Meeting Exchange 5.0 Service Pack 2 Configuration Guide for the S6X00 Servers

04-603321
Issue 1
March 2009

Contents

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this Documentation unless such modifications, additions, or deletions were performed by Avaya.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked third party Web sites referenced elsewhere within this Documentation and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). Customer may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

For full information, please see the complete document, Avaya Third Party Terms, Document number 04-601558. To locate this document on the website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-

3-2353 for the United States and Canada. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Trademarks

Avaya and the Avaya logo are registered trademarks of Avaya Inc. in the United States of America and other jurisdictions. Unless otherwise provided in this Documentation, marks identified by "®," "™" and "SM" are registered marks, trademarks and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support

Chapter 1: Overview

Product

The Avaya S6200/S6800 Conferencing Servers provide a highly scalable, highly configurable, audio conferencing facility. The S6x00 media servers are SIP-based voice and web conferencing solutions that extend Avaya's teleconferencing applications, including reservation-less, attended, event, mobile, and web conferencing, to support IP network implementations. This solution offers a flexible, comprehensive conferencing solution in a pure IP environment.

Scope

This document describes only the software configuration of the S6200/S6800 Conferencing Servers and associated CRS and application servers. After the equipment is installed and connected to the LAN and network, the servers are configured by Avaya Support using LAN or modem connections.

Tip:

For information on configuring the server with the Electronic Preinstallation Worksheet (EPW) available from Avaya, see: Electronic Preinstallation Worksheet (EPW) on page 22

Audience

This document is intended for authorized Avaya personnel who install software and configure the S6200/S6800 Conferencing Servers. It includes instructions for setting up and configuring factory-installed hardware and system software and enabling system features. It also includes additional information for troubleshooting and maintaining the system.

This document is not intended for customer use. Most of the procedures described in this document require root level or administrator level access. The account names and passwords are not provided to the customer for security reasons.

Users of this guide should have basic knowledge of Linux shell commands and resources, Windows® 2003 Server Edition network setup, and S6200/S6800 Conferencing Servers features.

Conventions

This guide uses the following conventions:

Convention	Description
`System`	Used for text the Linux system displays, including script text. For example: `This installation may be used to install the Easysoft ODBC-ODBC Bridge.`
`System Bold`	Used for text you enter at the Linux command line and in response to script prompts. For example: **`pkgadd -d /patch/ptf7401c`**
Bold	Used to highlight keyboard commands, screen, menu, menu option, and screen option references, for emphasizing other terms where required. For example: Press **Enter** to select **Default (all packages)**.
Italic	Used for references to publications. For example: See the *Meeting Exchange® 4.1 Administration and Maintenance Guide for the S*S6200/ S6800 Conferencing Servers.
“Double Quotes”	Used for references to sections in this manual. For example: See “Chapter 1: Overview” for more information.
Vertical Slash (|)	Used to indicate the navigational path to an option. For example: Select **Host** | **Exit** means select the Exit option from the Host menu or option.

Note:

Provides additional information

⚠ **Important:**

Provides information of special importance.

⚠ **CAUTION:**

Provides information about actions that may corrupt system resources or processes.

⚠ **WARNING:**

Provides information relating to personal safety.

Related Documentation

Refer to the latest revisions of these Avaya documents for additional information.

- *Meeting Exchange® 5.0 Installing the S6200/S6800 Conferencing Servers.*
- *Meeting Exchange® 5.0 Administration and Maintenance Guide for the* S6200/S6800 Conferencing Servers. Describes how to use the system's management interface to configure system, conference, and network settings. It also describes how to use the system's file management utilities.
- *Meeting Exchange® 5.0 Relational Database Guide.*
- *Meeting Exchange® 5.0 Release Notes for the* S6200/S6800 Conferencing Servers*.* Describes known bugs for this release and bugs fixed from the previous release.

Refer to the latest revisions of these Dell documents for additional information about the Dell PowerEdge 1950 System:

- *Dell™ PowerEdge™ 1950 Systems Hardware Owner's Manual*
- Dell™ *Rack Installation Guide*
- *Dell™ PowerEdge™ 1950 Systems - Getting Started with Your System* - P/N Y C585

Refer to the latest revisions of these Convedia documents for additional information about the CMS-6000 media servers:

- *CMS-6000 Media Server Installation and Operations Manual*

Refer to the latest revision of these AudioCodes documents for additional information about the Gateway server:

- *AudioCodes Mediant 2000 SIP User's Manual -* Document #: LTRT-68805
- *AudioCodes Mediant 3000 SIP User's Manual -* Document #: LTRT-89701

Refer to the following document for information on the Conference Scheduler Plug-in for Microsoft Outlook:

- *Avaya Meeting Exchange® 5.0 for Microsoft Applications Installation and Configuration Guide*

Refer to the following document for information on the Conference Scheduler Plug-in for IBM Lotus Notes:

- *Avaya Meeting Exchange® 5.0 for IBM Applications Installation and Configuration Guide*

S6200/S6800 Conferencing Servers Overview

The S6200/S6800 Conferencing Servers consists of the S6200 media server by itself for small systems, in a cluster for larger systems or combined with an external hardware media server for larger systems.

Table 1: Configurations for S6200/S6800 Conferencing Servers

	S6200	**S6200** **(separate app and media servers)**	**S6800** **Media** **Server**[a]
Application Server	S6200 (standalone with integrated Media Server)	S6200 -max of 6 1 app + failover 3 media + failover	S6200 (up to 4 application servers)- 3 primary and 1 standby)
Client Registration System[b]	available	available	suggested
Server Redundancy[c]	available[d]	available	Workgroup
Hardware Media Server[e]	not applicable	not applicable	CMS-6000
AudioCodes Media Gateway Servers **(optional for TDM support)**	Mediant 2000 (24 to 384 T1 ports per Mediant server)	Mediant 2000 (24 to 384 T1 ports per Mediant server)	Mediant 3000 (168 to 2016 T3 ports) per server
Ports	up to 2000 with a 1 gigabit network	up to 2000	up to 6000

[a] S6800 supports up to 12 MPC cards, 9 used as primary MPC and 3 used as backup MPC. Suppport up to 4 application servers, 3 used as primary and 1 for backup.

[b] Optional. Booking and scheduling is handled by the CRS and the reservations are pushed down to the bridge.

[c] Optional.

[d] For failover with a single server solution, each backup server provides failover for only one specific primary server. Conference participants must reconnect their lines in the event of a failover

[e] The system currently supports only the Convedia hardware media server models identified in this table.

There may be additional redundant servers, as well as other types of application (Client Registration/Web Portal/Web Conferencing) servers included in the system.

Important:

For a multiserver solution, the network must support a Gigabit Ethernet.

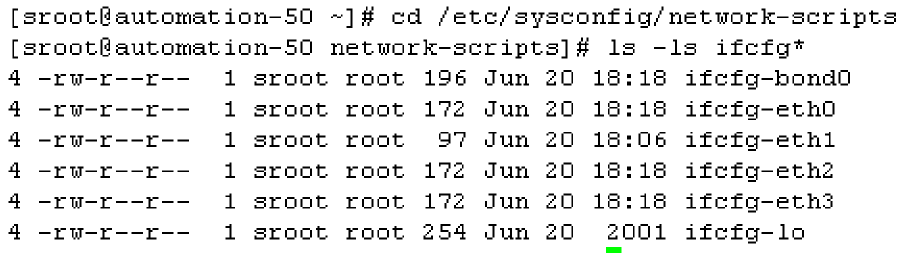
Gigabit Connections

For Application Servers connecting to a Gigabit switch,change the following configurations:

1. Go to the network-scripts directory:

   cd /etc/sysconfig/network-scripts

   ls -ls ifcfg*



```
[sroot@automation-50 ~]# cd /etc/sysconfig/network-scripts
[sroot@automation-50 network-scripts]# ls -ls ifcfg*
4 -rw-r--r--  1 sroot root 196 Jun 20 18:18 ifcfg-bond0
4 -rw-r--r--  1 sroot root 172 Jun 20 18:18 ifcfg-eth0
4 -rw-r--r--  1 sroot root  97 Jun 20 18:06 ifcfg-eth1
4 -rw-r--r--  1 sroot root 172 Jun 20 18:18 ifcfg-eth2
4 -rw-r--r--  1 sroot root 172 Jun 20 18:18 ifcfg-eth3
4 -rw-r--r--  1 sroot root 254 Jun 20  2001 ifcfg-lo
```

2. Edit the following the three configuration files, ifcfg-eth0, idcfg-eth2, ifcfg-eth3, as shown below to change the autoneg from Off to On and to set the speed from 100 to 1000. For each of the configuration files (eth0,eth2, eth3), edit the ETHTOOL_OPTS field as shown:

   ETHTOOL_OPTS="speed 1000 duplex full autoneg on".

   Tip:

   Do not connect a network cable on eth1

3. Verify that the network switch ports are also configured as above: gb, full duplex, autoneg on. This will ensure that the network will establish a gigabit link to the server.

4. Verify that the following is not added in the rc.local file:

   ethtool -s eth0 autoneg on

5. Reboot the server.

Failover Detection

Failover can be detected by setting the following parameters in mxMonitor.reg on page 63:

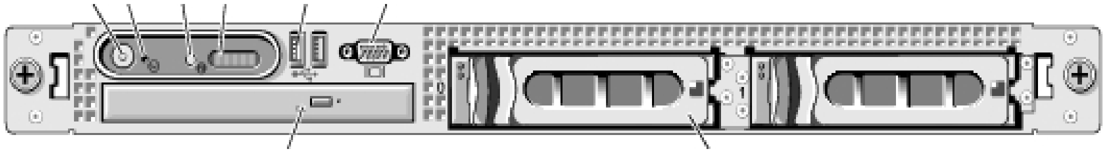
`checkstatustimer` (timer in milliseconds; default 60000)

`numstatusrequests` (number of times active server is checked in case of no-response; default is 2)

S6200 Media Server

The S6200 media server runs on a Linux host, the Dell™ PowerEdge™ 1950.

Figure 1: S6200 Media Server.



This solution provides the callhandler applications and the media resources required to support up to 600 ports in a standalone server, and up to 700 ports when configured with a separate application server.

The S6200 media server has these capabilities:

- 2000 ports of G.711 a-law or u-law

  Tip:

  2000 port single server solution requires a 1 gigabit network.

- RFC 2833 -DTMF support
- In-band DTMF support
- 70 operator conferences
- Up to 2000 participants in a single conference
- Full support of the media server interface
- Support for 1 recorded music channel, and up to 4 connection based (FDAPI) music channels

Convedia Hardware Media Servers

The hardware media server configuration works in conjunction with the S6200 software media server and supports any combination of G.711, G.722. G.726, G.729, and other codecs. This configuration offers the possibility of up to 2016 ports.

Other capabilities of the Hardware Media Servers are:

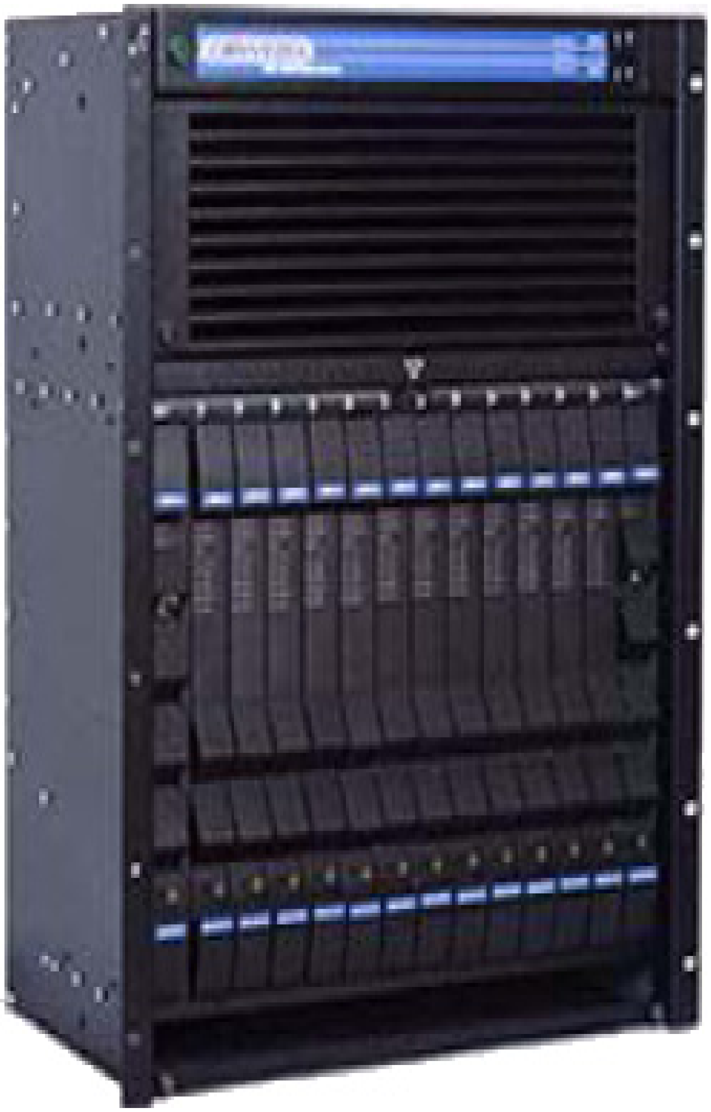
- RFC 2833 -DTMF support
- In-band and out-of-band DTMF support
- Up to 999 user conferences and 70 operator conferences
- Full support of the media server interface
- Support for 1 recorded music channel, and up to 4 connection based (FDAPI) music channels
- Support for wideband conferencing (16kHz sampling rate with a G.722 codec). Wideband conferencing is enabled via Conference Configuration > Sample Rate config of the CMS-6000 web configuration interface.

Currently the S6200 is compatible with the CMS-6000 Convedia server.

S6800 Media Server

The S6800 media server uses the S6200 as the application server and the CMS-6000 as a media server.

Figure 2: S6800 Media Server



Note:

Refer to Convedia's *CMS-6000 Media Server Installation and Operations Manual*, part number 95-0062-00-10, for additional information on the CMS-6000.

Server Redundancy

Server redundancy is not supported on the single S6200 media server because the application server and the media processing function are both part of a single-point-of-failure device. Redundancy requires that these functions be separated.

In the S6800 systems and the multiple S6200 solutions, there are separate application servers and media servers.

The S6800 systems use a workgroup to provide redundancy. Depending on the redundancy required, there can be up to three “active” application servers and one “standby” application server monitoring the “active” servers. Each S6800 server supports up to 9 active MPCs with 3 standby MPCs. Each set of 3 active MPCs is configured to fail over to a specific standby MPC.

In the multiple S6200 solution, there can be one "active" application server with one "standby" application server and up to four media servers. The four media servers share the call processing across all servers. If one of the media servers fails, the calls on that server fail over in equal proportion to the three remaining media servers. Each S6200 can process up to 2,000 calls.

The standby application server takes over automatically as necessary with a configurable period and exception count. The schedules from the CRS database are pushed to all application servers (active and standby) so that conferences are available on all application servers in case of any type of failover.

KVM Switch

A Keyboard/Video/Mouse switch (KVM) should be installed to allow one monitor and keyboard to connect to the S6200/S6800 Conferencing Servers and up to three associated application or media servers.

