE -> ADMIN_INS
OPER STATE -> Trunk group in-service
REGISTRATION-STATE -> Registered
REGISTERED-CONTACT -> USER:Jim
HOST:cisco.com
PORT:4444
REGISTRATION-EXPIRY-TIME -> Wed Apr 30 06:16:21 2008

```

Troubleshooting

If the Cisco BTS 10200 attempts to authenticate an incoming request on a SIP trunk and determines that the credentials for the trunk group is invalid, then the system fails the request. When the request fails, a SECURITY(7) warning alarm is generated.

When the registration expires on a trunk group that has registration enabled, the TRUNK-GRP-REG-EXPIRY alarm is generated. The receipt of a subsequent registration resets the alarm.

You can interpret the following datawords as follows:

- TGN_ID —The TG ID number over which the call was attempted, for example, TG ID=22
- SIP REG CONTACT —The contact that successfully registered with that trunk-grp
- REG EXPIRY TIME—The time when this registered contact expires and becomes invalid

When the authentication fails for a trunk group, the TRUNK-GRP-AUTH-FAILED alarm is generated. This is reported as a warning alarm.

You can interpret the following datawords as follows:

- AUTH USER—The authentication user name provisioned in sip_tg_auth_reg table for the trunk
- AUTH REALM—Realm in which the request received over this trunk group is challenged
- TGN_ID —The TG ID number over which the call was attempted, for example, TG ID=22
- SIP Request Message—The type of SIP request message, for example, Invite, Register, and so on

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved.