Abstract

This document provides guidelines for configuring a SIP Trunk between a CS 1000 Release 7.0 and Acme Packet Net-Net 6.2.0 Session Border Controller (3000 and 4000 series) at the customer premise and AT&T IP Flexible Reach (MIS/PNT and AVPN).
# Table of Contents

**INTRODUCTION** ........................................................................................................................................... 4

  - PRE-IP PBX CONFIGURATION ACTIVITY .................................................................................. 4
  - CUSTOMER QUESTIONS ........................................................................................................... 5
  - TROUBLE REPORTING .......................................................................................................... 5
  - DOCUMENT FEEDBACK ...................................................................................................... 5
  - DOCUMENT CHANGE HISTORY .......................................................................................... 5

**SPECIAL NOTES** ................................................................................................................................. 6

**OVERVIEW** ............................................................................................................................................... 8

**CS 1000 RELEASE 7 AND IP FLEXIBLE REACH** .............................................................................. 11

  - CS 1000 VERSION AND RELEASE ....................................................................................... 11
  - CS 1000 PATCHES ............................................................................................................... 12
  - NODE CONFIGURATION ....................................................................................................... 13
    - Voice Gateway (VGW) and Codecs .................................................................................. 13
    - LAN Configuration ........................................................................................................... 14
    - SIP Gateway Settings ...................................................................................................... 14
  - MEDIA GATEWAY CONTROLLER ....................................................................................... 17
  - BANDWIDTH ZONES ............................................................................................................ 19
  - VOIP TRUNKING .................................................................................................................. 20
    - Creating D-Channels ......................................................................................................... 20
    - Incoming Digit Conversion and CLID Trees ...................................................................... 21
    - Creating Routes ................................................................................................................ 23
    - Adding Trunks to the Specific Route ................................................................................ 25
    - Creating a Digit Manipulation Index (DMI) ..................................................................... 27
    - Creating Route List Block Indices (RLI) ........................................................................... 27
    - Allowing/Restricting Numbering Plan Area (NPA) Codes ............................................... 29
    - Configuring Special Numbers .......................................................................................... 29

**ACME PACKET NET-NET SESSION BORDER CONTROLLER** .......................................................... 31

**BASIC MONITORING AND CALL TRACING ON CS 1000** ............................................................ 58

  - VIEWING REGISTERED SETS ON CS 1000 ........................................................................ 58
  - ACTIVE CALL INFORMATION .............................................................................................. 58
  - SIP CALL TRACING ............................................................................................................. 59
  - PACKET CAPTURE TOOLS ................................................................................................. 60

**APPENDIX A: TABLE OF ACRONYMS** ................................................................................................. 61
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>AT&amp;T IP Flexible Reach Network</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>AT&amp;T IP Flexible Reach and Private Networking</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3</td>
<td>CS 1000 Release 6.0 Call Server Software Release</td>
<td>11</td>
</tr>
<tr>
<td>Figure 4</td>
<td>CS 1000 Release 7.0 Signaling Server Software Release</td>
<td>12</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Node Configuration Screen</td>
<td>13</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Voice codecs and Fax</td>
<td>14</td>
</tr>
<tr>
<td>Figure 7</td>
<td>RTP/RTCP Port for IP Sets</td>
<td>14</td>
</tr>
<tr>
<td>Figure 8</td>
<td>SIP GW Settings, General</td>
<td>15</td>
</tr>
<tr>
<td>Figure 9</td>
<td>SIP GW Settings</td>
<td>15</td>
</tr>
<tr>
<td>Figure 10</td>
<td>SIP URI Map</td>
<td>16</td>
</tr>
<tr>
<td>Figure 11</td>
<td>MGC VGW and IP Phone Codec Profile (1)</td>
<td>17</td>
</tr>
<tr>
<td>Figure 12</td>
<td>MGC VGW and IP Phone Codec Profile (2)</td>
<td>18</td>
</tr>
<tr>
<td>Figure 13</td>
<td>VTRK Bandwidth Zone</td>
<td>19</td>
</tr>
<tr>
<td>Figure 14</td>
<td>IP Phone Zone Settings</td>
<td>19</td>
</tr>
<tr>
<td>Figure 15</td>
<td>D-Channel Basic Configuration</td>
<td>20</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Remote Capabilities (RCAP)</td>
<td>21</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Incoming Digit Conversion Tree</td>
<td>21</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Route Configuration</td>
<td>24</td>
</tr>
<tr>
<td>Figure 19</td>
<td>IDC for route</td>
<td>25</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Adding Multiple Trunks</td>
<td>25</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Trunk Basic Configuration</td>
<td>26</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Trunk Advanced Configuration</td>
<td>26</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Disabling Media Security on the Trunk</td>
<td>26</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Digit Manipulation Index</td>
<td>27</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Route List Block Index 16</td>
<td>28</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Route List Block Index 17</td>
<td>28</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Route List Block Index 18</td>
<td>29</td>
</tr>
<tr>
<td>Figure 28</td>
<td>NPA Codes</td>
<td>29</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Special Numbers (International)</td>
<td>29</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Special Numbers (18YY)</td>
<td>30</td>
</tr>
<tr>
<td>Figure 31</td>
<td>Special Numbers (411)</td>
<td>30</td>
</tr>
</tbody>
</table>
Introduction

This document provides a configuration guide to assist Avaya Communication Server 1000 (CS 1000) and Acme Packet Net-Net Session Border Controller administrators in connecting to AT&T IP Flexible Reach service via SIP.

Avaya Communication Server 1000 Release 7.0 is a telephony application server and is the point of connection between the enterprise endpoints and the Acme Packet Net-Net Session Border Controller (SBC).

An Acme Packet Net-Net Session Border Controller is the point of connection between Avaya Communication Server 1000 and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice-over-IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise’s sites. The AT&T IP Flexible Reach service utilizes AVPN or MIS/PNT transport services.

This configuration guide pertains specifically to the AT&T IP Flexible Reach service and is not intended for configuring a CS 1000 system for new installation.

Pre-IP PBX Configuration Activity

This guide assumes that the administrator is knowledgeable in CS 1000 IP PBX programming and operations.

An important tool that the administrators should have at their disposal prior to testing their IP PBX with IP Flexible Reach is a network protocol analyzer. Such software can be used to run traces on problem calls so the information can be shared with equipment and network engineers. There is a free version of such software that can be obtained at http://www.wireshark.org/.

A second alternative that customers may use is TCPDUMP, which can be found on most UNIX and Linux systems. To use this software the customer should have Wireshark or TCPDUMP loaded on a server that is connected to a LAN switch or hub that can monitor both the signaling and media packets on any calls between the customer PBX and the IP Flexible Reach managed router. Please note, however, that AT&T does not offer, warrant, or support this software, and any use of the Wireshark or TCPDUMP software is entirely at the customer’s own risk.
Customer Questions

If there are any questions regarding the procedures in the guide, please contact Brian Stegemoller at +1 (972) 745-5139. When calling this number, please have the following information available:

- Company name
- Company location
- Administrator name and phone number
- IP PBX name and software version
- Customer Configuration Guide – Issue number and date

Trouble Reporting

Avaya and AT&T will make every effort to quickly resolve reported troubles. The time required for trouble shooting can be reduced if the customer has the necessary detailed information available when reporting a problem. Prior to reporting a problem please provide a Wireshark or TCPDUMP trace of the failed call.

Document Feedback

IP PBX administrators who would like to provide feedback on the contents of this document should send it to Brian Stegemoller (brianstegemo@avaya.com), with a copy to Albert Chee (alchee@avaya.com) and Steven Chen (stevenchen@avaya.com).

Document Change History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue 0.0</td>
<td>February 8, 2011;</td>
<td>Draft</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue 1.0</td>
<td>March 1, 2011;</td>
<td>Revised Issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue 1.1</td>
<td>April 12, 2011;</td>
<td>Revised Issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Special Notes

Emergency 911/E911 Services Limitations and Restrictions
Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer’s responsibility to ensure proper operation with its equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user’s CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer’s location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

Unattended Transfers Limitations
An unattended transfer is one in which the party initiating the transfer hangs up prior to answer by the party to whom the call is being transferred. When 2 phones are in an active call on the CS 1000 and one of those phones performs an unattended transfer to an endpoint on the AT&T network, the CS 1000 will not allow this call to be transferred. However, attended (consultative) transfers and conferences are allowed.

G.726 Codec not supported
CS 1000 does not support the G.726 codec; therefore, G.711 and G.729 codecs should be used. If the CS 1000 cannot negotiate a supported codec, it will respond with a “488 Not Acceptable Here” SIP error.

G.729 and G.711 Codec Preferences Should Match
G.729 and G.711 codec preferences should match in the CS 1000 in terms of voice payload size and voice activity detection (VAD). Additionally, the CS 1000 voice payload size settings should match with the Acme Packet Net-Net SBC in terms of ptime when configuring the SBC. The available options are 20 or 30.

DTMF Payload Type Renegotiation with CallPilot Applications
If you are encountering dropped calls in scenarios involving CallPilot applications such as auto attendant and voicemail, it may be attributed to DTMF payload type renegotiation. If AT&T Customer Care or Avaya Support determines that this is the case, they may ask you to use the following setting:

Change the CS 1000’s RFC2833 payload type from the default 101 to 100 via the command setRFC2833PT 100 in the Call Server’s PDT prompt. Note that the RFC2833 payload type...
parameter reverts to default upon reboot of the system; therefore, administrators would need to re-enter the command after a reboot.

**CS 1000 Mobile Extension (Mobile-X) Limitations**

CS1000 Mobile Extension features are currently limited to the following with AT&T IP Flexible Reach:

- Simultaneous ringing of desk and mobile phones
- Device handoff between desk and mobile phones
- Call in Progress features (i.e., conference and transfer) via the Mobile-X Feature Activation Code (MFAC)

Also, special numbers, such as 411 and 8YY, should not be used as Mobile Extension destinations.
Overview

This section provides a service overview of the Avaya Communication Server 1000 (CS 1000) IP PBX and Acme Packet Net-Net Session Border Controller integration with AT&T IP Flexible Reach service.

Customer Premises

- Phones and IP PBX Server in Private Address space
- AT&T CE Router (MIS/PNT requires an AT&T-managed router, AVPN can be either AT&T-managed or customer-managed)

Customer Sites connect to AT&T IP Border Element (IPBE)

The CS 1000 customer premises site shall consist of the following components:

- The Acme Packet Net-Net SBC provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. **The Net-Net 3000 and 4000 Series models, running Release 6.2.0 or greater, are supported.**
- Avaya CS 1000 IP PBX – This unit consists of the following:
  - Dedicated Signaling Server (COTS servers or CP-PM cards)
  - Call Server (with CP-PIV and/or CP-PM cards)
  - Media Gateway Controller (MGC) card to provide Digital Signaling Processor (DSP) resources for connecting IP and Time Division Multiplexing (TDM) devices together and for advanced applications such as conferences and voicemail access
  - CallPilot voicemail system (optional)
  - Digital Line Card (DLC) for Meridian digital sets (optional)
- Analog Message Waiting Line Card (AM/WLC) for connection to fax machines and analog sets (optional)
- Meridian Integration Recorded Announcement (MIRAN) card for recorded announcements and music-on-hold (optional)
- TMDI card for PRI/T1 trunking to the PSTN (optional)

- Avaya IP Phone 2000 series, 1100 series, IP Softphone 2050 (Release 3.00.0197 and up) – These phones use the Avaya UNIStim signaling protocol to communicate to the CS 1000 IP PBX for call feature and routing support. These phones can be connected to Avaya Ethernet switches (ES 470, ERS 5520, etc.) that supply in-line power (IEEE 802.3af) to the phones. For a complete list of supported phones, please refer to the CS 1000 documentation.

**IMPORTANT** A dedicated Signaling Server will be needed for connectivity to AT&T IP Flexible Reach service. Private MCDN features would require an additional Signaling Server. See figure below.

![Figure 2: AT&T IP Flexible Reach and private networking](image)

*Please note that this guide **DOES NOT** describe the procedures to configure private MCDN functionality with the CS 1000. This guide only pertains to the Signaling Server connected to AT&T IP Flexible Reach service.*

The following routing scenarios are supported by the Avaya CS 1000 IP PBX and **DO NOT** use the AT&T Call Control:

---

Reviewed: 4/12/2011

CS 1000 Application Notes

©2011 Avaya Inc. All Rights Reserved.

CS1000R7_AcmeR620_IPFR

18-603958
- Local CS 1000 phone to local CS 1000 phone

The following routing scenarios are supported by the CS 1000 IP PBX and **DO** use the AT&T Call Control. For voice calls, the G.729 codec shall be used:

- CS 1000 phones to PSTN (domestic US and international)
- CS 1000 phones to legacy PBX site with Cisco gateway
- Legacy PBX site with Cisco gateway to CS 1000 phones
- CS 1000 phones at one CS 1000 IP PBX site to CS 1000 phones at another CS 1000 IP PBX site.

If the customer has subscribed to Calling Plans B and C (Local), then the following routing scenarios are supported by the CS 1000 IP PBX and **DO** use the AT&T Call Control. For voice calls, the G.729 or G.711 codec may be used.

- Inbound PSTN to CS 1000 phone
- Outbound local PSTN calls from CS 1000 phone
- Outbound local N11 (i.e. 411, 911) calls from CS 1000 phone

Fax was tested and is supported on the CS 1000 using the T.38 fax protocol through the AT&T IP Flexible Reach network to/from the following:

- PSTN
- Legacy PBX site with Cisco gateway
- Another CS 1000 IP PBX site
CS 1000 Release 7 and IP Flexible Reach

This configuration guide contains the Avaya CS 1000 screens that must be configured and updated to support the AT&T IP Flexible Reach service.

CS 1000 Version and Release

The CS 1000 Call Server must be running release 700Q. You can check the version of CS 1000 by viewing the following screen on the Home page:

System Overview
This system has insecure passwords. Change the password to comply with security rules.

![System Overview Screen](image)

IP Address: 192.12.0.100
Type: Nortel Communication Server 1000E CPPM
Version: 4021
Release: 700 Q +

Figure 3: CS 1000 Release 6.0 Call Server software release

NOTE The Call Server can be either a CP-PM or CP-PIV processor.

The CS 1000 Signaling Server must be running release 7.00.20. This can be found in Base Manager.
These are the supported releases that are required for AT&T IP Flexible Reach service.

**CS 1000 Patches**

No specific patches are required for SIP interoperability with AT&T IP Flexible Reach.

However, it is strongly recommended to load the latest CS 1000 Service Packs, Service Updates and LOADWARE* into the system. These can be downloaded by going to [http://support.avaya.com/espl](http://support.avaya.com/espl).

* LOADWARE MGCCBD02 is required on the MGC card for successful inbound fax calls.
Node Configuration

Add or edit a SIPGw node in the System » IP Network » Node Configuration menu with the following configuration as noted in the below screenshots:

![Node configuration screen](image)

**Voice Gateway (VGW) and Codecs**

The following Voice Codecs should be enabled:

- **G711**
  - Voice payload size to 20 or 30 ms/frame (should match G.729 voice payload size)
  - VAD (optional, should match G.729 VAD setting)
- **G729**
  - Voice payload size to 20 or 30 ms/frame (should match G.711 voice payload size)
  - VAD (optional, should match G.711 VAD setting)
- **T38 FAX**

For default configurations, G.729A codec will be used for voice calls. However, in the case that G.729B needs to be configured instead of G.729A, ensure that VAD is checked.
LAN Configuration

All IP sets use the same port for media. This is specified in the LAN configuration section, under the Telephony LAN (TLAN) configuration sub-section. In the figure below, the port 28802 was entered for RTP/RTCP Starting Port.

SIP Gateway Settings
Select SIP Gateway (SIPGw) for the **Vtrk gateway application**. Enter the **SIP Domain name** as the Acme Packet Net-Net SBC’s trusted IP address. The **Local SIP Port** should be 5060.

![Figure 8: SIP GW settings, General](image)

AT&T IP Flexible Reach service does not support TLS Security, thus the **TLS Security** should be set to “Security Disabled.” Enter the Acme Packet Net-Net SBC’s trusted IP address for the **Proxy Server Route 1: Primary TLAN IP address**, ensure the **Port** used is 5060, and the **Transport Protocol** used is UDP.

![Figure 9: SIP GW Settings](image)

For **Proxy Server Route 2: Primary TLAN IP address**, enter the same as above if no secondary proxy server route is available.
Ensure that all parameters for the SIP URI Map are left blank.

![SIP URI Map](image)

*Figure 10: SIP URI map*
Media Gateway Controller

Ensure that the codec settings for the Media Gateway Controller (MGC) card, under the VGW and IP phone codec profile section in the System » IP Network » Media Gateways » IPMG x x Property Configuration » IPMG x x Media Gateway Controller (MGC) Configuration, match the codec settings for the Node interfacing with AT&T. For interoperability with AT&T, use the same codec configuration as for the Voice Codecs and Fax in Section 4.3.1.

Enable **V.21 FAX tone detection** for T.38 Fax.

```
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable echo canceller</td>
<td>✓</td>
</tr>
<tr>
<td>Echo canceller tail delay</td>
<td>64</td>
</tr>
<tr>
<td>Enable dynamic attenuation</td>
<td>✓</td>
</tr>
<tr>
<td>Voice activity detection threshold</td>
<td>1</td>
</tr>
<tr>
<td>Idle noise level</td>
<td>0</td>
</tr>
<tr>
<td>R factor calculation</td>
<td></td>
</tr>
<tr>
<td>DTMF tone detection</td>
<td>✓</td>
</tr>
<tr>
<td>Enable low latency mode</td>
<td></td>
</tr>
<tr>
<td>Remove DTMF delay (squelch DTMF from TDM to IP)</td>
<td>✓</td>
</tr>
<tr>
<td>Enable modem/fax pass through mode</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Enable V.21 FAX tone detection</strong></td>
<td>✓</td>
</tr>
<tr>
<td>Fax TCF method</td>
<td>2</td>
</tr>
<tr>
<td>FAX maximum rate</td>
<td>14400</td>
</tr>
<tr>
<td>FAX playout nominal delay</td>
<td>100</td>
</tr>
<tr>
<td>FAX no activity timeout</td>
<td>20</td>
</tr>
<tr>
<td>FAX packet size</td>
<td>30</td>
</tr>
</tbody>
</table>
```

Figure 11: MGC VGW and IP phone codec profile (1)
<table>
<thead>
<tr>
<th>Codec</th>
<th>Voice payload size</th>
<th>Voice playout (jitter buffer) nominal delay</th>
<th>Voice playout (jitter buffer) maximum delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>G711</td>
<td>30 ms/frame</td>
<td>60 ms</td>
<td>120 ms</td>
</tr>
<tr>
<td>G729A</td>
<td>30 ms/frame</td>
<td>60 ms</td>
<td>120 ms</td>
</tr>
<tr>
<td>G723.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T38 FAX</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modifications may cause changes to dependent settings

VAD

Figure 12: MGC VGW and IP phone codec profile (2)
Bandwidth Zones

To ensure that G.729 codec is used, SIP (VTRK) trunks should be in a ZONE that uses “Best Bandwidth (BB)” zone strategy. For G.711, use “Best Quality (BQ).”

If phones and voice resources are in other zones, Interzone Strategy settings should be configured accordingly to get the desired codec preferences. Below is an example of the IP Phone zone settings:

The CS 1000 will determine the codec used based the combination of the Interzone Strategy settings between the two zones. If both zones are configured for Best Bandwidth, CS 1000 will negotiate G.729 codec. If both zones are configured for Best Quality, G.711 will be used. If one zone is configured for Best Quality and the other for Best Bandwidth, G.729 will be used.
VoIP Trunking

Voice over IP (VoIP) lines, are signaling channels that simulate how CO lines work. However, VoIP lines transmit data to the IP network over a LAN or IP network rather than over physical lines.

To create VoIP trunks on the CS 1000 to the AT&T IP Flexible Reach service, the following steps need to be executed:

- Create D-Channels
- Create Incoming Digit Conversion (IDC) and Calling Line Identification (CLID) trees
- Create Routes
- Add trunks to the specific Route
- Create a Digit Manipulation Index (DMI)
- Create Route List Block Indices (RLI)
- Allow/Restrict NPA Codes
- Configure Special Numbers

Creating D-Channels

Call signaling on the CS 1000 resides on the D-channels. A route will be mapped to this D-channel, in which the Signaling Server will send call signaling to the AT&T IP Flexible Reach service using the specified D-channel. Under the Routes and Trunks » D-Channels, add a D-channel with the following configuration (only required program settings is shown):

![D-channel basic configuration](image-url)
Under **Remote Capabilities (RCAP)**, we used Network name display method 2 (ND2).

![Remote Capabilities (RCAP)](image)

**Incoming Digit Conversion and CLID Trees**

Recommended best practices for planning DNs with DIDs is to map the last four digits of the Direct Inward Dialing (DID) number to the CS 1000 DNs. However, there will be scenarios where DNs may not match with the AT&T-provided DID number extensions. In this case, the Incoming Digit Conversion (IDC) and Calling Line Identification (CLID) trees will be used.

**Creating IDC Trees**

The IDC tree will allow incoming digits to be converted to specified local extensions. These local extensions can be IP phones, voicemail retrieval extensions, control DNs (CDNs), etc. This is done in **Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree x Configuration** menu, clicking “Add,” then entering incoming and converted digits; see figure below:

![Digit Conversion Tree 1 Configuration](image)

If AT&T IP Flexible Reach service sends 732-216-2779 to the CS 1000, the CS 1000 will use entry 2 to strip 732-216-2, convert the digits to 2, append the remainder of the digits and ring the set with DN 2779.
IDC trees can also be configured via the Call Server CLI. For example, to convert 732-368-0430 to 2001, go to LD 49:

```
>ld 49
DGT000
MEM AVAIL: (U/P): 99201863 USED U P: 5027918 40040 TOT: 104269821
DISK SPACE NEEDED: 41 KBYTES
REQ chg
TYPE idc
CUST 0  <customer number>
DCNO 1  <digit conversion tree number>
IDGT 7323680430  <incoming digit>
7323680432 2001  <converted digit>
IDGT
```

**Creating CLID Trees**

The same concept is applied to Direct Outward Dialing (DOD) numbers for outbound calling numbers. This is done in the Call Server CLI, LD 15.

For matching DNs and DODs, for example, DN 2779 to 732-216-2779:

```
>ld 15
MEM AVAIL: (U/P): 99201833 USED U P: 5027918 40070 TOT: 104269821
DISK SPACE NEEDED: 41 KBYTES
REQ chg
TYPE: net
CUST 0
OPT AC2
FNP
CLID yes
SIZE INTL
ENTRY <enter #>
HNTN 732
ESA_HLCL
ESA_INHN
ESA_APDN
HLCL 216
DIDN YES  * use when DN matches DOD extension
HLOC
LSC
CLASS_FMT DN
ENTRY # SAVED!
```

Be sure when you configure the keys for the IP set in LD 11 with the above configuration, use the appropriate CLID table entry #. For example, KEY 0 scr 2779 # will allow the CS 1000 to send calling party number of 732-216-2779 out to AT&T IP Flexible Reach service.

For non-matching DODs and DNs, for example, DN 2001 needs to be converted to DOD 732-368-0430:

```
>ld 49
DGT000
MEM AVAIL: (U/P): 99201863 USED U P: 5027918 40040 TOT: 104269821
DISK SPACE NEEDED: 41 KBYTES
REQ chg
TYPE idc
CUST 0  <customer number>
DCNO 1  <digit conversion tree number>
IDGT 7323680430  <incoming digit>
7323680432 2001  <converted digit>
IDGT
```
Be sure to use the appropriate CLID table entry # when configuring the keys for the IP set in LD 11.

Creating Routes

Once the D-Channel is created, routes will be created to map to the D-Channel and the IDC trees, if applicable. The route will be configured with SIP trunking to the AT&T IP Flexible Reach service. At the Routes and Trunks » Routes and Trunks screen, add a route (only required program settings are shown):

```
>ld 15

MEM AVAIL: (U/P): 99201833 USED U P: 5027918 40070 TOT: 104269821
DISK SPACE NEEDED: 41 KBYTES
REQ: chg
TYPE: net
CUST 0
OPT
AC2
FNP
CLID yes
SIZE
INTL
ENTRY <enter #>
  HNTN 732
  ESA_HLCL
  ESA_INHN
  ESA_APDN
  HLCL 3680430
  DIDN NO
  * use when DN DOES NOT match DOD extension
  HLOC
  LSC
  CLASS_FMT DN
  ENTRY # SAVED!
```
Ensure of the following settings:

- **Trunk Type** is TIE
- **Incoming and Outgoing trunk** is Incoming and Outgoing (IAO)
- **The route is a virtual trunk route** is checked
- **Node ID of signaling server** is set to Signaling Server peering with AT&T IP Flexible Reach service
- **Zone for codec selection and bandwidth management** is set to a zone for the virtual trunks
- **Protocol ID for the route** is SIP
- **ISDN option** is checked
- **Mode of operation** is ISLD
- **D channel number** is D-channel created for IP Flexible Reach
- **Private Network Identifier (PNI)** is 0
Furthermore, under the same screen, in **Basic Route Options**, ensure that IDC is checked and enter in IDC tree numbers for both Day and Night IDC trees.

![Basic Route Options](image)

**Figure 19: IDC for route**

### Adding Trunks to the Specific Route

Trunks can now be added to associate with a given route. Back to the **Routes and Trunks » Routes and Trunks** screen, for the route created in the previous section, click “Add trunk.”

![Adding multiple trunks](image)

**Figure 20: Adding multiple trunks**

**NOTE:** To add multiple trunks, select the number of trunks to add from the drop-down menu in **MTINPUT**.

### Under the Basic Configuration, ensure the following:

- **TYPE** is IPT1
- Enter **TN** for the trunks
- **XTRK** is VTRK
- **CDEN** is 8D
- **STRI, STRO** is IMM
- **CHID** is a different number for each trunk
- **INC** set to YES
Under the **Advanced Trunk Configurations**, ensure that SUPN and STYP are checked and PIP, respectively:

![Figure 21: Trunk basic configuration](image)

**Disabling Media Security on Virtual Trunks**

In conference and transfer call scenarios where the CS 1000 sends a SIP re-INVITE to an endpoint via the virtual trunks to AT&T, if “Media Security” is enabled on these trunks, calls will fail. In order to fully interoperate with AT&T IP Flexible Reach service, “Media Security” must be set to “Media Security Never (MSNV)” under the **Routes and Trunks » Routes and Trunks » Customer 0, Route x, Trunk x Property Configuration » Class of Service Configuration** for each virtual trunk peering with AT&T IP Flexible Reach service.

![Figure 22: Trunk advanced configuration](image)

![Figure 23: Disabling media security on the trunk](image)
Creating a Digit Manipulation Index (DMI)

In order for outbound calls (more specifically, special numbers) to send the correct information to the AT&T network, ensure that Digit Manipulation Indexes (DMI) are created in Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block.

Configure these per NARS/BARS specifications or refer to the CS 1000 technical documentation for more information.

In the example below, different DMI’s were created/used for different external numbers, i.e. international, N11. DMI 16 will be used for non-special local and long-distance destinations, DMI 17 will be used for international dialing, and DMI 18 for special numbers (N11, 0).

In the screenshot below:
- RLI 16 will be used with Route Number 16 and DMI 16 for non-special local and long-distance destinations.
- RLI 17 will be used with Route Number 16 and DMI 17 for international dialing.

Creating Route List Block Indices (RLI)

When an outbound call is made, based on the number dialed, a route list block index is used to determine the route and D-channel used for call signaling.

To create/modify a RLI, go to Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks.

Ensure that Route Number is set to the appropriate route number created in the “Creating Routes” section and Digit Manipulation Index is set to the desired DMI created in the “Creating a Digit Manipulation Index” section.

In the screenshot below:
- RLI 16 will be used with Route Number 16 and DMI 16 for non-special local and long-distance destinations.
- RLI 17 will be used with Route Number 16 and DMI 17 for international dialing.
- RLI 18 will be used with Route Number 16 and DMI 18 for special numbers (N11, 0).

- **Route List Block Index -- 16**
  - Initial Set: 0
  - Number of Alternate Routing Attempts: 5
  - Set Minimum Facility Restriction Level: 0
  - **Data Entry Index -- 0**
    - Route Number: 16
    - Expensive Route: N
    - Facility Restriction Level: 0
    - Digit Manipulation Index: 16
    - ISL D-Channel Down Digit Manipulation Index: 0
    - Free Calling Area Screening Index: 0
    - Free Special Number Screening Index: 0

  *Figure 25: Route List Block Index 16*

- **Route List Block Index -- 17**
  - Initial Set: 0
  - Number of Alternate Routing Attempts: 5
  - Set Minimum Facility Restriction Level: 0
  - **Data Entry Index -- 0**
    - Route Number: 16
    - Expensive Route: N
    - Facility Restriction Level: 0
    - Digit Manipulation Index: 17
    - ISL D-Channel Down Digit Manipulation Index: 0
    - Free Calling Area Screening Index: 0
    - Free Special Number Screening Index: 0

  *Figure 26: Route List Block Index 17*
Allowing/Restricting Numbering Plan Area (NPA) Codes

Add the allowed NPA codes for the CS 1000 in the **Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Numbering Plan Area Code List** menu, and map the Route List Index to the desired RLI configured in the previous section. Below is an example for area code 732:

![Route List Block Index 18](image)

Configuring Special Numbers

Special numbers are numbers that do not follow the NPA dial plans. Examples are 8YY, N11 (411, 911, etc.), and international calls. To configure these, go to **Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Special Number List**, and add allowed special numbers. Map these numbers to the desired RLIs. Below are examples for international (011), 1800, and 411 numbers:

![Special Number (international)](image)
- **Special Number -- 1800**

  Flexible Length: 11  
  Inhibit Time-out Handler: N0  
  Type of call that is defined by the special number: NONE  
  Route List Index: 16

  Figure 30: Special numbers (18YY)

- **Special Number -- 411**

  Flexible Length: 3  
  Inhibit Time-out Handler: N0  
  Type of call that is defined by the special number: NATL  
  Route List Index: 18

  Figure 31: Special numbers (411)
Acme Packet Net-Net Session Border Controller

The Acme Packet Net-Net Session Border Controller is required to interface the Communication Server 1000 Release 7.0 with AT&T IP Flexible Reach. The Acme Packet Net-Net Session Border Controller must be running on Release 6.2.0 or greater.

The following models are supported:

- 3000 Series
- 4000 Series

For configuration support, please contact Acme Packet.

NOTE  The AT&T IP Flexible Reach service border element IP addresses shown in this document are examples. AT&T Customer Care will provide the actual IP addresses as part of the IP Flexible Reach provisioning process.

NOTE  Acme Packet Net-Net SBC provisioning applicable to the reference configuration is shown in bold text. Other parameters and setting are shown for informational purposes.
**ANNOTATION:** The local policy below governs the routing of SIP messages from the AT&T IP Flexible Reach service to Communication Server 1000.

```plaintext
classic-policy
  from-address  *
  to-address  *
  source-realm  peer
description  N/A
activate-time  N/A
deactivate-time  N/A
state  enabled
policy-priority  none
  policy-attribute
    next-hop  172.16.6.110
    realm  enterprise
    action  none
    terminate-recursion  disabled
carrier
    start-time  0000
    end-time  2400
days-of-week  U-S
cost  0
app-protocol  SIP
state  enabled
methods
media-profiles
lookup  single
next-key
eloc-str-lkup  disabled
eloc-str-match
```

**ANNOTATION:** The local policies below govern the routing of SIP messages from elements on the network on which the Avaya elements (e.g. Communication Server 1000) reside to the AT&T IP Flexible Reach service.

```plaintext
classic-policy
  from-address  *
  to-address  *
  source-realm  enterprise
description  N/A
activate-time  N/A
deactivate-time  N/A
state  enabled
policy-priority  none
  policy-attribute
    next-hop  207.242.225.210
    realm  peer
```

<table>
<thead>
<tr>
<th>Action</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate-recursion</td>
<td>disabled</td>
</tr>
<tr>
<td>Carrier</td>
<td></td>
</tr>
<tr>
<td>Start-time</td>
<td>0000</td>
</tr>
<tr>
<td>End-time</td>
<td>2400</td>
</tr>
<tr>
<td>Days-of-week</td>
<td>U-S</td>
</tr>
<tr>
<td>Cost</td>
<td>0</td>
</tr>
<tr>
<td>App-protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>State</td>
<td>enabled</td>
</tr>
</tbody>
</table>

Methods

| Media-profiles |  |
| Media-manager |  |
| State | enabled |
| Latching | disabled |
| Flow-time-limit | 86400 |
| Initial-guard-timer | 300 |
| Subsq-guard-timer | 300 |
| Tcp-flow-time-limit | 86400 |
| Tcp-initial-guard-timer | 300 |
| Tcp-subsq-guard-timer | 300 |
| Tcp-number-of-ports-per-flow | 2 |
| Hnt-rtcp | disabled |
| Algdl-log-level | NOTICE |
| Mbcd-log-level | NOTICE |
| Red-flow-port | 1985 |
| Red-mgcp-port | 1986 |
| Red-max-trans | 10000 |
| Red-sync-start-time | 5000 |
| Red-sync-comp-time | 1000 |
| Media-policing | enabled |
| Max-signaling-bandwidth | 1000000 |
| Max-untrusted-signaling | 100 |
| Min-untrusted-signaling | 30 |
| App-signaling-bandwidth | 0 |
| Tolerance-window | 30 |
| Rtcp-rate-limit | 0 |
| Trap-on-demote-to-deny | enabled |
| Min-media-allocation | 2000 |
| Min-trusted-allocation | 4000 |
| Deny-allocation | 64000 |
| Anonymous-sdp | disabled |
| Arp-msg-bandwidth | 32000 |
| Fragment-msg-bandwidth | 0 |
| Rfc2833-timestamp | disabled |
| Default-2833-duration | 100 |
| Rfc2833-end-pkts-only-for-non-sig | enabled |
| Translate-non-rfc2833-event | disabled |
| Media-supervision-traps | disabled |
| Dnsalg-server-failover | disabled |
The network interface below defines the IP addresses on the interface connected to the network on which the AT&T IP Flexible Reach service resides.

```
network-interface
    name                           peer
    sub-port-id                    0
    description                   
    hostname                      
    ip-address                    12.40.234.2
    pri-utility-addr              
    sec-utility-addr              
    netmask                       255.255.255.224
    gateway                       12.40.234.1
    sec-gateway                   
    gw-heartbeat                  
        state                     disabled
        heartbeat                  0
        retry-count                0
        retry-timeout              1
        health-score               0
    dns-ip-primary                
    dns-ip-backup1                
    dns-ip-backup2                
    dns-domain                    
    dns-timeout                   11
    hip-ip-list                    12.40.234.2
    ftp-address                   
    icmp-address                  12.40.234.2
    snmp-address                  
    telnet-address                
    ssh-address                   

ANOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