Installation Steps

Installation consists of the following steps:

6. Verify installation of power, thermal management, LAN, and network connections.
7. Verify receipt of necessary hardware and cables.
8. Mount hardware to racks or as specified.
9. Connect power, keyboard/video/mouse, modems, LAN, and network connections.
10. Verify system operation.
11. Notify Support Help Desk that system is ready to be configured. Note any discrepancies between installed facilities and Site Survey.

12. Install the Linux Operating System and the Meeting Exchange software.
13. Configure the system.

The first six steps are covered in *Meeting Exchange*® *5.0 Installing the* S6200/S6800 Conferencing Servers. Step 7 and 8 are the subject of this document.

Chapter 2: Configuration

This chapter describes basic configuration recommendations for the supported S6x00 configurations as well as information regarding core services integration.

Introduction

Following the initial software installation you will need to configure server-specific files. The following sections describe the configuration requirements for the following:

- Configuring and loading the Electronic Preinstallation Worksheet (EPW)
- Configuring and verifying SNMP
- Verifying core services
- Software Application and Media Servers (S6200)
- Hardware Media Servers (S6800)
- Setting Time Zones on a Linux server

Enabling sroot login

When an S6200 server is newly installed, you must log in using craft, then su to sroot. To add sroot as a direct login, log in with craft and the craft password. Enter the following command:

```
su - sroot
vi /etc/ssh/sshd_config
```

Page down to the entry:

```
PermitRootLogin no
```

Change the entry to permit root login:

```
PermitRootLogin yes
```

Save the change. Issue a restart command for the new setting to take effect;

```
/sbin/service sshd restart
```

Electronic Preinstallation Worksheet (EPW)

To facilitate configuration of settings for the conferencing server, an Electronic Preinstallation Worksheet is included with the software installation. After you install the Linux and Meeting Exchange software on your server, use SCP to copy the EPW to your PC. Configure the settings for your conferencing server and download the completed EPW to the conferencing server.

Tip:

Use the EPW only for a new install, not for an upgrade.

Obtaining a copy of the EPW

1. Go to `/usr/dcb/bin/mx_epw`
2. Copy the EPW_MX.xls file to `/usr/dcbguest`
3. Open a WinSCP session on your PC
4. Enter conferencing server IP address
5. Login: dcbguest

   Password: abc123
6. Protocol: SFTP
7. Click Login
8. Copy EPW_MX.xls from `dcbguest` to a directory on your PC.
9. Close WinSCP

Configuring the EPW

Open the worksheet on your pc and enter specifics about your conferencing server by paging through the tabs at the bottom of the page. You will need information for the following pages shown in Table 2

Table 2: EPW Settings

EPW Page	Description	Information Cross Reference
Intro	Provides description of EPW	Read-only
Status	Quick reference to determine completion status of each EPW page	Read-only
Checklist	Overview of items needed for software install	Read-only
Usage - Platform Information	Enter server names and IP Addresses	Verifying Network Configuration and adding NTP Servers on page 130 **Note:** If the conferencing server does not use NTP, provide an IP address of 0.0.0.0 in this field.
NFS Config	Details for setting up an NFS server for audio files	Configuring the NFS Server on page 56
Server		
	Server Configuration Parameters	Table 4: System.cfg General Information Settings on page 39
	Media Server Runtime Parameters	Sample softMediaServer.cfg file on page 44
	Media Server Interface Configuration	Configuring the NFS Server on page 56
	Video Conferencing - System Parameters	Media Server Interface Configuration: Video Settings on page 118
	Process Configuration Parameters	Table 7: processTable.cfg on page 51
System	System Configuration	*Meeting Exchange 5.0 Administration and Maintenance S6200/S6800 Media Servers,* Document 04-602167, Chapter 4

Table 2: EPW Settings

EPW Page	Description	Information Cross Reference
Scheduler	Scheduler Settings	*Meeting Exchange 5.0 Bridge Talk User's Guide,* Document 04-602163, Chapter 11
Sign-in	Maintenance, Operator and Scheduler sign-in configuration	*Meeting Exchange 5.0 Administration and Maintenance S6200/S6800 Media Servers,* Document 04-602167, Chapter 2
SIP		
	SIP Proxy Configuration	Proxy Address with which to register
	URI to Telephone Number Configuration	URI to telephone number translation table on page 50
	Telephone Number to URI Configuration	Telephone number to URI translation table on page 49
Logging	Set file to capture logging information	default = /var/log/MX
SNMP	Configure IP for SNMP trap receivers	Verifying SNMP trap information using the EPW on page 25

Loading the EPW

Once you have configured all the settings in the EPW, download the spreadsheet to your conferencing server.

1. Follow steps 1 through 6 in Obtaining a copy of the EPW on page 22.
2. Copy the completed EPW from your PC to /usr/dcbguest on the conferencing server.
3. Close your WinSCP session.
4. Log in to the server as a superuser.
5. Copy the new file from dcbguest to /usr/dcb/bin/mx_epw.
6. Stop the server

```
service mx-bridge stop
```

7. Run the utility

```
./run_mx_epw.sh <Excel_spreadsheet_name>
```

8. Verify the installation in the generated log file at: `/var/disk/logs/run_mx_epw.log`

9. If you are using SNMP, run the commands shown in Verifying SNMP trap information using the EPW on page 25.
10. Reboot the server to install the new configurations.

Verifying SNMP trap information using the EPW

The EPW utility modifies a SQL script, `/usr/ipcb/config/mxalarms.postgres.sql`, which is then used to populate the trap destination information into the snmptrapreceiver table in the Core Services database.

To verify that the SNMP trap information has been populated to postgres, execute the following commands after running the EPW utility:

```
su postgres
```

At the bash prompt, enter:

```
psql coreservices -f /usr/ipcb/config/mxalarms.postgres.sql
```

This command will execute the /usr/ipcb/config/mxalarms.postgres.sql command which will populate the snmptrapreceivers table.

To see the configured SNMP trap services, at the bash prompt, enter:

```
psql coreservices
```

At the coreservices # prompt, enter:

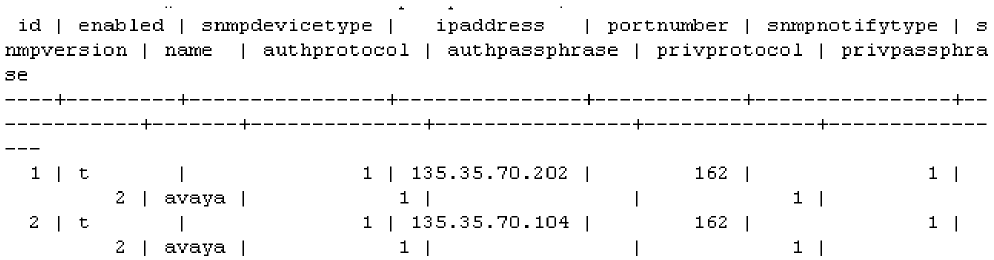
```
select * from snmptrapreceiver;
```

Tip:

Verify that you have included the semicolon at the end of the command.

This will return the information for the SNMP trap server that has been set up for your system.

The following is sample output from a conferencing server that has SNMP trap servers configured.



```
 id | enabled | snmpdevicetype |   ipaddress    | portnumber | snmpnotifytype | s
nmpversion | name  | authprotocol | authpassphrase | privprotocol | privpassphra
se
----+---------+----------------+----------------+------------+----------------+--
-----------+-------+--------------+----------------+--------------+-------------
---
  1 | t       |              1 | 135.35.70.202  |        162 |              1 |
          2 | avaya |            1 |                |            1 |
  2 | t       |              1 | 135.35.70.104  |        162 |              1 |
          2 | avaya |            1 |                |            1 |
```

Working with SNMP

This section describes simple network management protocol (SNMP). Avaya use SNMP to monitor the performance of the conferencing server. The SNMP system emits alarms, which are called traps. You can use the EPW to configure SNMP traps or you can use a manual method. This section describes the manual method.

If you do not use the EPW to configure the audio conferencing server, the mandatory tasks required to use SNMP alarming are:

- Inserting and deleting entries in the snmptrapreceiver table
- Setting the productid in system.cfg if using INADS

This section also describes a number of additional tasks. It contains the following sections:

- Verifying that SNMP is running
- Looking at the SNMP traps
- Debugging SNMP

Note:

If you make changes to `system.cfg`, you must restart the server. If you make changes to the database, you do not need to restart the server.

Inserting and deleting entries in the snmptrapreceiver table

The following script provides an example for manually inserting and deleting an SNMP trap receiver entry. Each entry requires a unique ID. In this example, the ID is 1, the trap receiver IP is 10.110.120.130, and the port is 162.

To insert an SNMP trap receiver entry:

1. Obtain the IP address of the SNMP trap destination.
2. Connect to coreservices database:

```
[sroot@nidhi ~]# su postgres
bash-3.00$ psql coreservices
Welcome to psql 8.1.4, the PostgreSQL interactive terminal.
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
```

3. View the SNMP trap receiver table:

```
coreservices=# select * from snmptrapreceiver;

 id | enabled | snmpdevicetype | ipaddress | portnumber |
  snmpnotifytype | snmpversion | name | authprotocol |
  authpassphrase | privprotocol | privpassphrase

----+---------+--------------+----------+-----------+---------
  ------+------------+-----+------------+--------------+-----
  ---------+---------------

(0 rows)
```

4. Insert or delete the SNMP trap receiver entry:

- To insert:

  You must configure the SNMP in the database for Network Management System (NMS) and Initialization and Administration System (INADS). Configuring the traps is slightly different in both cases:

  - For NMS, the SNMPdevicetype = 1
  - For INADS, the SNMPdevicetype = 2

  ```
  coreservices=# insert into snmptrapreceiver (id, enabled,
    snmpdevicetype, ipaddress, portnumber, snmpnotifytype,
    snmpversion, name, authprotocol,authpassphrase, privprotocol,
    privpassphrase) values ('1', 'true', 1, '100.110.120.130', 162,
    1, 2, 'avaya', 1, '', 1, '');

  INSERT 0 1
  ```

- To delete:

  Enter the following command:

  ```
  coreservices=# delete from snmptrapreceiver where id = '1';

  DELETE 1
  ```

5.Verify the insertion or deletion.

- To verify an insertion:

  ```
  coreservices=# select * from snmptrapreceiver;

   id | enabled | snmpdevicetype |    ipaddress    | portnumber |
    snmpnotifytype | snmpversion | name  | authprotocol |
    authpassphrase | privprotocol | privpassphrase

  ----+---------+----------------+-----------------+------------+--
    --------------+-------------+-------+--------------+-----------
    -----+-------------+---------------

    1 | t      |            1 | 100.110.120.130 |       162 |
    1 |          2 | avaya |           1 |               |
    1 |

  (1 row)
  ```

- To verify a deletion:

  ```
  coreservices=# select * from snmptrapreceiver;

   id | enabled | snmpdevicetype | ipaddress | portnumber |
    snmpnotifytype | snmpversion | name | authprotocol |
    authpassphrase | privprotocol | privpassphrase

  ----+---------+----------------+-----------+------------+-------
    --------+-------------+------+--------------+----------------+-
    ------------+---------------

  (0 rows)
  ```

6.Exit Coreservices.

```
coreservices=# \q

bash-3.00$ exit

exit

[sroot@nidhi ~]#
```

Setting the productid in system.cfg if using INADS

You must set the Product ID if you are using INADS. You can configure the Product ID either using the EPW method or by configuring the `system.cfg` file. The Product ID must be a unique number, of no more than 10 digits, which is sent in all INADS traps to distinguish which system is generating the traps.

Note:

If you make changes to `system.cfg`, you must restart the server. If you make changes to the database, you do not need to restart the server.

Verifying that SNMP is running

To verify that SNMP is operating correctly, run the following commands to verify that the SNMP trap receiver is receiving the traps:

```
bridge restart
```

You should receive multiple traps.

Looking at the SNMP traps

Table 3 shows the SNMP traps generated by the system. These traps operate for both NMS and INADS:

Table 3: SNMP Traps

Trap	Trap Description
avMX6200ProcessStartedNotification	This trap is generated when a critical Avaya Meeting Exchange process has been started.
avMX6200ProcessStoppedNotification	This trap is generated when an Avaya Meeting Exchange process has been stopped. When you kill a softms process on a Pyramid system, the following is the trap sequence: Kill softms A. Trap receiver shows: ● softms A stopped ● softms B started ● softms C started ● softms B stopped
avMX6200ApplicationServerFailover	This trap is generated when the application server fails over.
avMX6200MediaServerFailed	This trap is generated when the media server does not respond. **Note:** This trap is only generated on 6200 & 6800 configurations. It is not generated in a Pyramid system.

Table 3: SNMP Traps

Trap	Trap Description
avMX6200PortPoolUsageIncrease	Generated when the port pool usage exceeds 80% of the maximum number of ports
avMX6200PortPoolUsageDecrease	Generated when the port pool usage no longer exceeds 80% of the maximum number of ports

Most of the traps generated by the system come from the Meeting Exchange MIB:

```
AV-MX-S6200-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, enterprises
        FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
        FROM SNMPv2-CONF
    sysName
        FROM SNMPv2-MIB
    entPhysicalAssetID
        FROM ENTITY-MIB
    applSrvName
        FROM APPLICATION-MIB
    ipAdEntAddr
        FROM IP-MIB
    ItuPerceivedSeverity
    FROM ITU-ALARM-TC-MIB
    ituAlarmAdditionalText
        FROM ITU-ALARM-MIB;

avmx6200mib MODULE-IDENTITY
       LAST-UPDATED "200609300000Z"-- 30 Sep 2006
       ORGANIZATION "AVAYA"
       CONTACT-INFO "Avaya Customer Services
```

```
                        Postal: Avaya, Inc.
                                211 Mount Airy Rd
                                Basking Ridge. NJ 07920
                                USA
                                Tel: +1 908 953 6000
                                WWW: http://www.avaya.com"

       DESCRIPTION  "A MIB to support Meeting Exchange Groupware
Edition S6200.
                     Copyright (C) 2007 by Avaya Inc.  All rights
reserved."

       REVISION     "01" -- 30 September 2006
       DESCRIPTION
           "Revision 1.0.0 - Marc Zehngut
            Original version."

       ::= { avMX6200Mibs 1 }

--
-- The following are defined in AVAYA-GEN MIB
--
avaya              OBJECT IDENTIFIER ::= { enterprises 6889 }
products           OBJECT IDENTIFIER ::= { avaya 1 }
mibs               OBJECT IDENTIFIER ::= { avaya 2 }

avMX6200Prod OBJECT IDENTIFIER ::= { products 22 }
avMX6200Mibs OBJECT IDENTIFIER ::= { mibs 22 }

--
-- Top level components of this MIB
--
avMX6200Notifications OBJECT IDENTIFIER ::= { avmx6200mib 1 } --
Notification group
```

```
avMX6200Objects       OBJECT IDENTIFIER ::= { avmx6200mib 2 } --
Objects


--
-- Common Object groups for CoreServices MIB
--
avMX6200NotifyObj     OBJECT IDENTIFIER ::= { avMX6200Objects 1 }


--
-- Core Services Notify group (csNotifyObj)
--
avMX6200AlarmSeverity OBJECT-TYPE
    SYNTAX      ItuPerceivedSeverity
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Alarm severities are based on ITUPerceivedSeverity (RFC 3877)"
    ::= { avMX6200NotifyObj 1 }


--
-- MX Suite 5.0 Notifications
--
avMX6200ProcessStartedNotification  NOTIFICATION-TYPE
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
```

```
       "This trap is generated when an Avaya Meeting Exchange process
has been started."
    ::= { avMX6200Notifications 101 }

avMX6200ProcessStoppedNotification  NOTIFICATION-TYPE
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
       "This trap is generated when an Avaya Meeting Exchange process
has been stopped."
    ::= { avMX6200Notifications 102 }

avMX6200PortPoolUsageIncrease  NOTIFICATION-TYPE
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
       "This trap is generated when the port pool usage exceeds 80% of
the maximum number of ports."
    ::= { avMX6200Notifications 103 }

avMX6200PortPoolUsageDecrease  NOTIFICATION-TYPE
```

```
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
        "This trap is generated when the port pool usage no longer
exceeds 80% of the maximum number of ports."
    ::= { avMX6200Notifications 104 }


avMX6200ApplicationServerFailover  NOTIFICATION-TYPE
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
        "This trap is generated when the application server fails
over."
    ::= { avMX6200Notifications 105 }

avMX6200MediaServerFailed  NOTIFICATION-TYPE
    OBJECTS {
        sysName,
        ipAdEntAddr,
        entPhysicalAssetID,
        csAlarmSeverity,
        applSrvName,
        ituAlarmAdditionalText
    }
    STATUS  current
    DESCRIPTION
        "This trap is generated when the media server does not
respond."
    ::= { avMX6200Notifications 106 }

END
```

Debugging SNMP

This section describes some of the common issues with SNMP. It contains steps and suggestions to overcome these issues.

- If traps are not generating, you should ensure the following core services are running:

  ```
  /opt/coreservices/lifecycle/bin/lc list
  ```

  There should be 12 services started.

  ```
  /opt/coreservices/dss/bin/dss list -h localhost -p 50000
  ```

  There should be 2 services started.

  ```
  /opt/coreservices/dss/bin/dss list -h localhost -p 31050
  ```

  There should be 21 services started.

  Note:

  If coreservices does not appear to be running properly see Running and verifying Core Services on page 35 for advice on how to restart core services correctly.

Running and verifying Core Services

Core services are integrated with the S6200/6800 Meeting Exchange solution. Use the following commands to start, stop, and verify core services.

- Start

  ```
  /sbin/service wdinit start
  ```

- Stop

  `/sbin/service wdinit stop`

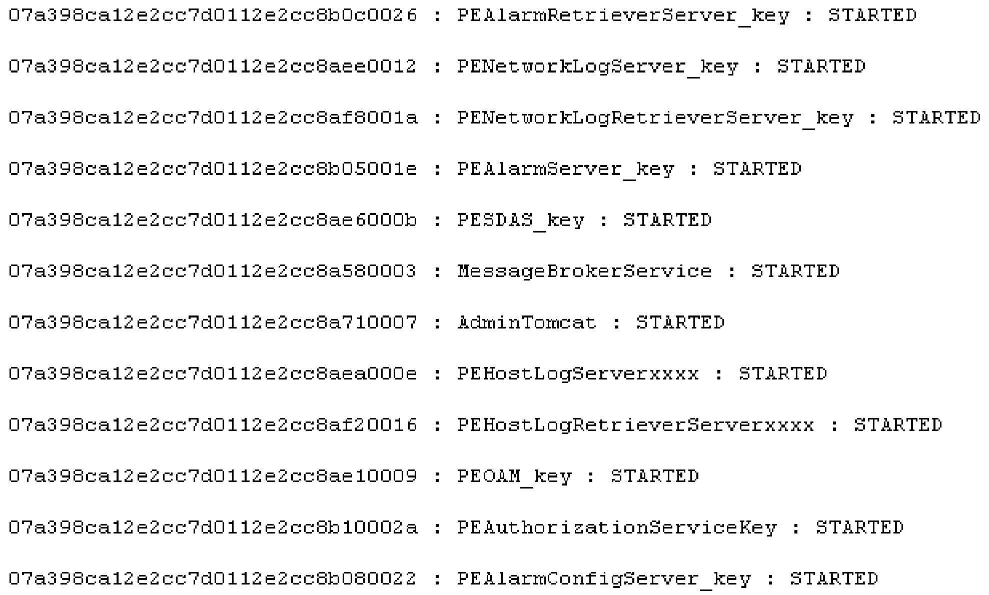
- Restart

  `/sbin/service wdinit restart`

To verify that all processes are running as part of core services, execute the following command:

```
/opt/coreservices/lifecycle/bin/lc list
```

The output will include the ten services listed as started in the figure below:



```
07a398ca12e2cc7d0112e2cc8b0c0026 : PEAlarmRetrieverServer_key : STARTED

07a398ca12e2cc7d0112e2cc8aee0012 : PENetworkLogServer_key : STARTED

07a398ca12e2cc7d0112e2cc8af8001a : PENetworkLogRetrieverServer_key : STARTED

07a398ca12e2cc7d0112e2cc8b05001e : PEAlarmServer_key : STARTED

07a398ca12e2cc7d0112e2cc8ae6000b : PESDAS_key : STARTED

07a398ca12e2cc7d0112e2cc8a580003 : MessageBrokerService : STARTED

07a398ca12e2cc7d0112e2cc8a710007 : AdminTomcat : STARTED

07a398ca12e2cc7d0112e2cc8aea000e : PEHostLogServerxxxx : STARTED

07a398ca12e2cc7d0112e2cc8af20016 : PEHostLogRetrieverServerxxxx : STARTED

07a398ca12e2cc7d0112e2cc8ae10009 : PEOAM_key : STARTED

07a398ca12e2cc7d0112e2cc8b10002a : PEAuthorizationServiceKey : STARTED

07a398ca12e2cc7d0112e2cc8b080022 : PEAlarmConfigServer_key : STARTED
```

If the services are not up and running, the user may see STOPPED status for some of them.. The verification command generates an exception if the core services are stopped.

⚠ **CAUTION:**

If the core services do not start up, the conferencing server will come up within one minute. If the core services start up correctly, the server will take between 10 and 15 minutes to fully load.

Core Services Logging

To control logging to the host log server provided by core services, modify the following .xml file on the conferencing server:

/usr/ipcb/config/ipcblog4j.xml

The following lines at the end of the file enable the logging to HOST_LOG_SERVER:

```
<root>
  <priority value=”all” />
  <appender-ref ref=”system‟ />
  <appender-ref
  ref=”HOST_LOG_SERVER” />
</root>
```

In order to -disable logging to HOST_LOG_SERVER, modify the lines to:

```
<root>
  <priority value=”all” />
  <appender-ref ref=”system‟ />
  <!--appender-ref
  ref=”HOST_LOG_SERVER”/-->
</root>
```

Using the log viewer

To use the log viewer:

1. On the internet, go to:http://bridgeIP:8080/CS-OAM

   Example: http//12.21.12.125:8080/CS-OAM

   Tip:

   Disable pop-up blockers.

2. On the logging screen enter the following:

   Login ID : sroot

   Password: srootpw

3. Go to **System Maintenance > Log Viewer or Alarm Manager**
4. Select the required settings and click OK.
5. The logs/alarms display in a popup window.

Core Services limitations and known issues

The following limitations and known issues have been identified with core services:

1. Core services may fail to come up. First verify that core services are installed then run the following command:

   ```
   cd /etc/rc.d/init.d
   ```

   ```
   ./mx-runOnce
   ```

2. Checking the status of core services with `/opt/coreservices/bin/lifecycle/lc list` will cause an exception if core services have been stopped with the following command: /sbin/services wdinit stop.
3. Reboot of a conferencing server results in core services restarting. A complete reboot takes 10 to 15 minutes.

General System Configuration

If the EPW is not used for configuration, to manually configure settings, you will need to configure:

1. The system.cfg, located in /usr/ipcb/config.

You may also need to configure the server to support:

2. conference scheduler
3. call branding

The following sub-sections describe how to configure these features.

System Information: system.cfg

S6200/S6800 Conferencing Servers default system information must be configured in order for the system to function properly. The configuration file is named system.cfg and is located in /usr/ipcb/config.

Follow this procedure to configure S6200/S6800 Conferencing Servers:

1. Open the system.cfg file for editing.
2. Locate the General system information section.

3. Edit the address and extension settings for the site. Table 4 describes the settings and System Configuration File: system.cfg on page 114 contains example files.

Table 4: System.cfg General Information Settings

Setting	Description
IPAddress	The IP address of the S6200/S6800 Conferencing Servers
MyListener **Note:** Use tls when only the current hop (bridge to next level) requires tls. Use Sips when you need the entire end to end transport to be secured by tls so that each hop uses tls.	The SIP URI of the port and transport on which S6200/ S6800 Conferencing Servers listen. To listen to a different port number, to the end of the entry add ":####", where #### is the port number. To use a different transport, add "sips" for a secured transport or ";transport=tls" to the end of the entry. Example: sip:001s6800@<IP Address of S6200> If an Avaya CM is being used, add one of the following lines. Comment out the unused transport type: For secure transport: `MyListener=sip:6000@135.35.32.35:5061;transport=tls` For TCP: MyListener=sip:6000@135.35.32.35:5060;transport=tcp

respContact	This setting overwrites the default contact header on responses. If an Avaya CM is being used, add the following lines: Comment out the unused transport type: SIP Address.
	For secure transport:
	`respContact=<sip:6000@135.35.32.35:5061;transport=tls>`
	For TCP:
	`respContact=<sip:6000@135.35.32.35:5060;transport=tcp>`

MaxChannelCount	Set this value to: ● 700 with one media server ● 1500 with two media servers ● 2000 with three media servers
MaxVideoChannelsAllowed	Set the number of video licenses Values allowed: 0-2000. Default = 0.

1 of 3

Table 4: System.cfg General Information Settings (continued)

Setting	Description
DiffServTOSValues	Value that is inserted into the IP header's type of service (TOS) field. This is used to differentiate the service. Some routers will route specific values faster or with priority. DiffServSignallingTOSValue= DiffServMediaTOSValue=
EthernetVlanValues	Value that is inserted into the IP header's virtual LAN (VLAN) field. EthernetSignallingTOSValue= EthernetMediaTOSValue=
MaxMeetingCount	Not implemented in this release
MaxConferenceCount	Not Implemented in this release
MaxOperatorCount	Not Implemented in this release
BillingDirectory	Not implemented in this release
PlatformName	Not implemented in this release
AdHocMinPortsAvailable	Not implemented in this release
AdHocDefaultConferenceSize	Number of ports set aside per conference for ad hoc conferences default=5
SippingNotificationInterval	Notifications are sent from Notification Service to populate ad hoc conferences for an external device. With SippingNotificationInterval set to 5, one notification per conference with updated participant information is sent every 5 seconds. Default=5 (Select 1-15)
processKeepAlivePollTime	Number of seconds between polls for process functionality. Keepalive polls the processes 3 times at the specified poll intervals. If the processes do not respond after the third poll, they will be restarted. default=11 (seconds)
softmsTimeInterval	Packetization interval for RTP. For each interval, softms reads and sends out a packet default= 20000 (microseconds)
bridgetranslatorTimeInterval	Time interval to convert data to allow two way data flow between endpoints default=6 (seconds)
	2 of 3

Table 4: System.cfg General Information Settings (continued)

Setting	Description
Back to Back User Agent allRouteTo	B2BUA Reroutes calls from standby to active server =sip:4001@<active server IP>
MediaServerExecName	/usr/dcb/bin/convMS.
MediaServerPriority	Designates the server number of the application server when part of a cluster. (If there are 3 app servers and 3 media servers per bridge,the second app server has MediaServerPriority 4 , and the third app server has MediaServerPriority 7)
NumMediaServers	Number of media servers in the conferencing solution. (1 +)
	3 of 3

4. Save the changes.

Supported Video Channels

The maximum number of video channels supported by the server depends on the number of licenses purchased and the bit rate used. Video port licensing is configured in the MaxVideoChannelsAllowed parameter as shown in System.cfg General Information Settings on page 39

The S6800 supports from 128 to 768 kilobits per second. Table 5 shows the number of video channels available based on supported bitrates, picture size, and frame rate.

Tip:

A maximum of 16 video channels are supported in a single conference for bi-directional video ports.

Supported Video Endpoints

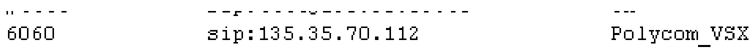
The conferencing server supports the following video endpoints:

- Polycom_VSX 8.5.3
- Polycom V500 8.5.3
- Polycom V700 8.5.3
- Polycom HDX Series
- Avaya IPSP H.323
- Avaya UC Communicator H.323 & SIP

Tip:

To dial out to a Polycom VSX endpoint, configure the Polycom in the TelnumtoURI table as shown in Figure 3

Figure 3: Polycom Endpoint Configuration



```
6060          sip:135.35.70.112          Polycom_VSX
```

Table 5: Video Channel Limits with CMS 6000

Total Bit Rate	Picture Size:MPI	Audio Codec	# Ports per MPC	Resource Allocation % for Video on MPC
768 kbits/s	CIF1	G.711	45	91%
512 kbits/s	CIF:2	G.711	80	83%
384 kbits/s	CIF:1	G.711	90	83%
256 kbits/s	CIF:4	G.711	170	75%
128 kbits/s	QCIF:4	G.711	250	66%
768 kbits/s	CIF:2	G.722	40	83%
384 kbits/s	CIF:4	G.722	80	66%

The video codec setting for the CMS 6000 is H.263 as shown in Figure 5.

Note:

Convedia does not support linking of video conferences.

See Media Server Interface Configuration: Video Settings on page 118 for detailed information to enable video for your conferencing server.

Video Configurations for CMS 6000

Set the following configurations on your Convedia media server for video conferencing.