```
network-interface
    name                           enterprise
    sub-port-id                    0
    description                   
    hostname                      
    ip-address                    172.16.6.1
    pri-utility-addr              
    sec-utility-addr              
    netmask                       255.255.255.0
    gateway                       <Enter IP gateway here>
    sec-gateway                   
    gw-heartbeat                  
        state                     disabled
        heartbeat                  0
        retry-count                0
        retry-timeout              1
        health-score               0
    dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
  hip-ip-list 172.16.6.1
ftp-address
  icmp-address 172.16.6.1
snmp-address
telnet-address
ssh-address

phy-interface
  name enterprise
  operation-type Media
  port 0
  slot 0
  virtual-mac
  admin-state enabled
  auto-negotiation disabled
  duplex-mode FULL
  speed 100
  overload-protection disabled

phy-interface
  name peer
  operation-type Media
  port 1
  slot 0
  virtual-mac
  admin-state enabled
  auto-negotiation enabled
  duplex-mode FULL
  speed 100
  overload-protection disabled

realm-config
  identifier peer
  description
  addr-prefix 0.0.0.0
  network-interfaces
    peer:0
    mm-in-realm enabled
    mm-in-network enabled
    mm-same-ip enabled
    mm-in-system enabled
    bw-cac-non-mm disabled
    msm-release disabled
    generate-UDP-checksum disabled
    max-bandwidth 0
    fallback-bandwidth 0
    max-priority-bandwidth 0

ANNOTATION: The realm configuration “peer” below represents the external network on which the AT&T IP Flexible Reach service resides.
max-latency: 0
max-jitter: 0
max-packet-loss: 0
observe-window-size: 0
parent-realm
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit: 0
access-control-trust-level: none
invalid-signal-threshold: 0
maximum-signal-threshold: 0
untrusted-signal-threshold: 0
nat-trust-threshold: 0
deny-period: 30
ext-policy-svr
diam-e2-address-realm
symmetric-latching: disabled
pai-strip: disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching: none
restriction-mask: 32
accounting-enable: enabled
user-cac-mode: none
user-cac-bandwidth: 0
user-cac-sessions: 0
icmp.detect-multiplier: 0
icmp.advertisement-interval: 0
icmp.target-ip
monthly-minutes: 0
net-management-control: disabled
delay-media-update: disabled
refer-call-transfer: disabled
dyn-refer-term: disabled
codec-policy
codec-manip.in-realm: disabled
constraint-name
call-recording-server-id
xnq-state: xnq-unknown
hairpin-id: 0
stun-enable: disabled
stun-server-ip: 0.0.0.0
stun-server-port: 3478
stun.changed-ip: 0.0.0.0
stun.changed-port: 3479
match-media-profiles
qos-constraint
sip-profile
disabled
sip-isup-profile
block-rtcp
disabled
hide-egress-media-update
disabled

**ANNOTATION**: The realm configuration “enterprise” below represents the internal network on which the Avaya elements reside.

```plaintext
dns-realm
media-policy
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit
access-control-trust-level
invalid-signal-threshold
maximum-signal-threshold
untrusted-signal-threshold
nat-trust-threshold
deny-period
enforcement-profile
```
additional-prefixes
restricted-latching none
restriction-mask 32
accounting-enable enabled
user-cac-mode none
user-cac-bandwidth 0
user-cac-sessions 0
icmp-detect-multiplier 0
icmp-advertisement-interval 0
icmp-target-ip
monthly-minutes 0
net-management-control disabled
delay-media-update disabled
refer-call-transfer disabled
dyn-refer-term disabled
codec-policy
codec-manip-in-realm disabled
constraint-name
call-recording-server-id
xnq-state xnq-unknown
hairpin-id 0
stun-enable disabled
stun-server-ip 0.0.0.0
stun-server-port 3478
stun-changed-ip 0.0.0.0
stun-changed-port 3479
match-media-profiles
gos-constraint
sip-profile
sip-isup-profile
block-rtcp disabled
hide-egress-media-update disabled

ANNOTATION: The session agent below represents the AT&T IP Flexible Reach service border element. The AT&T IP Flexible Reach service border element is also specified in the session-group section below.

session-agent
hostname 207.242.225.210
ip-address
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id peer
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate               0
max-inbound-burst-rate       0
max-outbound-burst-rate      0
max-sustain-rate             0
max-inbound-sustain-rate     0
max-outbound-sustain-rate    0
min-seizures                 5
min-asr                      0
time-to-resume               0
ttr-no-response              0
in-service-period            0
burst-rate-window            0
sustain-rate-window          0
req-uri-carrier-mode         None
proxy-mode                   
redirect-action              
loose-routing                enabled
send-media-session           enabled
response-map                 
ping-method                  
ping-interval                0
ping-send-mode               keep-alive
ping-all-addresses           disabled
ping-in-service-response-codes
out-service-response-codes   
media-profiles               
in-translationid             
out-translationid            
trust-me                     disabled
request-uri-headers         
stop-recurse                 
local-response-map           
ping-to-user-part            
ping-from-user-part          
l1-trust-me                  disabled
in-manipulationid            
out-manipulationid           
manipulation-string          
manipulation-pattern         
p-asserted-id                
trunk-group                  
max-register-sustain-rate    0
early-media-allow            
invalidate-registrations     disabled
rfc2833-mode                 none
rfc2833-payload              0
codec-policy                 
enforcement-profile          
refer-call-transfer          disabled
reuse-connections            NONE
tcp-keepalive                none
tcp-reconn-interval          0
max-register-burst-rate      0
register-burst-window        0
sip-profile                  
sip-isup-profile             