Log into the Convedia web interface: http://<Convedia IP>

From the interface:

1. Go to Configuration > Slot Configurtion > Configure Video

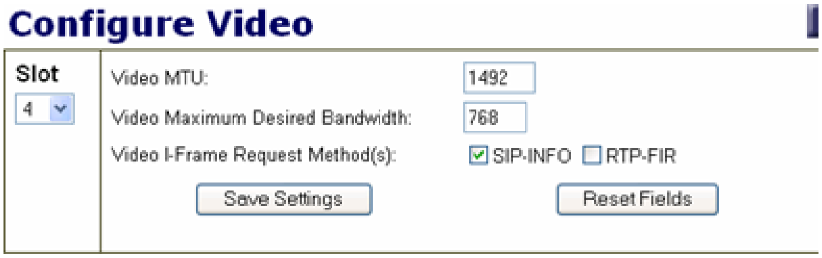
2. Set Video Maximum Desired Bandwidth to 768

Tip:

Set this to the maximum supported setting of 768 and let the VdeoBandwidth setting in the S6200 mediaServerInterface.cfg limit the bandwidth

3. Select SIP-INFO as the Video I-Frame Request Method.

Figure 4: Convedia Video Configuration



Configure Video

Slot: 4

Video MTU: 1492

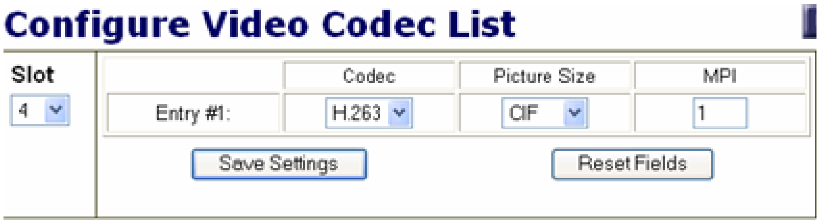
Video Maximum Desired Bandwidth: 768

Video I-Frame Request Method(s): ☑ SIP-INFO ☐ RTP-FIR

4. Go to Configuration > Slot Configuration > Configure Video Codec List

5. Set the codec as shown in Figure 5

Figure 5: Convedia Video Codec



Configure Video Codec List

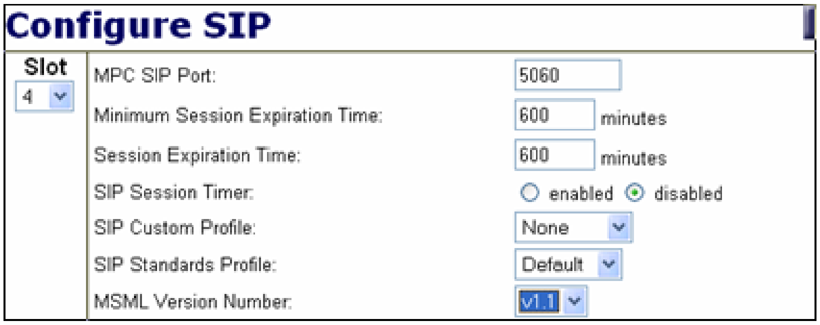
Slot: 4

	Codec	Picture Size	MPI
Entry #1:	H.263	CIF	1

6. Go to Configuration > Slot Configuration > Configure Resource Allocation

7. Configure SIP settings according to recommendations shown in .Table 5: Video Channel Limits with CMS 6000 on page 42.

Figure 6: Convedia SIP Configuration



Configure SIP

Slot: 4

MPC SIP Port: 5060

Minimum Session Expiration Time: 600 minutes

Session Expiration Time: 600 minutes

SIP Session Timer: ○ enabled ● disabled

SIP Custom Profile: None

SIP Standards Profile: Default

MSML Version Number: v1.1

Software Media Server Configuration (S6200 only)

The software media server features are configured in the softMediaServer.cfg. This file is stored in the /usr/ipcb/config directory.

The sample softMediaServer file, shown in the following example, contains field explanations.

Sample softMediaServer.cfg file

```
# Media server runtime parameters
# Automatic gain on or off 1 or 0
AutomaticGain=0
# generate confort noise on =1 off = 0
ComfortNoiseGeneration=0
# initial port for the rtp data
baseRtpPort=42000
# Max number of channels in media server
maxChannels=702
# Max conference size
maxChannelsPerConference=300

# Ip Address for NFS Server (Pyramid) mounts.
# If not set then default to appserver ip address
#NFSServerIPAddress=10.1.2.3
```

Setting the active speaker notification interval

By default, the S6200 bridge checks each channel every 2000ms to see if someone is speaking. This value can be changed by setting the asninterval in the `softMediaServer.cfg` file as shown in the example below.

```
# Active speaker notification interval

asnInterval=500
```

If `asnInterval` is specified as 500, each channel is checked every 500ms to monitor if someone is speaking.

Note:

The `asnInterval` value overrides the bridge default value.

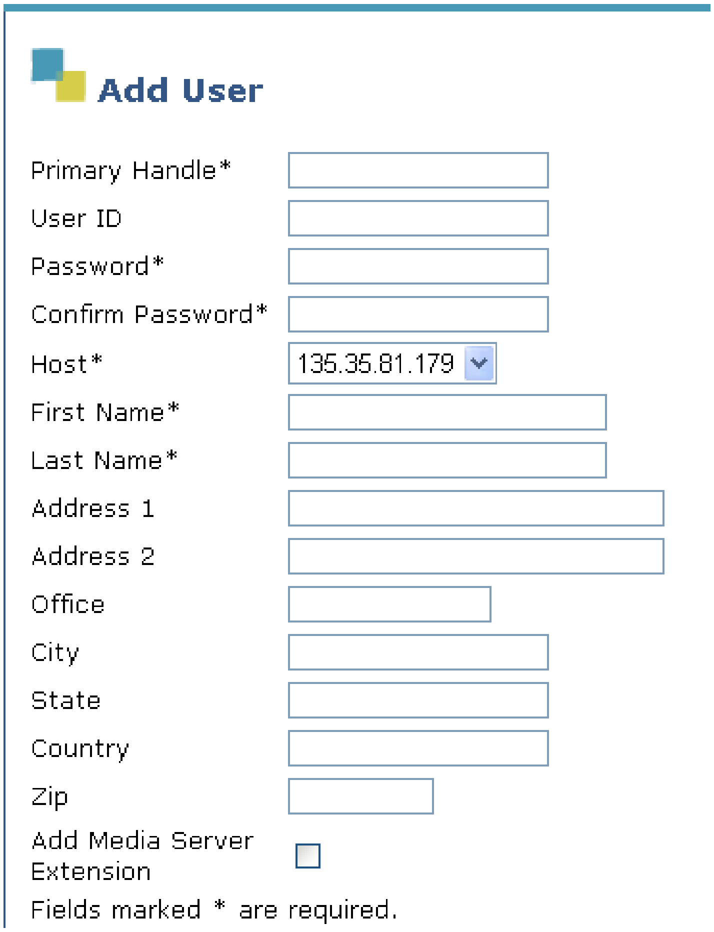
SIP Enablement Server (SES) and Meeting Exchange

When the Meeting Exchange solution includes an SES Server, all DNIS/DDI numbers must be added as users on the the SES server.

1. Obtain a list of all DNIS/DDI configured for the Meeting Exchange server.
2. Log into the SES Server as follows:

   https://<SES IP>/admin
3. Click OK at the digital certificate prompt.
4. Click Yes at the Security Alert.
5. Click Continue.
6. Log in ID: craft

   Password: craft01
7. Click Yes at Suppress alarm origination prompt.
8. Select Launch Administration Web Interface.
9. On the web interface, select Users > Add. The following screen appears:



Add User

Primary Handle*

User ID

Password*

Confirm Password*

Host* 135.35.81.179

First Name*

Last Name*

Address 1

Address 2

Office

City

State

Country

Zip

Add Media Server Extension □

Fields marked * are required.

10. Enter user information. Fields with an asterisk (*) are required.

    Primary Handle: Meeting Exchange DNIS/DDI, for example, 5500.

    Password: Must be a minimum of 6 characters

    Host: IP of the SES Server

    First Name: Enter a name, for example: mx

    Last Name: Enter a name, for example: bridge

11. SAVE the new user information.
12. Create a new user for each DNIS/DDI configured on the conferencing server.
13. Telnet to the SES server.
14. Enter terminal type: vt100

15. Enter the following command:

```
vi /usr/impress/sip-server/etc/ccs.conf
```

16. Arrow down to the Registrar section.
17. Set “EnableAuthentication” to false.
18. Restart the SES server.
19. Add each SES User to the proxy configuration table as shown in the next section.

Tip:

If the Meeting Exchange solution includes a CRS, do not add the proxy information to proxyConfigTable.cfg. See Configure the CRS on page 67 to add proxy information.

Proxy Configuration: proxyConfigTable.cfg

When the Meeting Exchange solution does not include a CRS, each proxy that the S6x00 registers with is configured in the proxy configuration table file, proxyConfigTable.cfg, in /usr/ipcb/config.

The following example proxyConfigTable.cfg file wraps for clarity.

proxyConfigTable.cfg file example

```
# proxy configuration
ProxyUriContactTo
From usrNamepassWord refreshTime
sip:10.220.15.50sip:0192@10.221.10.192sip:0192@10.220.15.50sip:0192@10.221.10.192
customerABC123 180
```

Add each proxy as shown in Table 6.

Table 6: Proxy Configuration Settings

Setting	Description
ProxyURI	The valid SIP URI of the Proxy Server.
Contact	The default Contact SIP header used on dialouts or on the proxy registration.
To	The default To SIP header used by the system when dialing out or on the proxy registration.
From	The default From SIP header used by the system when dialing out or on the proxy registration.
	1 of 2

Table 6: Proxy Configuration Settings (continued)

Setting	Description
usrName	The user name of the person listed as the contact.
passWord	The password of the user.
refreshTime	The refresh rate for the SIP timer. The default is 180. Support suggests a value of 360, or six minutes.
	2 of 2

Refer to Proxy Table Configuration for use with Operator Dial In on page 129 for another example of this file.

Telephone number to URI translation table

S6200/S6800 Conferencing Servers allows conferees to dial out during a conference by pressing *1 followed by the phone number. The system matches the entered DTMF number to an entry in the telnumToUri.tab file. This file resides in the /usr/ipcb/config directory.

Sample telnumToUri.tab file

```
#telnum to uri conversion table
# This file is for dialing out from the Bridge to an external party.
# The digits that are dialed are converted into the Request URI
# in the SIP INVITE.
# For example, if the digits dialed were 936543, and one of the
# patterns was “93????" a match would take place.
# If the conversion for that match was $1, then the Request URI
# for the SIP INVITE would be sip:936543@10.221.11.250
# Entries to any column may not contain SPACES. For example,
# a valid entry in the Comment Column is "Operator_Line",
# while "Operator Line" is not valid.
# note: 0000 entry is used to dialout operator
TelnumPattern TelnumConversioncomment
"0000” sip:6352@10.221.10.111Bridge
"93????” sip:93$1@10.221.11.25mediagateway
#*    sip:$0@10.221.10.111:5060;transport=tcp defaultmediagateway
#*    sip:$0@10.221.10.111:5061;transport=tls defaultmediagateway
```

Tip:

Add either `transport=tcp` or `transport=tls` to `media gateway` only if connecting with an Avaya CM.

Note:

The last entry in the file is always an asterisk (*). This is the default number that the system dials when a number is not entered via DTMF.

In the preceding file sample, if “0000” is dialed during a conference after *1 then the “sip:6352@10.221.10.111” URI would be used to dial out. The“6352” is the dialout attendant and “10.221.10.111” is the IP address of the IP phone or proxy server. If “936388” is entered during a conference after *1 then “sip:936388@10.221.11.250” is dialed where “936388” is the line dialed and “10.221.11.250” is the IP address of the media gateway.

Note:

The $1 in the TelnumConversion column replaces the first wildcard matched from the TelnumPattern column.

Configuration for Web Portal or Bridge Control API(BCAPI)

Audio Console and BCAPI need to be able to place a call, which does not connect, but at the same time, does not receive a disconnect. To create this situation, add entries to the telnumToUri table that will route the moderator call to the web server or to BCAPI. When a CRS is installed, this routing allows the call to not be answered, and not be disconnected.

Edit the telnumToUri table to replace the last wildcard entry with the following lines:

```
TelnumPatternTelnumConversioncomment
"0*" sip:0$1@<gateway ip address> defaultmediagateway
"1*" sip:1$1@<gateway ip address> AnyNumber1xxxx
"2*" sip:2$1@<gateway ip address> AnyNumber2xxxx
"3*" sip:3$1@<gateway ip address> AnyNumber3xxxx
"4*" sip:4$1@<gateway ip address>AnyNumber4xxxx
"5*" sip:5$1@<gateway ip address> AnyNumber5xxxx
"6*" sip:6$1@<gateway ip address> AnyNumber6xxxx
"7*" sip:7$1@<gateway ip address> AnyNumber7xxxx
"8*" sip:8$1@<gateway ip address> AnyNumber8xxxx
"9*" sip:9$1@<gateway ip address> AnyNumber9xxxx
*    sip:1234@<webportal ip address> APIDialOutOperator
```

Where:

<gateway ip address> is the IP address of the gateway or proxy server to be used.

<webportal ip address> is the IP address of the server where Web Portal resides.

URI to telephone number translation table

The S6x00 servers allow different participants dialing into the system to be routed to different call flows. Call routing is determined by entries in the UriToTelnum.tab file located in the /usr/ipcb/config directory.

Example UriToTelnum.tab file

```
# request URI to telnum conversion table
# This table converts the Request URI in the SIP INVITE request to the
# appropriate value specified when a pattern is matched.
# For example, if the request Uri was "<sip:3333@10.220.10.4>" and
# one of the patterns was "<sip:*@*" a match would take place.
# If the conversion for that match was $1 then 3333 would be passed
# as the ddi for the call. If the conversion for that match were "0000"
# then 0000 would be passed as the ddi for the call.
#
TelnumPatternTelnumConversioncomment
"*@10.221.10.90”$0Bridge
"*@*”$0OtherBridge
```

Software Process Configuration

The processTable.cfg file defines all software processes started by ipcbinit. Usually, following installation, there is a version of processTable.cfg for each supported media server: S6200 media server (Software based DSP) or S6800 media server.

Following installation:

1. Copy the appropriate version of processTable.cfg to /usr/ipcb/config/processTable.cfg.
2. Edit the file to delete extra media servers. Other settings retain the default settings installed.

The processTable.cfg file may contain comment lines, which start with the “#”. Any blank lines in the file are ignored. Table 7 defines the fields contained in the file.

Table 7: processTable.cfg

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>processName</td><td>This string identifies which process to run. The process name starts an executable file, where:
<table>
<tr><th>Process Name</th><th>Starts this executable:</th></tr>
<tr><td>initipcb</td><td>initipcb</td></tr>
<tr><td>bridget700</td><td>bridgeTranslator</td></tr>
<tr><td>commsProcess</td><td>serverComms</td></tr>
<tr><td>sipAgent</td><td>sipagent</td></tr>
<tr><td>msDispatcher</td><td>msdispatcher</td></tr>
<tr><td>mediaServer</td><td>softms for S6200: convms for S6800.</td></tr>
<tr><td>notifyService</td><td>notifyservice</td></tr>
<tr><td>snmpAgent</td><td>snmpAgent</td></tr>
</table>
</td></tr>
<tr><td>IpcKeyNumber</td><td>This is a unique number used to identify the System V message queue used as the input for each process. To list all the IPC queues and the keys they use, enter the “ipcs -q” command.</td></tr>
<tr><td></td><td>*1 of 2*</td></tr>
</table>

Table 7: processTable.cfg (continued)

Field	Description
autoStart	The value in this column determines whether initipcb will automatically start processes when it runs. ● When **`autoStart=0`** then initipcb will not automatically start the process until told to do that by another process (such as mxshare or mxmonitor). ● When **`autoStart=1`** then the process automatically starts if the IP address is for the local machine and the full path to the executable is correct. **Note:** When new software is used with prior versions of the processTable.cfg, the default for autoStart is “1”; initipcb starts all processes it finds in the processTable.cfg unless the IP address was for a remote computer or the path name was set to “noexecute”.
ProcessExe	This is the path to the executable file for this process. It is used by the ipcbinit process to automatically start and stop processes. If you don't want a process started or stopped then set this to “noexecute”. For example, use noexecute for processes that are started by dcbinit such as bridget700.
IpAddress	This is the IP address of the computer where this process runs. You can enter it in numeric format such as 10.221.10.192, use “local” (without quotes), or 0.0.0.0 for processes running on the local computer where the processTable.cfg file is located. Use 0.0.0.0 for processes that should run on each system in a multiserver configuration.
Route	This defines the destination processes for messages sent by the process being defined. If there is more than one use a comma separated list.
ProcessArgs	These are command line arguments passed to a process. The use is specific to the process so there is no general guideline on what values to use.
	2 of 2

Refer to Appendix C: Configuration Files on page 109 to view example files for various media server configurations.

Log Files

The log files for the platform processes are located in /usr3/ipcb/log directory. The log name format is **system.log.<year><month><day>**, for example, **system.log.2007-04-22**.

The file contains all logging information for the processes.

Music Source

Music sources are implemented as audio files in /usr2/annun on the media servers. Music file names are music_source<1-4>. Customized music files can be created in .pcm format and copied in place of the default music sources.

Setting Time Zones for a Linux Operating System

Use the following utility to set time zones with Meeting Exchange 5.0 and above, as Linux does not support the scoadmin utility.

> ⚠ **Important:**
> Set the bridge time zone after the Linux box has been set to the correct time zone.

Time Zone Setting Procedure

1. Access the server via SSH. Log in with sroot. You will be logged into: `root@server_IP>`
2. `root@server_IP]#` **`cd /usr/dcb/bin`**
3. `root@server_IP]#` **`tzset help`**

This returns a list of supported time zones and the number associated with them. For example, the number 82 corresponds to US:Eastern.

When the system returns to `root@server_IP>`, enter the desired time zone for your conferencing server. For example:

```
root@server_IP]# tzset
```

Message displays: **`Enter timezone number or press ‘0’ for list of timezones.`**

```
root@server_IP]# 82
```

Message displays: **`Bridge timezone will be set to :US/Eastern. Please restart computer in order the changes will take effect.`**

4. `root@server_IP]#` **init 6**

Once the reboot is complete, verify that the new timezone has taken effect.

5. `root@server_IP]#` **`echo $TZ`**

The system displays the currently supported time zone.

> ⚠ **Important:**
> If you do not run **`tzset`** for your server, logs will be generated in GMT.

Using an NFS Server

The S6x00 can create audio recordings of conferences. Software media servers running directly on the S6x00 use a local file system to write recording files. Hardware media servers use NFS to write recording files to an NFS server.

Note:

Recording files are stored in /usr3/ipcb/usr3/confrp as raw pcm files. The Convedia servers store recording files with the digit names and a wav extension. These servers do not use raw pcm files. Files in /usr3/confrp will not have the wav extension, are 0 bytes in length, and cannot be played in BridgeTalk.

Install the software and the hardware media servers prior to configuring the NFS server. You need the following information about your hardware media servers:

- IP address assigned to each hardware media server.
- The fully qualified DNS host name for each hardware media server or the DNS alias name for each.

These steps are required to configure an NFS Server for use with the S6800 Hardware Media Server solutions:

- Configure the NFS Server
- Configure the Convedia Media Server
- Configure the software media server.

Upgrading from a prior configuration

When upgrading from an earlier version of the media server, you will need to run a script that moves audio files into the /usr3 directory and creates links, so that the server can locate the files.

After successful installation of the media server, follow this procedure to run the script.

1. Log in as sroot.
2. Execute this command:

```
/ipcb_nfsinst.sh
```

⚠ **Important:**

Do not interrupt this process. The script may take a few minutes to run if there are existing recording files.

Configuring the NFS Server

The NFS server can be running on one or more Application (APP) servers or on one or more NFS servers. The instructions below are split into three sections for clarity: NFS, APP, and media server. The media server section is divided into hardware and software media servers.

When the same machine runs as both NFS and APP servers, use the same server IP for both the APP and the NFS.

Firewall

Turn off the iptables firewall:

```
chkconfig -level 0123456 iptables off
```

Conferencing Application Server

The following steps configure NFS on the Application Server.

1. For solutions installed with an S6800, on th Application Server, go to:

   /usr/ipcb/config/mediaServerInterface.cfg.

2. Specify NFSServerIPAddress.
3. Add the following entries to /etc/exports:

   ```
   /usr3/ipcb/usr3/confrp MS_1 (rw,async,no_root_squash)
   /usr3/ipcb/usr2/roster MS_1 (rw,async,no_root_squash)
   ```

   Tip:

   If you have multiple MPCs, add entries for each one. For example:

   ```
   /usr3/ipcb/usr3/confrp MS_1 (rw,async,no_root_squash) /usr3/
     ipcb/usr3/confrp MS_2 (rw,async,no_root_squash)
   /usr3/ipcb/usr2/roster MS_1 (rw,async,no_root_squash) /usr3/
     ipcb/usr2/roster MS_2 (rw,async,no_root_squash)
   ```

4. If you plan to record additional Prompt sets, create the following directory:

   ```
   mkdir -p /usr3/ipcb/usr3/confrp/Prompts
   ```

5. Restart the NFS services

   ```
   service nfs restart
   ```

Linux NFS Server

The following steps describe the configuration of NFS on a separate NFS server.

1. Create an entry for each MPC into local /etc/hosts. For example:

```
10.0.0.101 MS_1.company.com MS_1
10.0.0.102 MS_2.company.com MS_2
10.0.0.103  MS_3.company.com MS_3
```

2. Verify the following directories exist or create as needed:

   - NFS server on the APP server:

   ```
   /usr/dcb/bin/ipcb/nfsinst.sh
   ```

3. Restart the NFS server.

```
service nfs restart
```

Note:

Restart forces nfs to flush its cache host name.

Hardware Media Servers

Set up the APP and NFS servers as described in Conferencing Application Server and Linux NFS Server before configuring the Convedia media servers.

1. Configure a mount point on each MPC to reference the exported directory “/usr3/ipcb” on the NFS server.
2. Configure the MPC to automount the exported directory as startup.
3. Mount the export directory and verify correct operations.

Software Media Servers

In a solution with S6200 media servers, NFS will be automatically mounted. To confirm the NFS mount point on the server, log in as a superuser. Enter mount to see a listing of NFS directories.

```
sroot> mount
```

Server Redundancy

Server redundancy, or failover, occurs when the primary application server fails and the standby server automatically assumes operation for the failed server.

When this failover occurs, the standby server:

- Changes its role from standby to primary.
- Sends the Takeover message to the Client Registration Server (CRS)
  - View the server role changes in the Bridge tab of the CRS front end.
- Registers with the SIP proxy server so that calls intended for the failed server route to the standby.
- Ceases monitoring the other application servers.
- If a call is sent to a standby server, the Back to Back User Agent (B2BUA) redirects the call to the active server.

Sites installed with at least three application servers, a single Client Registration Server, and a standby server can use the Workgroup Redundancy Setup. One of the servers is reserved as a standby server. This method is detailed later in this section, but first you will need to configure the application server so that it can identify the CRS

Establishing the CRS Data Source

Systems configured for failover rely on the Client Registration Server (CRS). The chdbased.reg file, found in /usr/dcb/dbase/admin, identifies the CRS to the application server. This file contains the section, [crsdatasource], with the settings required to connect the application server to a CRS.

Most of the default attribute values set in this file apply to any installation. However, the ‘address’ attribute specifies the name of the CRS. Make sure that you edit the file to supply the address attribute, but remember that raw IP addresses are not supported.

Tip:

If the CRS is not registered with the Domain Name Service, add an entry for the CRS in the application server’s /etc/hosts file. Find the default settings in the following example, CRS data source section of the hosts file.

CRS data source section of the hosts file

```
[crsdatasource]
installed=true
name=crsdatasource
version=0.1
address=voyager
port=5050
user=ACS
cabinet="14." <—obtain this value from the CRS.>
```

Important:

If the CRS is running when the mxmonitor process starts up, then the mxmonitor process initializes and begins polling for sip data. Later, if the CRS stops running, the polling thread continuously attempts to reconnect and when the CRS comes back, will reconnect. In the interim. the system runs with the data it has until the connection to the CRS is restored.

The system is not usable if mxmonitor cannot get at an initial copy of sip data from the CRS. Therefore, if the CRS is not running when the mxmonitor starts up, the system kills the mxmonitor process and the initpcb process tries to restart the mxmonitor process. In this situation, mxmonitor writes a core file to the /usr/dcb directory. These files can quickly fill the drive.

Note:

Additional information on installing the Client Registration Server is available in the following document: *System Administrator Guide for CRS.*

Obtain the SIP proxy settings

Run ./specteltest from the application server's command line to identify the SIP proxy entries that are needed to configure the CRS Front End. The file is located in /usr/dcb/bin directory.

Follow these steps to discover the SIP proxy entries need by the CRS front end.

1. Type this command:

   ./specteltest

   The system displays:

```
Menu choices:
        v   - validate passcode
        n   - new reservation
        u   - update reservation
        t   - update reservation by tui
        e   - extend reservation
        r   - resinst test
        a   - auto add
        p   - display product info
        l   - list reservations
        z   - get time zone ref
        c   - add entry to call branding table
        1   - update an entry in the call branding table
        2   - delete an entry in the call branding table
        3   - list all entries in the call branding table
        4   - get the total number of entries in the call branding table
        5   - get list of duplicate entries created for new DNIS length
        6   - set the DNIS length to a new value and delete duplicates
        7   - add our test set to the call branding table
        8   - dump secCode for first conference.
        9   - list sip proxy configuration entries.
        x   - update sip proxy configuration table.
        y   - take over for specific cabinet.
        d   - get call brand entry by DNIS
        b   - test Config Services
        ?|h - print this message
        q   - quit
```

2. Type "9" at the command line:

   The system displays this prompt:

```
Enter Bridge Reference Number:
```

3. Type the bridge number at the command line, for example, 5:

   The system displays the information related to bridge 5:

```
Ref    ProxyURI            Contact          To                 From
   UsrName Pwd     RefreshTime     DNIS
=================================================================================
   =============================================================
10    sip:10.220.15.50    sip:1900@10.220.15.52    sip:1900@10.220.15.50
   sip:1900@10.220.15.50   user1 password 120            1900
11    sip:10.220.15.50    sip:2000@10.220.15.52    sip:2000@10.220.15.50
   sip:2000@10.220.15.50   user1 password 120            2000

Press ENTER to continue...
```

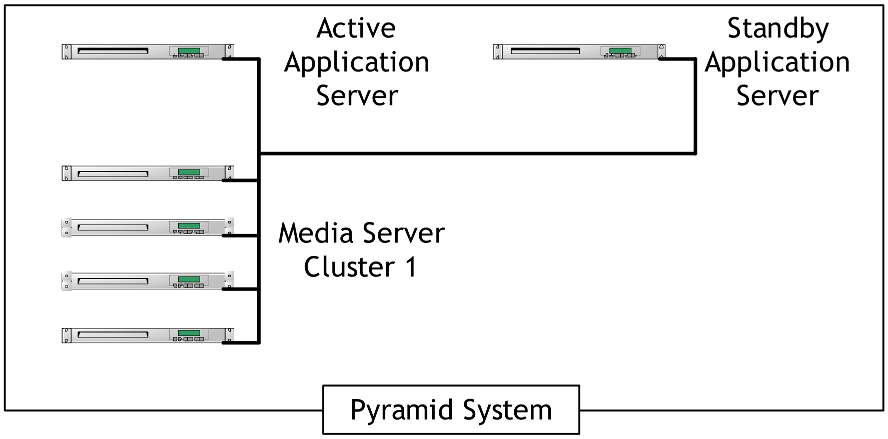
   Important:
   This list contains the information that you will enter to Configure the CRS.

   Press the Enter key to display additional information.

Workgroup Redundancy Setup

A workgroup architecture provides support for server redundancy. In the default configuration, a workgroup is defined as three primary application servers, one standby application server, and one Client Registration Server (CRS). Figure 7 illustrates a typical workgroup.

Figure 7: Application Server Workgroup



The primary application server provides the IP Audio Conferencing Application. Each application server can support a specific number of IP calls and audio conferences. The standby server monitors each primary application server in its workgroup and detects failure. When a primary application server fails, the standby server assumes the failed server's role in the workgroup and ceases its monitoring function. This takeover function is possible because:

- Each Application Server and the Standby Server contain all reservations for that workgroup.
- Each Application Server and the Standby Server contain all Call Branding Tables for that workgroup.
- Each Application Server and the Standby Server contain, or have access to via the CRS, the SIP Proxy configuration data for that workgroup.

Failover is enabled on the system when:

- Each server in the workgroup contains the configuration file, mxmonitor.reg. Configuring the mxMonitor on page 62 describes this file.
- Each server in the workgroup is configured for redundancy by editing the processTable configuration file. Activating the Monitor Process on page 66 provides information on configuring the Process Table.
- Each server in the workgroup is configured to send messages to a Client Registration Server, CRS. Refer to Establishing the CRS Data Source on page 59.

Configuring the mxMonitor

The mxmonitor process identifies the servers and monitors each server to ensure that it responds to request messages. When a server denies a request from the monitor, the monitor sends the request to the next server in the workgroup. The server that responds to the request takes over the role of the server that denied the request.

When a server is configured as a standby, but determines that the workgroup already has a standby via a denied request, it switches to an active server and restarts the registration process. This design ensures that a failed application server can re-join the workgroup and take over as the standby.

Each server requires a configuration file named mxmonitor.reg. This file contains the list of servers comprising the workgroup. The file has a section for each server containing its configuration, as well as a section titled [mxconfig] containing attributes common to all servers regardless of their role. For example, the sipupdateperiod attribute specifies how often, in milliseconds, the CRS is checked for SIP Configuration data. mxMonitor.reg shows a sample of file installed on each system.

mxMonitor.reg

```
# List the systems in our workgroup.  Note, we are included in the list.
[mxworkgroup]
aps1
aps2
aps3
standby

# Which system are we and what is the DDI refresh rate?  That is, how
# often to we get the DDI/SIP config data from the database or CRS?
# Note, only 'crs' is supported as the source for DDI/SIP config data.
# Future versions may support storing this data in the local database.
#
# NOTE the cabinet reference under aps1,aps2...is the Reference value
# on the Bridges Tab on CRS Front End.
[mxconfig]
trace=false
sipsource=crs
sipupdateperiod=60000
reqtimeout=30000
checkstatustimer=60000
numstatusrequests=2
#Name of cache file. If the file name is empty, caching will not be used.
cachefile=sipproxy.tab
#Rate of cache refresh in milliseconds, defaults to 1 hour
cacherefresh=3600000
#Source for SIP proxy data. Currently only “crs” is used. In the new version, it
will be “none” #if CRS is not used. The default value will be “crs”.
sipsource=crs

[aps1]
process=aps1
role=active
cabinet=1

[aps2]
process=aps2
role=active
cabinet=2

[aps3]
process=aps3
role=active
cabinet=3

[standby]
process=standby
role=standby
cabinet=4
```

Table 8: mxMonitor Configuration Settings describes each section of this file and lists valid attributes with default settings.