Reviewed: 4/12/2011
CS 1000 Application Notes 39 of 63
CS1000R7_AcmeR620_IPFR 18-603958
**ANNOTATION:** The session agent below represents the Communication Server 1000 Node used in the reference configuration.

```
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-agent</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>172.16.6.110</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>5060</td>
</tr>
<tr>
<td>state</td>
<td>enabled</td>
</tr>
<tr>
<td>app-protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>app-type</td>
<td></td>
</tr>
<tr>
<td>transport-method</td>
<td>UDP</td>
</tr>
<tr>
<td>realm-id</td>
<td>enterprise</td>
</tr>
<tr>
<td>egress-realm-id</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td></td>
</tr>
<tr>
<td>carriers</td>
<td></td>
</tr>
<tr>
<td>allow-next-hop-lp</td>
<td>enabled</td>
</tr>
<tr>
<td>constraints</td>
<td>disabled</td>
</tr>
<tr>
<td>max-sessions</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-sessions</td>
<td>0</td>
</tr>
<tr>
<td>max-outbound-sessions</td>
<td>0</td>
</tr>
<tr>
<td>max-burst-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-burst-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-outbound-burst-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-outbound-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>min-seizures</td>
<td>5</td>
</tr>
<tr>
<td>min-asr</td>
<td>0</td>
</tr>
<tr>
<td>time-to-resume</td>
<td>0</td>
</tr>
<tr>
<td>ttr-no-response</td>
<td>0</td>
</tr>
<tr>
<td>in-service-period</td>
<td>0</td>
</tr>
<tr>
<td>burst-rate-window</td>
<td>0</td>
</tr>
<tr>
<td>sustain-rate-window</td>
<td>0</td>
</tr>
<tr>
<td>req-uri-carrier-mode</td>
<td>None</td>
</tr>
<tr>
<td>proxy-mode</td>
<td></td>
</tr>
<tr>
<td>redirect-action</td>
<td>enabled</td>
</tr>
<tr>
<td>loose-routing</td>
<td>enabled</td>
</tr>
<tr>
<td>send-media-session</td>
<td>enabled</td>
</tr>
<tr>
<td>response-map</td>
<td></td>
</tr>
<tr>
<td>ping-method</td>
<td></td>
</tr>
<tr>
<td>ping-interval</td>
<td>0</td>
</tr>
<tr>
<td>ping-send-mode</td>
<td>keep-alive</td>
</tr>
<tr>
<td>ping-all-addresses</td>
<td>disabled</td>
</tr>
<tr>
<td>ping-in-service-response-codes</td>
<td></td>
</tr>
<tr>
<td>out-service-response-codes</td>
<td></td>
</tr>
<tr>
<td>media-profiles</td>
<td></td>
</tr>
<tr>
<td>in-translationid</td>
<td></td>
</tr>
<tr>
<td>out-translationid</td>
<td></td>
</tr>
<tr>
<td>trust-me</td>
<td>disabled</td>
</tr>
<tr>
<td>request-uri-headers</td>
<td></td>
</tr>
<tr>
<td>stop-recurse</td>
<td></td>
</tr>
<tr>
<td>local-response-map</td>
<td></td>
</tr>
<tr>
<td>ping-to-user-part</td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping-from-user-part</td>
<td></td>
</tr>
<tr>
<td>li-trust-me</td>
<td>disabled</td>
</tr>
<tr>
<td>in-manipulationid</td>
<td></td>
</tr>
<tr>
<td>out-manipulationid</td>
<td></td>
</tr>
<tr>
<td>manipulation-string</td>
<td></td>
</tr>
<tr>
<td>manipulation-pattern</td>
<td></td>
</tr>
<tr>
<td>p-asserted-id</td>
<td></td>
</tr>
<tr>
<td>trunk-group</td>
<td></td>
</tr>
<tr>
<td>max-register-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>early-media-allow</td>
<td></td>
</tr>
<tr>
<td>invalidate-registrations</td>
<td>disabled</td>
</tr>
<tr>
<td>rfc2833-mode</td>
<td>none</td>
</tr>
<tr>
<td>rfc2833-payload</td>
<td>0</td>
</tr>
<tr>
<td>codec-policy</td>
<td></td>
</tr>
<tr>
<td>enforcement-profile</td>
<td></td>
</tr>
<tr>
<td>refer-call-transfer</td>
<td>disabled</td>
</tr>
<tr>
<td>reuse-connections</td>
<td>NONE</td>
</tr>
<tr>
<td>tcp-keepalive</td>
<td>none</td>
</tr>
<tr>
<td>tcp-reconn-interval</td>
<td>0</td>
</tr>
<tr>
<td>max-register-burst-rate</td>
<td>0</td>
</tr>
<tr>
<td>register-burst-window</td>
<td>0</td>
</tr>
<tr>
<td>sip-profile</td>
<td></td>
</tr>
<tr>
<td>sip-isup-profile</td>
<td></td>
</tr>
</tbody>
</table>

**ANNOTATION:** The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
  state                                        enabled
  operation-mode                              dialog
  dialog-transparency                          enabled
  home-realm-id                               enabled
  egress-realm-id                             enterprise
    nat-mode                                   Public
    registrar-domain                         
    registrar-host                            0
    register-service-route                     always
    init-timer                                 500
    max-timer                                  4000
    trans-expire                               32
    invite-expire                              180
    inactive-dynamic-conn                      32
    enforcement-profile                        
    pac-method                                 
    pac-interval                               10
    pac-strategy                               PropDist
    pac-load-weight                            1
    pac-session-weight                         1
    pac-route-weight                           1
    pac-callid-lifetime                         600
    pac-user-lifetime                          3600
    red-sip-port                               1988
```
red-max-trans                  10000
red-sync-start-time            5000
red-sync-comp-time             1000
add-reason-header              disabled
sip-message-len                4096
enum-sag-match                 disabled
extra-method-stats             disabled
rph-feature                    disabled
nsep-user-sessions-rate        0
nsep-sa-sessions-rate          0
registration-cache-limit       0
register-use-to-for-lp         disabled
**options**
  add-prov-to-tag=no
  insert-arp-header
  max-udp-length=0
  set-inv-exp-at-100-resp
  refer-src-routing              disabled
  add-ucid-header                disabled
  proxy-sub-events               disabled
  pass-gruu-contact              disabled
  sag-lookup-on-redirect         disabled
  set-disconnect-time-on-bye     disabled

**ANNOTATION**: The SIP interface below is used by the Acme Packet 3800 to communicate with Communication Server 1000. This SIP interface uses the **Privacy** sip-manipulation.

```
sip-interface
  state enabled
  realm-id enterprise
description
sip-port
  address 172.16.6.1
  port 5060
  transport-protocol UDP
tls-profile
  allow-anonymous all
  ims-aka-profile
  carriers
  trans-expire 0
  invite-expire 0
  max-redirect-contacts 0
  proxy-mode
  redirect-action
  contact-mode none
  nat-traversal none
  nat-interval 30
  tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 3600
route-to-registrar disabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
```
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid             Privacy
manipulation-string
manipulation-pattern
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
sip-profile
sip-isup-profile

ANNOTATION: The SIP interface below is used by the Acme Packet SBC to communicate with the AT&T IP Flexible Reach service. This SIP interface uses the public sip-manipulation and transparent for rfc2833-mode.

sip-interface
state                     enabled
realm-id                  peer
description
sip-port
  address                  12.40.234.2
  port                     5060
  transport-protocol      UDP

Reviewed: 4/12/2011
CS 1000 Application Notes
©2011 Avaya Inc. All Rights Reserved.
18-603958
CS1000R7_AcmeR620_IPFR
tls-profile

allow-anonymous all

ims-aka-profile

carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode none
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 3600
route-to-registrar disabled
secured-network disabled
teluri-scheme disabled
uri-fqdn-domain
trust-mode all
max-nat-interval 3600
nat-int-increment 10
nat-test-increment 30
sip-dynamic-hnt disabled
stop-recurse 401,407
port-map-start 0
port-map-end 0
in-manipulationid
out-manipulationid public

manipulation-string
manipulation-pattern
sip-ims-feature disabled
operator-identifier
anonymous-priority none
max-incoming-conns 0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout 0
untrusted-conn-timeout 0
network-id
ext-policy-server
default-location-string
charging-vector-mode pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile

**ANNOTATION:** The following sip-manipulation Privacy is applied to enterprise realm out-manipulationid. These rules perform the following:

- The header rules From_Header and To_Header perform address translation and topology hiding for SIP messages between the AT&T IP Flexible Reach services and the Avaya elements.

- The header rules delXNTMCDN, delXNTEPID, and xnt remove Nortel-specific SIP headers and convert the multi-part MIME MCDN information into a single SDP body.

- The header rules HistRegex, AddDiversion, and delHist extract the information from the History-Info SIP header from the Communication Server 1000, add a Diversion header using the information in the History-Info header, and delete the History-Info header.

- The header rules addPtime, ModSDP, and delMaxP remove the maxptime attribute in the SDP and add a ptime attribute with the desired voice payload size (20 or 30).

- The header rules ruri and uinfo_touri extracts user information from the Request-URI and replaces the user information from the To header with the extracted information.

```
sip-manipulation  
name              Privacy
                        description
split-headers
join-headers
header-rule
name                  PAI_Header
header-name           passer
action                delete
comparison-type       case-sensitive
msg-type              any
methods
match-value
new-value
header-rule
name                  PPI_Header
header-name           P-Preferred-Identity
action                manipulate
comparison-type       case-sensitive
msg-type              any
methods
match-value
new-value
element-rule
name                  PPI_Local_IP
```
parameter-name
type uri-host
action replace
match-val-type any
comparison-type case-sensitive
match-value
new-value

debug-rule
name From_Header
debug-name From
action manipulate
debug-type request
debug-methods
debug-match-value
debug-new-value

debug-rule
name To_Header
debug-name To
action manipulate
debug-type request
debug-methods
debug-match-value
debug-new-value

debug-rule
name RPI_Header
debug-name Remote-Party-ID
action manipulate
debug-type case-sensitive
debug-methods
debug-match-value
debug-new-value