Table 8: mxMonitor Configuration Settings

[Section]	Description	Attribute	Description	Default
mxworkgroup	Lists the servers in the workgroup. The name corresponds to the section for that server's configuration.	**not applicable**	not applicable	aps1 aps2 aps3 standby
mxconfig	General configuration information.	**trace**	Turns on diagnostic tracing when set to true.	false
		sipsource	Identifies the location of the SIP proxy settings. **Note:** Support for CRS only for this release.	crs
		sipupdateperiod	Frequency in milliseconds to request the SIP proxy configuration from the source.	60000 (1 minute)
		startdelaytimeout	Time in milliseconds that sip request will time out if no reponse	30000 (30 secs)
		reqtimeoutperiod	Time to wait in milliseconds for a response to an MXMONITOR REGISTER REQUEST message.	300000 (5 minutes)
		checkstatustimer	Frequency in milliseconds for the standby server to check the status of the application servers.	60000 (1 minute)
				1 of 3

Table 8: mxMonitor Configuration Settings (continued)

[Section]	Description	Attribute	Description	Default
		numstatusrequests	Number of check status retries before declaring an application server failure. **Note:** This value is zero based. The default value of 2 really means if it does not get a response after 1 attempt, the AppServer will fail over.	2
aps1	Application Server configuration	**process**	Process name. This value matches the value specified as the last property in the mxmonitor entry in processTable.cfg. Do not change this value without changing the processTable.cfg file.	aps1
		role	The server's role. Set to active for an application server. Set to standby for a for the standby server.	active
		cabinet	Identifies this application server to the CRS which uses this value to know which set of Sip Proxy Configuration data to send when requested. This attribute matches the bridgeref attribute in CRS.	1
		role	The server's role. Set to active for an active server. Set to standby for a standby server.	active

2 of 3

Table 8: mxMonitor Configuration Settings (continued)

[Section]	Description	Attribute	Description	Default
		cabinet	Identifies this application server to the CRS. The CRS uses this to discern which set of Sip Proxy Configuration data to send when requested. **Tip:** This attribute matches the bridgeref attribute in CRS.	2
standby	Application Server configuration	**process**	Process name. This value matches the value specified as the last property in the mxmonitor entry in processTable.cfg. Do not change this value without changing the processTable.cfg file.	standby
		role	The server's role. Set to active for an active server. Set to standby for a standby server.	active
		cabinet	Identifies this application server to the CRS which uses this value to know which set of Sip Proxy Configuration data to send when requested. This attribute matches the bridgeref attribute in CRS.	standby

3 of 3

Activating the Monitor Process

Following the installation, the processTable.cfg file contains the required lines for server redundancy. However, these lines are commented out by default. The installer may use a text editor to remove the comment character (#) from these mxmonitor process lines to enable redundancy. Notice the mxmonitor lines in the following processTable.cfg excerpt. The TCP/IP address is a sample.

processTable.cfg with entries for server redundancy

```
# processes file, enumerates the number of processes in the network
...
mxmonitor         201 1               /usr/dcb/bin/mxmonitor         1
35.35.23.71   appEvents/msDispatcher,netEvents/msDispatcher   aps1
mxmonitor         201 1               /usr/dcb/bin/mxmonitor         1
35.35.23.73   appEvents/msDispatcher,netEvents/msDispatcher   aps1
mxmonitor         203          1               /usr/dcb/bin/mxmonitor         1
35.35.23.74   appEvents/msDispatcher,netEvents/msDispatcher   standby
```

Important:

Configure each application and standby server with the settings required for its workgroup.

Configure the CRS

This section outlines the steps required to configure the CRS with the S6x00 media servers in order to provide server redundancy.

Tip:

Refer to document number, 04-602179, *Avaya Meeting Exchange 5.0 Client Registration Server System Administrator Guide,* for configuration details on clustering.

Follow this procedure to configure the CRS:

1. Configure new Direct Dial Inward (DDI) phone entries using the CRS front end.
2. Set up the telephone numbers.
   a. Select the **DDI**.
   b. Enter the digits of the **Phone Number** associated with the DDI.
   c. Enter descriptive information in the **Location** and **Description** fields.
   d. Enter the sip address of the application server in the **URI proxy** field. Use sip format, e.g. sip:111:222:333:000.
   e. Enter the sip address of the application server, using the value in the **Phone number** field, in the **URI contact** field. Use sip format, e.g. sip:1234@000:222:333:444
   f. Enter the sip address of the proxy to which the application server forwards the number in the **URI to** field.
   g. Enter the sip address of the proxy from which the application server expects the number in the **URI from** field.
   h. Enter the login information, which the application server uses to log in to the CRS in the **URI user name** and **URI password** fields.

i. Enter ***120*** (or site specific value) in the **URI Refresh** field. This is the number of milliseconds that the CRS uses to send changes to the application server.

j. Enter the digits of dialed number to be forwarded to an answering service, such as, 1234, in the **URI DNIS** field.

3. Configure the S6x00 media server.

   Tip:

   Set up one bridge in the CRS for each active and standby application server. Initially, reset the status of the active and standby application servers.

4. Configure the cabinet. Map each cabinet to the S6x00 media server acting as the bridge.

Working with Prompt Sets

The system has 20 prompt sets available for recording messages in multiple languages.

By default the following prompt sets are stored on the system::

Table 9: Prompt Sets

/usr2 prompt set number	Bridge Talk prompt set number	Language
0	1	English
1	2	Canadian French
2	3	Parisian French
3	4	Latin American Spanish
4	5	European Spanish
5	6	German
6	7	Russian

Adding new Prompt Sets

Before adding new prompts to the conferencing server, be sure that the selected prompt set does not have a link to Set0.

Breaking the link between prompt sets

Log in with sroot

```
cd /usr2/Prompts
ls -l
```

If the prompt set that you wish to copy to, for example Set15, does not show as the following, Set15 -> Set0, then the link is already broken, and you may copy the new prompts to this set.

If the set is linked to Set0, enter the following:

```
rm Set15
mkdir Set15
```

You may also create separate directories for the messages and the numbers:

```
mkdir Set15/messages
mkdir Set15/numbers
```

Set15 can now be used to copy new prompts.

Replacing the link between prompt sets

If you wish to re-establish the link between Set15 and Set0:

```
mv Set15 Set15.sav
```

This will save a backup copy of Set15. To add the link:

```
rm -rf ./Set15
ln -s Set0 Set15
```

The link has now been re-established between Set15 and Set0. If you copy new files to Set15, they will also copy to Set0.

Recording Messages

For best performance, create the recordings in any manner that will result in a good quality digital file. Then use an audio editing program to insert or trim the leading and/or trailing silences as described below.

Each message has a beginning and an end. Some messages are Initial Segments (e.g. “The file number you entered is...”), some (mostly the digits 0-9) are Middle segments, some are Tail Segments, (e.g. “...participants currently in your conference”), and some are stand-alone segments (e.g. “Conference security has been activated”).

Each segment of the recorded message must be preceded and followed by silence. Record approximately 0.5 - 0.9 seconds of complete silence before and after the “complete sentence”. The silence before a segment that will be combined with another segment is generally 0.05 -

0.09 seconds. If the segment will lead into another segment, then its trailing silence is shorter, in the range of 0.2 - 0.3 seconds.

The following examples show the silence increments in square brackets, [].

Initial	Middle	Tail
[.5] There are currently [.03]	[.05] seven [.03]	[.05] participants currently in conference [.5]

Stand-alone Segment
[.5] "Conference security has been activated [.9]

Loading the customized prompts onto the Media Server

S6200 Media Server

To load the prompts onto an S6200 media server, verify that there is no link between the Prompt set you wish to install and Set0. See: Breaking the link between prompt sets on page 69. Use WinSCP to copy the newly recorded files from your PC to the dcbguest directory on the conferencing server.

1. Open a WinSCP session on your PC
2. Enter conferencing server IP address
3. Login: dcbguest

   Password: abc123
4. Protocol: SFTP
5. Click Login
6. Copy the prompt set (ex. Set8) from a directory on your PC to dcbguest.
7. Close WinSCP
8. Log into the conferencing server as a superuser.

```
cd /usr/dcbguest
cp Set8 /usr2/Prompts/Set8
```

Verify that the /usr2/Prompts/Set8 directory has been updated.

Convedia Media Server

For complete documentation on how to load audio prompts on to the Convedia Media Server, please refer to the Audio Storage Management section of the *CMS-6000 Installation and Operations Manual.*

Here's a simple list of what needs to be done:

- Record or convert the audio prompt to Microsoft wav format G.711, 8kHz sample rate, 16-bit resolution, mono, mu-Law.
- If Bridge Talk is used to record audio prompts, the audio prompts will be recorded in the correct Microsoft wav format to the /usr2/Prompts directory on the NFS share where recordings are configured to be saved.
- Configure the TFTP Server's root directory to be the directory where the audio prompts reside.
- Use the Convedia User Interface to add the audio prompt to the Convedia Media Server.
  - The clip type should be "named"
  - The audio clip identifier should be the /usr2/Prompts/set1/message followed by the audio prompt file number with a wav file extension. For example, the Welcome prompt would be "/usr2/Prompts/set1/0.wav"
  - The IP address should be the IP address of the TFTP server.

The path and filename on the TFTP Server should be the audio prompt file number with a wav file extension. For example, the Welcome prompt would be "0.wav".

About Annunciator Numbering

The system stores 400 annunciator messages. Each annunciator is associated with a unique file number (0—399). This file number is always one less than message number displayed on the Flexible Annunciator Messages screen. These files have no extension. For example annunciator 2 is stored in a file named, "1" and annunciator 1 is stored in a file named "0".

Technically, you can use any annunciator message for any purpose; however, the following configuration works most often:

- Annunciators 1 to 178 are used for the dial-in greetings, dial-out greetings, and Call Routing messages. These messages are customized.
- Annunciators 179 to 253, 384 to 428, and 436 to 438 are factory prerecorded and used for various system prompts and messages, but you can replace them with different messages that meet conference-specific requirements.

- Annunciators 254 to 300 are not preonfigured.
- Annunciators 301 to 383 and 428-435 are used for Flex messages, but you can replace them with different messages that meet conference-specific requirements.

Messages are limited to a one minute in duration.

Table 10: Annunciator Messages and Message Numbering describes each message.

Table 10: Annunciator Messages and Message Numbering

File Number	Message Number	Message
0	1	Welcome. You have reached the Audioconferencing System. After the tone, enter your conference security code, followed by the pound key. Thank you.
1-177	2 - 178	configurable
178	179	After the tone, please state your name, followed by the pound key.
179	180	The following participants have been connected to the conference.
180	181	I'm sorry. Originator Dial Out is currently unavailable.
181	182	I'm sorry. Your conference is at capacity. Originator dial out cannot be performed.
182	183	The system is unable to authorize access to the dial out feature.
183	184	Conference security feature has been activated.
184	185	Conference security has been turned off. .
185	186	Someone has entered the conference.
186	187	Someone has left the conference.
187	188	I'm sorry. You have entered an invalid security code. Please try again.
188	189	I'm sorry. You have entered an invalid security code. Please stay on the line for the next available operator.
189	190	I'm sorry. You have entered an invalid PIN code. Please try again.
190	191	I'm sorry. You have entered an invalid PIN code. Please stay on the line for the next available operator.
191	192	You conference is scheduled to end in 15 minutes.
192	193	.........14 minutes

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
193	194	.........13 minutes
194	195	.........12 minutes
195	196	.........11 minutes
196	197	.........10 minutes
197	198	..........9 minutes
198	199	.........8 minutes
199	200	.........7 minutes
200	201	.........6 minutes
201	202	.........5 minutes
202	203	.........4 minutes
203	204	.........3 minutes
204	205	.........2 minutes
205	206	.........1 minute
206	207	Your conference time has now expired. Thank you.
207	208	Thank you for your patience. Please stay on the line for the next available operator.
208	209	I’m sorry. Conference recording is unavailable.
209	210	I’m sorry. Conference playback is unavailable.
210	211	Please enter your conference file number followed by the the pound key or press star to cancel.
211	212	Conference recording has stopped. .
212	213	The recording file name is…*(digits played here)*.
213	214	Press 1 to begin recording, press 2 to re- enter the file number, or press * to cancel.
214	215	Press 1 to begin the playback, press 2 to re- enter the file number, or press * to cancel.
215	216	Conference playback has stopped.
216	217	I’m sorry. The number you have entered cannot be used.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
217	218	Conference recording has been turned on.
218	219	Conference playback has been turned on.
219	220	Enter the number of minutes to skip, starting at the beginning of the playback followed by the pound key or press the * key to cancel.
220	221	You are currently the only participant in this conference.
221	222	There are currently . . .(*number of participants)*.
222	223	. . . . participants in your conference. **Note:** Messages 222 and 223 are played as one sentence.
223	224	Roster playback is complete.
224	225	Please enter the phone number that you wish to dial followed by the pound key or press * to cancel.
225	226	Originator Dial Out has been cancelled.
226	227	The phone number you have entered is . . . *(digits).*
227	228	Press 1 to make this call, press 2 to re-enter the phone number, or press * to cancel.
228	229	Your call could not be completed as dialed or the line was busy.
229	230	The selected conference is not currently active. Please confirm the scheduled time including the time zone.
230	231	This conference has been secured by the moderator and entry is not allowed at this time. Please contact the meeting organizer for additional information.
231	232	This conference has reached its maximum capacity. Please contact the meeting organizer for additional information.
232	233	No security code has been detected. To obtain a security code, please contact the meeting organizer.
233	234	Please enter the Billing Code for this conference, followed by the pound sign, or press * to cancel.
234	235	The Billing Code entered for this conference is . . . *(digits).*
235	236	Press one to accept, press two to change, or press star to cancel.
236	237	This conference will end when the last moderator hangs up.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
237	238	This conference will continue when the last moderator hangs up.
238	239	This operation has been cancelled.
239	240	This operation is currently unavailable.
240	241	Your conference has been extended an additional 25 minutes.
241	242	Hello. Your conference call is about to begin. To join the conference, please enter one on your touch tone keypad. Thank you.
242	243	Hello. Your conference call is about to begin. To join the conference, please enter your security code, followed by the pound key. Thank you.
243	244	Please stand by while your participants are dialed.
244	245	Not enough lines were available to dial all of your numbers. Please stand by while some of your numbers are dialed. To determine the number of people in your call, press * eight when dialing is complete.
245	246	Your blast dialing is complete.
246	247	Please enter your PIN code followed by the pound key. (An alternate version of this message is available from annunciator file 246a / message 247a.)
246a	247a	Please enter your PIN code followed by the pound key. If you don't have a PIN Code, simply press pound.
247	248	The system is unable to recognize the security code that was entered. Please disconnect now, thank you.
248	249	The system is unable to recognize the PIN code that was entered. Please disconnect now. Thank you.
249	250	The main conference has been secured and entry is not allowed at this time. The moderator has been notified of your request. Please stand by.
250	251	Your conference is currently secured. A participant of the Sub Conference is requesting re-entry. Please turn off security to unlock the conference.
251	252	Re-entry to the main conference is now allowed.
252	253	You are the only moderator in this conference. Please unlock the conference before joining the sub-conference.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
253	254	Your operator request has been cancelled.
254	255	Operator unavailable.
255	256	Plays a list of dtmf commands available to moderators
256	257	Plays a list of dtmf commands available to conferees
257	258	You are being placed into conference in self mute mode. To unmute yourself, press *7. (For Mute All command)
258	259	I'm sorry. The system did not detect any entry.
300	301	Thank you
301	302	Enter the area code and number followed by the pound sign. To cancel this request and return to the conference, press star.
302	303	The number you dialed is …
303	304	To proceed with dialing, press #. To change this number, press *.
304	305	… is invalid. Please enter the correct digits, followed by pound.
305	306	The following options are available once you press pound to begin dialing. To join the participant to conference, press star 1; to join the participant and continue dialing, press star 2; to disconnect the line, press star 3; to disconnect the line and continue dialing, press star 4.To proceed with dialing, press pound.
306	307	I am sorry, your entry …
307	308	…, is not valid. Enter the valid digits followed by pound.
308	309	After joining the call, to record your conference, press star 2. For assistance, press star 0. To start your conference, press 1 now.
309	310	Default conference options. All changes made to the default options will apply to active and future conferences with the exception of Quick Start. Changes to Quick Start will apply to future conference only. (When a system is configured to work with an external server such as EPV or a CRS, this message states: Default conference options. All changes made to the default options will apply to active conferences.)

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
310	311	Main Menu: To change your 4-digit Leader PIN, press 1. To configure Participant Name Record and entry and exit announcement options, press 2. To change Quick Start options, press 3. To change Auto Continuation option, press 4. For an overview of different conference options, press 9. To return to the previous menu, press star.
311	312	I"m sorry. This feature is not enabled. Please contact your service provider to change your leader PIN. To return to the previous menu, press star.
312	313	I’m sorry. This feature is not enabled.
313	314	Default options overview. Role call prompts callers to record their name as they join a conference call. At any time during the conference these names can be replayed privately to any conference participant by pressing star 9. Quick Start allows conferences to begin immediately without waiting for the leader to arrive. Auto continuation allows all conferences to automatically continue after the leader disconnects. Entry and exit announcement options determine what will be heard when participants join and leave the conference. Options include name announce, tones, or silence.
314	315	Quick Start is on. To turn Quick Start off, press 1. To return to the previous menu, press star.
315	316	Quick Start is off. To turn Quick Start on, press 1. To return to the previous menu, press star.
316	317	Auto continuation is on. To turn auto continuation off, press 1. To return to the previous menu, press star.
317	318	Auto continuation is off. To turn auto continuation on, press 1. To return to the previous menu, press star.
318	319	Participant name record is on. To turn participant name record off, press 1. To change conference entry and exit announcement options, press 2. To return to the previous menu, press star.
319	320	Participant name record is off. To turn participant name record on, press 1. To change conference entry and exit announcement options, press 2. To return to the previous menu, press star.
320	321	Participants will be announced when joining and leaving the conference with tones. To select name announce, press 1. To select tones, press 2. To select silence, press 3. To return to the previous menu, press star.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
321	322	Participants will be announced when joining and leaving the conference with names. To select name announce, press 1. To select tones, press 2. To select silence, press 3. To return to the previous menu, press star.
322	323	Participants will be announced when joining and leaving the conference with silence. To select name announce, press 1. To select tones, press 2. To select silence, press 3. To return to the previous menu, press star.
323	324	I'm sorry, participant record name must be on to choose this option.
324	325	I'm sorry, that entry is not valid.
325	326	I'm sorry, this feature is not currently implemented.
326	327	I'm sorry, that conference code is invalid. For assistance, please contact your service provider.
327	328	You will now be placed into conference. To mute your line, press star 6. To unmute, press star 7.
328	329	You are the first participant. To mute your line, press star 6. To unmute, press star 7.
329	330	To mute your line, press star 6. To unmute, press star 7.
330	331	I'm sorry, your entry is invalid. Enter the valid digits followed by pound.
331	332	Welcome to Avaya's instant conferencing. Enter your conference code followed by pound.
332	333	The conference has been locked by the leader.
333	334	The conference has been unlocked.
334	335	If you are the leader, press star now.
335	336	Please enter your leader PIN followed by pound.
336	337	I'm sorry, this conference has been locked by the leader. Please hang up and contact your service provider for assistance. You will now be disconnected by the system.
337	338	<Short silence.>

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
338	339	The following conference commands are available to the leader. To request an operator join your conference, press star 0. To request an operator speak to you individually, press 00. To dial out, press star 1. To record the conference, press star 2. To change conference entry and exit announcement options, press star 3. To lock the conference, press star 4. To unlock the conference, press star 5. To mute your individual line, press star 6. To unmute your line, press star 7. To select or de-select conference continuation after you disconnect, press star 8. To hear a private roll call of participants, press star 9. To hear a private participant count, press star #. To mute all lines except the leader, press ##. To unmute all lines, press 99. To join a sub-conference press 93. To hear the recording file name press 94. To end the conference press 77.
339	340	The following conference commands are available. To request an operator join your conference, press star 0. To request an operator speak to you individually, press 00. To mute your line, press star 6. To unmute your line, press star 7. To hear a private roll call of participants, press star 9. To hear a private participant count, press star #. To join a subconference, press 93.
340	341	You are now muted.
341	342	You are no longer muted.
342	343	The conference is now in silent mode
343	344	The conference is now in talk mode
344	345	I am sorry, that entry is not valid. Stand by for an operator. (sequence of 4 short beeps).
345	346	I’m sorry. This feature is not enabled.
346	347	The following participants are in the conference.
347	348	<Name> has joined the conference.
348	349	<Name> has left the conference.
349	350	Your request will be answered by the next available operator. To cancel your request, press star 0.
350	351	Your operator request has been cancelled.
351	352	To change conference entry and exit announcement options, press 2. To return to conference, press star.
352	353	The conference will be allowed to continue after you disconnect. To set the conference to end when you disconnect, press star 8.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
353	354	The conference will end when you disconnect. To allow the conference to continue after you disconnect, press star 8.
354	355	You will now be placed into conference. To mute your line, press star 6. To unmute, press star 7.
355	356	The leader has not arrived yet. Please stand by.
356	357	To start the conference recording, press 1. To cancel, press star.
357	358	Please stand by while your recording connection is established. To cancel the recording, press star 2.
358	359	The conference is now being recorded.
359	360	To stop the conference recording, press 1. To cancel, press star.
360	361	This conference is no longer being recorded.
361	362	After tone, state your name, followed by pound.
362	363	Sorry, no dial-out line is available.
363	364	<The system sounds two short beeps.>
364	365	I’m sorry, that conference code is invalid. Please stay on the line for the next available operator.
365	366	I’m sorry, the Leader PIN is invalid. For assistance, please contact your service provider.
366	367	An operator is requesting to join your lockedconference. To allow operator entry, press star 5 to unlock your conference.
367	368	This is a Quick Start conference.
368	369	Please enter your new leader PIN followed by a pound sign. The leader PIN must be..
369	370	to …
370	371	… digits. To return to the previous menu, press star.
371	372	Your new leader PIN is …
372	373	I’m sorry, the leader PIN must be between …
373	374	and …
374	375	… digits long. Please, re-enter your leader PIN followed by a pound sign.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
375	376	To bypass a conference passcode, press star now. To enter a conference passcode, please enter the conference passcode, followed by the pound sign. The passcode may be 4 to 9 digits.
376	377	A conference passcode will not be required for this conference.
377	378	Your conference passcode is…
378	379	To change this entry, press star now.
379	380	Please enter the conference passcode followed by the pound sign.
380	381	I’m sorry, the conference passcode must be between four and nine digits long. Please re-enter your passcode followed by the pound sign.
381	382	Please enter the conference passcode followed by the pound sign.
382	383	I’m sorry, that conference passcode is not correct. For assistance, please contact your conference leader
383	384	Please enter the Billing Code for this conference, followed by pound .
384	385	You will now be disconnected by the leader
385	386	The phone number you entered is not allowed at this time.
386	387	This conference has been secured by the moderator and entry is not allowed at this time. Please disconnect now. Thank you.
387	388	I'm sorry, we did not get your name. After you state your name, please press the pound key.
388	389	Your call will now begin. For operator assistance anytime during your call, press star zero. To mute your line press star six. To unmute press star seven. For more information, press star star.
388a	389a	Your call will now begin. For operator assistance anytime during your call, press star zero. To mute your line press star six. To unmute press pound six. For more information, press star star.
389	390	Recording...
390	391	You are being placed into a conference in muted mode.
391	392	To stop conference recording, press star two.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
392	393	An Operator is requesting to join your locked conference. To allow Operator entry, press star seven to unlock your conference.
393	394	I'm sorry, we did not get your name. Please stand by for an operator
394	395	Please select the sub conference you wish to join by pressing a digit between one and nine. You may also enter zero to go back to the main conference, or star to cancel.
395	396	The sub conference number you have entered is invalid. You will now be returned to your conference.
396	397	The sub conference number you have entered is invalid.
397	398	A moderator has requested for everyone to rejoin the main conference. You will now be transferred back to the main conference.
398	399	Sub conference...(*number one - nine).*
399	400	… is currently locked. A participant from another sub conference is trying to enter this sub conference. Press one to unlock sub conference or press star to cancel. **Note:** File 399 and 400 are played as one sentence.
400	401	The main conference is currently locked. A participant from a sub conference is requesting re-entry. Press one to unlock the main conference or press star to cancel.
401	402	…has been locked by the moderator and entry is not allowed at this time. A moderator has been notified of your request. Please stand by. **Note:** Message 399 and 402 are played as one sentence.
402	403	Everyone has been moved back to the main conference. Please rejoin the main conference now *(by pressing *93/93 0)*
403	404	Entry to the sub conference you were trying to join is now allowed.
404	405	I am sorry but the conference you were trying to join cannot be unlocked at this time.
405	406	Please enter one through nine to join a sub conference. Enter zero to go back to the main conference, pound to return all participants to the main conference, or press star to cancel.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
406	407	Your conference is currently locked so an operator is unable to assist you. Press one if you want to unlock your conference and request help. Press star if you want to cancel the help request.
407	408	Your conference is in the help queue. If you secure it an operator will be unable to assist you. Press 1 if you want to secure your conference and be removed from the help queue. Press * if you want to cancel the secure request and remain in the help queue.
408	409	Your conference is currently secured, so an operator is unable to assist you.
409	410	The Conference File Number is...
410	411	Please hold while an operator is dialed. After the operator joins, press *1 to add the operator to your conference, or *2 to hang up the operator and return to your conference.
411	412	I am sorry. An operator cannot be reached at this time. Please try again later. You will now be returned to your conference.
412	413	This is a secure conference. The option to add the operator to the conference is not available at this time.
413	414	Please hold while an operator is dialed. Press *2 to hang up the operator at anytime.
414	415	I'm sorry. An operator cannot be reached at this time. Please, try again later. You will now be disconnected
415	416	Please dial <*insert number here*> for operator assistance.
416	417	I'm sorry. Conference recording was unable to start
417	418	Please press any key on your phone to remain in conference.
418	419	Virtual Link Line
419	420	Someone has joined the conference ... Virtual Link Line.
420	421	Someone has left the conference ... Virtual Link Line.
421	422	Virtual Link Line has entered the conference.
422	423	Virtual Link Line has left the conference.
423	424	Conference gain is on
424	425	Conference gain is off.
425	426	Please stand by for Operator Help.

Table 10: Annunciator Messages and Message Numbering (continued)

File Number	Message Number	Message
426	427	The conference is in lecture mode.
427	428	The conference is no longer in lecture mode.
428	429	Your leader PIN has expired and must be changed now.
429	430	Your leader PIN will expire in… **Note:** used with 430 and 431.
430	431	…days. To change your leader PIN, press 1. To keep your current leader PIN and continue, press 2. **Note:** used with 429.
431	432	…day. To change your leader PIN, press 1. To keep your current leader PIN and continue, press 2. **Note:** used with 429.
432	433	Your new leader PIN must be different from the current leader PIN.
433	434	…digits. **Note:** used at the end of 436.
434	435	There was a system error when trying to change your leader PIN. The leader PIN is still…
435	436	The billing code entered is invalid, and you will now be disconnected.
436	437	The number of participants is below the minimum required. The call will be disconnected if more participants do not join.
437	438	The conference will now be disconnected.

Chapter 3: Switched Circuit Integration (optional)

This chapter describes the hardware features and configuration procedures for the AudioCodes Gateway server, which enables S6x00 servers to process incoming calls from switched circuit networks. Once the AudioCode'media gateway server is connected to the conferencing server, customers can easily integrate existing PSTN T1/E1 users into their IP network.

Overview

The AudioCode's Mediant 2000 and 3000 media gateway servers provide PCI Boards that may be connected to the S6200 media server to act as a gateway. Installation instructions are provided in "Chapter 3 Updating Hardware " of *Meeting Exchange® 5.0 Installing the* S6200/ S6800 Conferencing Servers.

Complete information on AudioCodes Mediant 2000 and 3000 is available from the manufacturer. Refer to the following AudioCodes documents for detailed configuration information for the gateway servers:

AudioCodes SIP Mediant 2000 TP-1610 Board User's Manual Document Version 5.0, Document #: LTRT-68805

AudioCodes SIP Mediant 2000 TP-6310 Board User's Manual Document Version 4.8, Document #: LTRT-89701

Before you begin, ensure that you have the software identified in Table 11.

Table 11: Media Requirements

Part Number	Media Description	Comments
	Mx6200- Manufacturing Image CD	OS + Informix + DCB + S6x00 Image, GA releases
	Mediant 2000 or 3000 Software CD	Configuration Utilities, Gateway Software Required

Configuring the S6200 Server

Set the following configurations on the S6200 Application server:

```
cd /usr/ipcb/config
vi system.cfg
```

Add the following lines to set the Min-SE timer to 1800 seconds in SIP INVITE messages:

```
sessionRefreshTimerValue=1800
minSETimerValue=1800
```

Note:

These values are provisioned in seconds and should be provisioned to be greater than or equal to the value used by SIP User Agents, such as the Audio Codes Mediant 2000, connecting to the server.

Configuring the Gateway

In order to configure the AudioCodes gateway server, you need to connect the server to a laptop or PC, which is running the Microsoft Windows XP or Windows2000 operating system.

⚠ **Important:**

Verify that the media server software is fully installed, configured, and tested before you configure the AudioCodes server.

Configuring the AudioCodes Mediant 2000

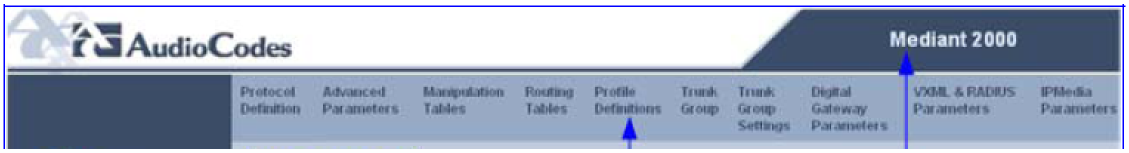
The following section describes the steps to configure the AudioCodes Mediant 2000 Media Gateway to interoperate with both the conferencing server and the PSTN. To configure the AudioCodes server:

1. Open a web browser and enter the following:

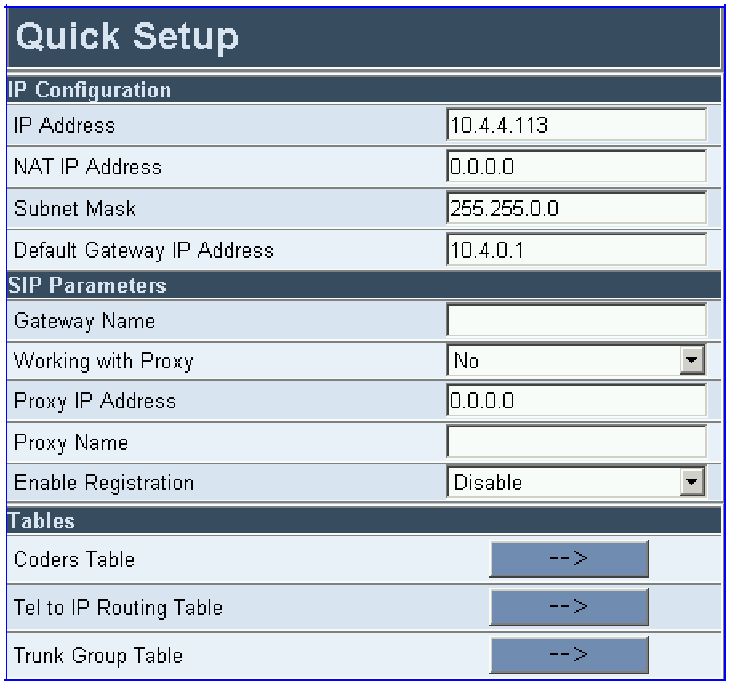
   ```
   http://<IP Address of AC Mediant 2000 Media Gateway>
   ```

2. Log into the Gateway with the appropriate credentials
3. Use the AudioCodes Mediant 2000 Web interface to configure and view settings for the menus shown in Figure 8:

Figure 8: Mediant 2000 Setup Menus



Quick Setup



Quick Setup

IP Configuration	
IP Address	10.4.4.113
NAT IP Address	0.0.0.0
Subnet Mask	255.255.0.0
Default Gateway IP Address	10.4.0.1
SIP Parameters	
Gateway Name	
Working with Proxy	No
Proxy IP Address	0.0.0.0
Proxy Name	
Enable Registration	Disable
Tables	
Coders Table	-->
Tel to IP Routing Table	-->
Trunk Group Table	-->

Use this menu to configure the server's basic settings including IP Configuration, Trunk Configuration, and SIP Parameters. Use Quick Setup also to configure the Tel to IP Routing Table, Trunk Group Table , and the Coders Table.