debug-rule
name RPI_header
debug-name Remote-Party-ID
action manipulate
debug-type case-sensitive
debug-methods
debug-match-value
debug-new-value
action                         replace
match-val-type                 any
comparison-type                case-sensitive
match-value
new-value
$header-rule$
name                           Refer_header
header-name                    Referred-By
action                         manipulate
comparison-type                case-sensitive
msg-type                       any
methods
match-value
new-value
$element-rule$
name                           referredbyhdr
parameter-name
action                         replace
match-val-type                 any
comparison-type                case-sensitive
match-value
new-value
$REMOTE_IP$
$mime-rule$
name                           delXNMTCDN
content-type                   application/x-nt-mcdn-frag-hex
action                         delete
comparison-type                case-sensitive
msg-type                       request
methods                        INVITE
format                         ascii-string
match-value
new-value
$mime-rule$
name                           delXNTEPID
content-type                   application/x-nt-epid-frag-hex
action                         delete
comparison-type                case-sensitive
msg-type: request
methods: INVITE
format: ascii-string

header-rule
name: xnt
header-name: x-nt-e164-clid
type: xnt
action: delete
comparison-type: case-sensitive

header-rule
name:HistRegex
header-name: History-Info
type: HistRegex
action: store
comparison-type: pattern-rule
methods: INVITE
match-value:
new-value:

element-rule
name: GetUser
parameter-name: type
name: GetUser
parameter-name: action
name: GetUser
parameter-name: match-val-type
name: GetUser
parameter-name: comparison-type
match-value: $HistRegex
new-value: <sip:+$HistRegex[0].$GetUser.$0+@$HistRegex[0].$GetHost.$0>;privacy=off;reason=unconditional;screen=no

header-rule
name: AddDiversion
header-name: Diversion
action: add
comparison-type: boolean
methods: INVITE
match-value: $HistRegex
new-value:

header-rule
name: delHist
header-name: History-Info
action: delete
comparison-type                case-sensitive
msg-type                       any
methods
match-value
new-value

header-rule
name                           addPtime
header-name                    Content-Type
action                         store
comparison-type                case-sensitive
msg-type                       any
methods
match-value
new-value

element-rule
name                           checkSdp
parameter-name                 application/sdp
type                           mime
action                         store
match-val-type                 any
comparison-type                pattern-rule
match-value

9\{1,2\}(\n|\r\n)

new-value

header-rule
name                           ModSDP
header-name                    Content-Type
action                         manipulate
comparison-type                boolean
msg-type                       any
methods
match-value
new-value

element-rule
name                           modSdp1
parameter-name                 application/sdp
type                           mime
action                         find-replace-all
match-val-type                 any
comparison-type                pattern-rule
match-value
new-value
$a=addPtime.$checkSdp
\Rm=audio.*\R()\[[1:\]]
a=ptime:30+$CRLF

ANNOTATION: A Communication Server 1000 voice payload size of 30ms is used here. If 20ms is desired, modify the string to 20.
new-value
element-rule
  name
delMaxptime
  parameter-name
application/sdp
  type
mime
  action
find-replace-all
  match-val-type
any
  comparison-type
pattern-rule
  match-value
 Ra=maxptime:.*
new-value

header-rule
  name
ruri
  header-name
request-uri
  action
store
  comparison-type
pattern-rule
  msg-type
any
  methods

header-rule
  name
uinfo
  header-name
uri-user
  action
store
  match-val-type
any
  comparison-type
pattern-rule
  match-value
.
new-value

header-rule
  name
uinfo_touri
  header-name
To
  action
manipulate
  comparison-type
case-sensitive
  msg-type
request
  methods
INVITE
  match-value

header-rule
  name
to_uinfo
  parameter-name
uri-user
  action
replace
  match-val-type
any
  comparison-type
case-sensitive
  match-value
new-value
$ruri.$uinfo.$0

header-rule
  name
to_uhost
  parameter-name
uri-host
  action
replace
  match-val-type
any
  comparison-type
case-sensitive
  match-value
new-value
$REMOTE_IP
ANNOTATION: The following header rules are used for the CS 1000 Mobile Extension (Mobile-X) Call in Progress features, where the incoming RFC2833 digits are converted to SIP INFO messages with specific CS 1000 headers and attributes.

These header rules are only needed if CS 1000 Mobile Extension Call in Progress features are required.

```plaintext
header-rule
  name                           manNT
  header-name                    Content-Type
  action                         find-replace-all
  comparison-type                case-sensitive
  msg-type                       request
  methods                        INFO
  match-value                    application/dtmf-relay
  new-value                      "application/vnd.nortelnetworks.digits"

header-rule
  name                           storeSignal
  header-name                    content-type
  action                         store
  comparison-type                pattern-rule
  msg-type                       any
  methods                        INFO
  match-value
  new-value
  element-rule
    name                           storeSig
    parameter-name                application/vnd.nortelnetworks.digits
    type                           mime
    action                        store
    match-val-type                any
    comparison-type               pattern-rule
    match-value                   (Signal=)(.*)
    new-value

header-rule
  name                           changeContent
  header-name                    content-type
  action                         manipulate
  comparison-type                pattern-rule
  msg-type                       any
  methods                        INFO
  match-value
  new-value
  element-rule
    name                           changeContent
    parameter-name                *
    type                           mime
    action                        replace
    match-val-type                any
    comparison-type               pattern-rule
    match-value                   
    new-value                     d=n+$storeSignal.$storeSig.$2
```
ANNOTATION: The following sip-manipulation public is applied to peer realm out-manipulationid. These rules perform the following:

- The header rule From_Header modifies the From header IP address from the AT&T BE’s IP address to the SBC’s inside interface IP address.
- The header rule To_Header modifies the To header IP address from the SBC’s outside IP address to the Communication Server 1000’s Node IP address.
- The header rules delXNTMCDN, delXNTEPID, and xnt remove Nortel-specific SIP headers and convert the multi-part MIME MCDN information into a single SDP body.
- The header rules HistRegex, addDiversion, delHist, and Diversion_Header extract information from the History-Info header, add the information to the P-Asserted-Identity and Diversion headers, and delete History-Info header. It also determines when to add Diversion header for call forward scenarios.
- The header rule PAI_header modifies the IP address in the P-Asserted-Identity header from the SBC’s private interface address to public interface address.
new-value
element-rule
  name                           From_header
  parameter-name                 
  type                           uri-host
  action                         replace
  match-val-type                 any
  comparison-type                case-sensitive
  match-value
  new-value                      $LOCAL_IP
header-rule
  name                           To_Header
  header-name                    To
  action                         manipulate
  comparison-type                case-sensitive
  msg-type                       request
  methods
  match-value
  new-value
element-rule
  name                           To_header
  parameter-name                 
  type                           uri-host
  action                         replace
  match-val-type                 any
  comparison-type                case-sensitive
  match-value
  new-value                      $REMOTE_IP
header-rule
  name                           RPI_Header
  header-name                    Remote-Party-ID
  action                         manipulate
  comparison-type                case-sensitive
  msg-type                       any
  methods
  match-value
  new-value
element-rule
  name                           RPI_header
  parameter-name                 
  type                           uri-host
  action                         replace
  match-val-type                 any
  comparison-type                case-sensitive
  match-value
  new-value                      $LOCAL_IP
header-rule
  name                           Refer_header
  header-name                    Referred-By
  action                         manipulate
  comparison-type                case-sensitive
  msg-type                       any
  methods
  match-value
  new-value
name                           referredbyhdr
parameter-name                 
action                         replace
match-val-type                 any
comparison-type                case-sensitive
match-value
new-value
$LOCAL_IP

header-rule
name                           Referto
header-name                    Refer-To
action                         manipulate
comparison-type                case-sensitive
msg-type
methods
match-value
new-value

mime-rule
name                           delXNTMCDN
content-type                   application/x-nt-mcdn-frag-hex
action                         delete
comparison-type                case-sensitive
msg-type
methods
format                         ascii-string
new-value

mime-rule
name                           delXNTEPID
content-type                   application/x-nt-epid-frag-hex
action                         delete
comparison-type                case-sensitive
msg-type
methods
format                         ascii-string
new-value

header-rule
name                           xnt
header-name                    x-nt-e164-clid
action                         delete
comparison-type                case-sensitive
msg-type
methods
match-value
new-value

header-rule
name                           HistRegex
header-name                    History-Info
action                         store
comparison-type                pattern-rule
msg-type                       request
methods
match-value
new-value

**element-rule**

name                           isREASON
parameter-name

**header-rule**

name                           addDiversion
header-name                    Diversion
action                         add
comparison-type                boolean
msg-type                       request
methods
match-value
new-value

**element-rule**

name                           getUser
parameter-name

**header-rule**

name                           delhist
header-name                    History-Info
action                         delete
comparison-type                case-sensitive
msg-type                       request
methods
match-value
new-value

**header-rule**

name                           PAI_header
header-name                    P-Asserted-Identity
action                         manipulate
comparison-type                case-sensitive
msg-type                       any
methods
match-value
new-value
**ANNOTATION**: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The “peer” realm IP Address will be used as the CPE media traffic IP Address to communicate with AT&T. **The “peer” realm RTP port range is an AT&T IP Flexible Reach service requirement.** Likewise, the IP Address and RTP port range defined for the “enterprise” realm steering pool will be used to communicate with the Avaya elements.

```yaml
steering-pool
  ip-address  172.16.6.1
  start-port   16384
  end-port    32767
  realm-id     enterprise
  network-interface

steering-pool
  ip-address  12.40.234.2
  start-port   16384
  end-port    32767
  realm-id     peer
  network-interface
```

```yaml
system-config
  hostname
  description
  location
  mib-system-contact
```

mib-system-name
mib-system-location
snmp-enabled enabled
enable-snmp-auth-traps disabled
enable-snmp-syslog-notify disabled
enable-snmp-monitor-traps disabled
enable-env-monitor-traps disabled
snmp-syslog-his-table-length 1
snmp-syslog-level WARNING
system-log-level WARNING
syslog-server
  address 10.10.10.85
  port 514
  facility 5
process-log-level NOTICE
process-log-ip-address 0.0.0.0
process-log-port 0
collect
  sample-interval 5
  push-interval 15
  boot-state disabled
  start-time now
  end-time never
  red-collect-state disabled
  red-max-trans 1000
  red-sync-start-time 5000
  red-sync-comp-time 1000
  push-success-trap-state disabled
  call-trace disabled
  internal-trace disabled
  log-filter all
  default-gateway 12.40.234.1
  restart enabled
exceptions
  telnet-timeout 0
  console-timeout 0
  remote-control enabled
  cli-audit-trail enabled
  link-redundancy-state disabled
  source-routing enabled
  cli-more disabled
  terminal-height 24
  debug-timeout 0
  trap-event-lifetime 0
  default-v6-gateway ::
  ipv6-support disabled
  cleanup-time-of-day 00:00
**Basic Monitoring and Call Tracing on CS 1000**

The following procedures below can be used to monitor and trace calls on the CS 1000. The CS 1000 has an extensive suite of diagnostic procedures and is out of the scope of this document. For more information on advanced diagnostics, please refer to the Nortel CS 1000 Release 5 Technical Documentation.

**Viewing Registered Sets on CS 1000**

The following Call Server CLI command in **LD 96** can be used to display registered IP sets based on the node, SS, or phone model:

```
=> ecnt node
Node: 1001
   Number of Registered Ethersets  : 5
```

```
=> ecnt ss
Signaling Server: SS_1001  IP: 192.12.0.10
   Number of Registered Ethersets  : 5
```

```
=> ecnt modl
2004P2: IP Phone 2004 Phase 2
   Number of IP phones:  2
   Number of IP phones:  3
```

**Active Call Information**

Administrators can view active call information for the specific DN while on a call. Go to **LD 80** in the Call Server CLI and enter the following command: `trac <customer #> <DN>`.

Information such as IP addresses, codecs, calling/called party numbers, etc. is displayed:

```
.trac 0 2001
ACTIVE  VTN 096 0 01 01
ORIG   VTN 096 1 02 00  VTRK IPTI  RMBR  16 1 INCOMING VOIP GW CALL
   FAR-END SIP SIGNALLING IP: 135.25.29.135
   FAR-END MEDIA ENDPOINT IP: 135.25.29.70  PORT: 16390
   FAR-END VendorID: Cisco-SIPGateway/IOS-12.x
TERM   VTN 096 0 01 01  KEY 0  SCR MARP CUST 0  DN 2001  TYPE 1140
   MEDIA ENDPOINT IP: 172.16.6.101  PORT: 28802
   MEDIA PROFILE: CODEC G.729 NO-LAW PAYLOAD 20 ms VAD ON
RFC2833:  RXPT  96  TXPT  96  DIAL DN 2001
MAIN PM  ESTD
TALKSLOT  ORIG  66  TERM  2
EES_DATA:
```

---

Reviewed: 4/12/2011
CS 1000 Application Notes
©2011 Avaya Inc. All Rights Reserved.
18-603958
CS1000R7_AcmeR620_IPFR
SIP Call Tracing

When a call is being placed to/from the CS 1000, the SIP messages can be outputted to the screen when logged into the Signaling Server CLI. The SIPCallTrace command can be turned on to view the SIP messages. The SIPTraceLevel command can be set to either 0 or 1; 0 for less-detailed output, 1 for more details.

```
NOTE
It is strongly recommended that this command be left off during normal operations; the command to disable is as follows:
SIPCallTrace off.
```

Below is a sample output:

```
oam> SIPTraceLevel 1
oam> SIPCallTrace on
oam>
oam> 02/10/2007 16:48:13 LOG0003 SIPNPM: sipNpmPrivacyHdrBuild: : PATCH - Privacy Value was equal to NONE, so header not added PATCH
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace: This is Outgoing Message
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace:
From: "Al Chee"<sip:7323680430@172.16.6.110;user=phone>
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace:
To: <sip:17324208823@135.25.29.135:135.25.29.135;user=phone>
User-Agent: Nortel CS1000 SIP GW release_5.0 version_sse-5.00.31
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace:

02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace: This is Incoming Message
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace:
Message: Incoming response 302 Moved Temporarily chid: 27 Called num: 17324208822
3 Far End Signaling IP: 135.25.29.135:65535 Transport:UDP CSeq: 1 INVITE
From: "Al Chee"<sip:7323680430@172.16.6.110;user=phone>
02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace:
To: <sip:17324208823@135.25.29.135:135.25.29.135;user=phone>
Contact: <sip:17324208823@135.25.29.135:135.25.29.135;user=phone>

02/10/2007 16:48:13 LOG0006 SIPNPM: SIPCallTrace: This is Outgoing Message
```
Packet Capture Tools

There are a few ways to take network packet captures on the CS 1000 (but not limited to):

- PCAP command (CLI)
- PCAP Tool for Signaling Server

For more information on using these tools, please refer to the CS 1000 Technical Documentation.

NOTE: Depending on the network architecture, not all IP packets will be captured by this tool, i.e. RTP packets from the IP sets.
### Appendix A: Table of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM/WLC</td>
<td>Analog Message Waiting Line Card: provides talk battery and signaling for regular 2-wire common battery 500-type (rotary dial) and 2500-type (Digitone dial) telephones and key telephone equipment. This card also supports message waiting indication for sets equipped with the message waiting feature.</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf: standard server hardware manufactured by a third-party; the CS 1000 supports the following COTS servers – IBM xSeries 306m (types 8848, 8491) and HP ProLiant DL320 G4 servers.</td>
</tr>
<tr>
<td>CP-PIV</td>
<td>Common Process Pentium IV: processor for the Call/Signaling Server on a legacy large system (CS 1000M), is also supported on CS 1000E systems.</td>
</tr>
<tr>
<td>CP-PM</td>
<td>Common Processor Pentium Mobile: the main processor for the Call Server, controlling all call processing and telephony services. It also provides the system memory required to store operating software and customer data. This is the default processor for the CS 1000E. Note: the Signaling Server can also be a CP-PM card.</td>
</tr>
<tr>
<td>CS 1000</td>
<td>Communications Server 1000</td>
</tr>
<tr>
<td>DLC</td>
<td>Digital Line Card: provides a multiplexed voice, data, and signaling path to and from a digital terminal (telephone) over a 2-wire full duplex 512 kHz Time Compression Multiplexed (TCM) digital link.</td>
</tr>
<tr>
<td>ISP 1100</td>
<td>Legacy Nortel Signaling Server running VxWorks real-time operating system. In order for compatibility with Release 5.0, the ISP 1100 must contain at least 1 GB of memory.</td>
</tr>
<tr>
<td>MCDN</td>
<td>Meridian Customer Defined Network: private voice networking functionalities/features in a Nortel IP PBX environment</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-------------</td>
</tr>
<tr>
<td>MGC</td>
<td>Media Gateway Controller: provides Digital Signaling Processor (DSP) resources for connecting IP and Time Division Multiplexing (TDM) devices together and for advanced applications such as conferences and voicemail access</td>
</tr>
<tr>
<td>MIRAN</td>
<td>Meridian Integrated Recorded Announcer card provides multi-tasking, voice-processing applications, such as Recorded Announcement (RAN) and Music-On-Hold (MOH)</td>
</tr>
<tr>
<td>TLAN</td>
<td>Telephony Local Area Network: network interfacing with AT&amp;T IP Flexible Reach service</td>
</tr>
<tr>
<td>TMDI</td>
<td>PRI circuit card to interface with PSTN (if needed)</td>
</tr>
</tbody>
</table>