1. If the gateway is connected to a router using NAT, determine the router's public IP address. If the IP address is static, enter the IP address in NAT IP Address. Enable the DMZ configuration on the router for the LAN port where the gateway is connected.
2. Optionally enter the gateway's domain name in the Gateway Name field.
3. If applicable, set Working with Proxy to Yes and enter the Proxy IP Address.

4. Optionally enter the Proxy Name. The proxy name will replace the proxy IP address in all SIP messages.
5. Enable Registration if the gateway registers to a proxy server/registrar upon start up.
6. Click the arrow associated with Coders Table. Use the Coders Screen to configure coders used with your gateway. List coders in order of preference, starting with the highest priority coder.
7. Click the arrow associated with Tel to IP Routing Table. Use the Tel to IP Routing Screen to route incoming telephone calls to IP addresses.
8. Click the arrow associated with Trunk Group Table . Use the Trunk Group Table Screen to configure E1/T1 B channels.
9. Click the Reset button and click OK at the prompt. The gateway applies the changes and restarts.
10. Once the gateway resets, select Advanced Configuration > Trunk Settings. Select the gateway's E1/T1 protocol type and the Framing method that meets your system requirements.

    Note:

    For E1 spans, always select Extended Super Frame.

The gateway server is ready to use with the basic settings configured as shown. To configure more advanced settings, go to Protocol Management.

Protocol Management.

To administer the gateway's SIP parameters and tables, select Protocol Management. Settings that can be configured from this menu include:

- Protocol Definition Parameters

  General parameters, supported codecs, DTMF and dialing parameters
- Advanced Parameters

  SIP protocol parameters and miscellaneous parameters
- Manipulation Tables

  IP to Tel Source and Destination tables, Tel to IP Source and Destination tables
- Routing Tables

  IP to Tel Routing Table, Tel to IP Routing Table, parameters associated with routing tables
- Profile Definitions

  Use Profile Definitions to set up preferred behavior for codecs, trunk groups, and trunk group routing.

- Trunk Group

  Use the Trunk Group table to assign trunk groups, profiles, and logical telephone numbers to the gateway's E1/T1 B-channels. Trunk Groups route IP to Tel calls.

  - Trunk Group Settings

    The Trunk Group Settings table is used to determine the order in which new calls are assigned to B-channels within each trunk group.

Note:

> To reduce glare conditions, set the channels to hunt from opposite sides of the hunt group on the user side and the PSTN side. For example, set Channel Select Mode to Ascending on the Mediant Gateway and Descending on the PSTN side.

Advanced Configuration

To set advanced configuration settings for the gateway server, select Advanced Configurations. Settings include:

- Network Settings

  Use Network Settings to configure IP settings, application settings, NFS settings, IP routing table, and VLAN settings

- Media Settings

  Use Media Settings to define Voice settings, FAX/Modem and CID settings, RTP/RTCP settings, IPmedia settings, and general media settings.

  - Trunk Settings

    Use Trunk Settings to configure trunk parameters.

- SS7 Configuration

  Use SS7 Configuration to configure SS7 tunneling parameters

- TDM Bus Settings

  Use TDM Bus Settings to configure PCM Law to A-law or mu-Law, TDM Bus Clock Source, and idle patters.

- Configuration File

  Use Configuration File to backup and restore the gateway's configuration via an *ini* file stored on a local computer.

- Regional Settings

  Use Regional Settings to set and view the server's internal date and time as well as to load Call Progress Tones, CAS, and Voice Prompt configuration files to the gateway.

- Security Settings

  Use Security Settings to configure Web User Accounts, the Web and Telnet Access List, Firewall Settings, Certificates, General Security Settings, the IPSec Table, and the IKE Table.

- Management Settings

  Use Management Settings to configure Syslog Settings, SNMP Settings, and Activity Types to report.

Statistics and Diagnostics

Use this menu to monitor Gateway Statistics, Message Logs, Device Information, Ethernet Port Information, and Performance Statistics.

Software Update

Use Software Update to upgrade the gateway server's software by loading a new *cmp* file along with the *ini* file and several auxiliary files.

Maintenance

Select Maintenance to lock and unlock the gateway server, save the gateway configuration ,and reset the gateway.

Note:

Detailed information for each setting listed above is provided in the following guide: *AudioCodes SIP Mediant 2000 TP-1610 Board User's Manual Document Version 5.0, Document #: LTRT-68805*

Configuring the AudioCodes Mediant 3000

The following section describes the steps to configure the AudioCodes Mediant 3000 Media Gateway to interoperate with both the conferencing server and the PSTN. To configure the AudioCodes server:

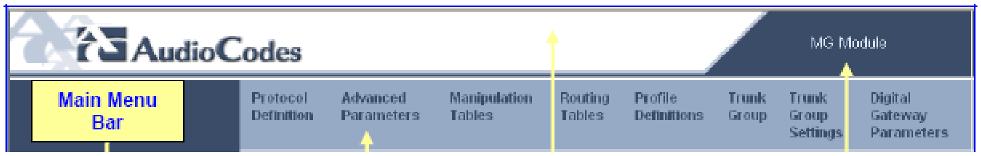
1. Open a web browser and enter the following:

   ```
   http://<IP Address of AC Mediant 3000 Media Gateway>
   ```

2. Log into the Gateway with the appropriate credentials.
3. Use the AudioCodes Mediant 3000 Web interface to configure settings as shown in Figure 9:

Figure 9: Mediant 3000 Menu Settings

Figure 5-2: Mediant 3000 Web Interface



Quick Setup - 3000

Use this menu to configure the server’s basic settings including IP Configuration, Trunk Configuration, and SIP Parameters. Use Quick Setup also to configure the Tel to IP Routing Table, Trunk Group Table , and the Coders Table.

Protocol Management - 3000

To administer the gateway’s SIP parameters and tables, select Protocol Management. Settings that can be configured from this menu include:

- Protocol Definition Parameters

  General parameters, supported codecs, DTMF and dialing parameters

- Advanced Parameters

  SIP protocol parameters and miscellaneous parameters

- Manipulation Tables

  IP to Tel Source and Destination tables, Tel to IP Source and Destination tables

- Routing Tables

  IP to Tel Routing Table, Tel to IP Routing Table, parameters associated with routing tables

- Profile Definitions

  Use Profile Definitions to set up preferred behavior for codecs, trunk groups, and trunk group routing.

- Trunk Group

  Use the Trunk Group table to assign trunk groups, profiles, and logical telephone numbers to the gateway’s E1/T1 B-channels. Trunk Groups route IP to Tel calls.

  - Trunk Group Settings

    The Trunk Group Settings table is used to determine the order in which new calls are assigned to B-channels within each trunk group.

Note:

To reduce glare conditions, set the channels to hunt from opposite sides of the hunt group on the user side and the PSTN side. For example, set Channel Select Mode to Ascending on the Mediant Gateway and Descending on the PSTN side.

Advanced Configuration - 3000

To set advanced configuration settings for the gateway server, select Advanced Configurations. Settings include:

- Network Settings

  Use Network Settings to configure IP settings, application settings, NFS settings, IP routing table, and VLAN settings

- Media Settings

  Use Media Settings to define Voice settings, FAX/Modem and CID settings, RTP/RTCP settings, IPmedia settings, and general media settings.

  - Trunk Settings

  Use Trunk Settings to configure trunk parameters.

- SS7 Configuration

  Use SS7 Configuration to configure SS7 tunneling parameters

- TDM Bus Settings

  Use TDM Bus Settings to configure PCM Law to A-law or mu-Law, TDM Bus Clock Source, and idle patters.

- Configuration File

  Use Configuration File to backup and restore the gateway's configuration via an *ini* file stored on a local computer.

- Regional Settings

  Use Regional Settings to set and view the server's internal date and time as well as to load Call Progress Tones, CAS, and Voice Prompt configuration files to the gateway.

- Security Settings

  Use Security Settings to configure Web User Accounts, the Web and Telnet Access List, Firewall Settings, Certificates, General Security Settings, the IPSec Table, and the IKE Table.

- Management Settings

  Use Management Settings to configure Syslog Settings, SNMP Settings, and Activity Types to report.

Statistics and Diagnostics - 3000

Use this menu to monitor Gateway Statistics, Message Logs, Device Information, Ethernet Port Information, and Performance Statistics.

Software Update - 3000

Use Software Update to upgrade the gateway server's software by loading a new *cmp* file along with the *ini* file and several auxiliary files.

Save Configuration

Select Save Configuration to save the current parameter configuration and the loaded auxiliary files to the non-volatile memory so they are available after a power failure.

Reset Device

User Reset Device to reset the Mediant 3000 gateway. Prior to resetting the gateway, you are provided with the option to save the current configurations.

Note:

Detailed information for each setting listed above is provided in the following guide: *AudioCodes SIP Mediant 2000 TP-6310 Board User's Manual Document Version 4.8, Document #: LTRT-89701*

Appendix A: Video Integration with Communication Manager

This appendix describes the configuration settings that are required when Meeting Exchange provides video integrated with Avaya's Communication Manager via a SIP Enablement Server.

Overview

Avaya's Communication Manager is an open, scalable telephony application that can be integrated with value-added applications to solve business challenges. It organizes and routes voice, data, and video transmissions. Communications Manager can connect to public and private networks, ethernet LANs, ATM networks, and the internet.

For Meeting Exchange, Communications Manager, in conjunction with an S6800 media server, enables a moderator to connect video endpoints to an ad hoc or scheduled conference via a button on an Avaya softphone. The moderator presses the softphone Conference button to dial out to the endpoint and presses the button again to transfer the caller into the ad hoc conference.

Note:

An Ad Hoc conference expires after 30 minutes if no one joins.

For more information about Avaya's Communication Manager, see *Overview for Communication Manager*, Release 4.1, Document 03-300468.

⚠ **Important:**

Video integration in Meeting Exchange requires an Avaya SIP Enablement Server in conjunction with Avaya Communication Manager.

Video Integration

Video integration with Meeting Exchange is limited to voice activated switching. It does not support the transcoding of different video signals into a conference. Therefore, a participant who connects in 768 kbps CIF video mode for an endpoint to endpoint call might join the conference in 128 kbps QCIF video mode in accordance with Meeting Exchange settings.

A participant establishes a conference call via Meeting Exchange as outlined in the following example:

1. Callers A and B are in an endpoint to endpoint call via Communication Manager.
2. Caller A presses Conference on their Avaya phone to invite caller C.
3. Caller A hears dial tone and dials out to Caller C who answers.

4. Caller A presses the Conference button again. The audio RTP stream for callers A and B is placed on the Communication Manager media processor into the same service as RTP for caller B.
5. Communication Manager detects a multiparty call and sends a SIP INVITE to Meeting Exchange with ad hoc conference URI.
6. Meeting Exchange creates an ad hoc conference reserving 6 lines from the demand port pool and returns conference URI.
7. Communication Manager invokes a SIP INVITE to Meeting Exchange with conference URI to each of the video endpoints.
8. Once Communication Manager has an RTP stream for each video endpoint, it invokes "bridgeMove" which moves each endpoint to the Meeting Exchange stream.
9. Communication Manager is no longer involved in the RTP stream between the video endpoints and Meeting Exchange.

Calls with more than two video endpoints will be transferred to the conferencing server via a Fast Transfer button on the Avaya phone. The originating caller will not be required to enter any dialing digits to initiate the dialout to the third party. Fast Transfer is facilitated with the SA8953 button that is controlled via the system parameters special-application form of the Communication Manager.

Callers without video capability will be connected to the conference as audio participants.

System.cfg Configurations

Configure the following fields in system.cfg to provide video conferencing integrated with Communication Manager:

Table 12: system.cfg for video

Field	Description	Settings
RAINotificationInterval **Note:** RAI = Resource Availability Indicator	The amount of time NotificationCtrlServer will wait before sending a forced RAI notification	1-300 seconds Default = 60
RAIHighThreshold	Value in percentage of the minimum number of ports in use when a notification is sent to Communication Manager with "AlmostOutOfResources=True"	Default = 90

Table 12: system.cfg for video

Field	Description	Settings
RAILowThreshold	Value in percentage of the maximum number of ports in use when a notification is sent to Communication Manager with "AlmostOutOfResources=False"	Default =75

MaxRAISubscribers	Maximum number of Communication Managers that can use a single Meeting Exchange server to create an ad hoc conference	Maximum = 10
		Default = 10

For a single server Meeting Exchange bridge, with video integration: With the maximum number of RAI subscribers set to 10 and the notification interval set to 60, the conferencing server will send 10 simultaneous notifications if the maximum number of subscribers is reached.

Configuring outbound SIP proxies

When using SIP proxies on the audio conferencing server, edit the `system.cfg` file on the server to add the outbound SIP proxy route:

1. Log in with craft login.
2. Type: **`vi /usr/ipcb/config/system.cfg`**
3. Go to the end of the file, press: SHIFT + g.
4. Type **`o`** to insert a new edit line.
5. For non-TLS servers, type: **`outboundProxyRoute=<sip:xxx.xx.xx.xx:5060;lr>`**
6. Replace **`xxx.xx.xx.xx`** with the IP of the sip proxy.
7. For TLS servers,type:
8. outboundProxyRoute=<sip:xxx.xx.xx.xx:5061;transport=tls;lr>
9. Press ESC to exit edit mode.
10. Save and quit. Type **`:wq!`**
11. Type: **`sudo lc restart ipcb`** to restart the ipcb processes.

Configuring Timer Settings

Configure the following two settings when connecting to Communication Manager.

Navigate to **system.cfg**.

In the `# Session Timers` section, ensure that the following values are set:

```
minSETimerValue=100
sessionRefreshTimer=1800
```

Important:

The `minSETimerValue` must be below the `minSETimerValue` default setting for when connecting to Communication Manager 4.0. If this value is not correctly configured, moderators cannot dial out from the conferencing server. The server generates `422 session too small` errors.

Configuring Communication Manager

Tip:

For additional information related to SIP trunking and signaling on the Communication Manager, refer to document number 555-245-206, *SIP Support in Avaya Communication Manager*.

Follow these steps to configure connectivity from Avaya Communication Manager to the S6200/S6800 Conferencing Servers.

1. Add a Node Name for the S6200/S6800 by entering **change node-name IP**. This value is the SES.
2. Select a CLAN or G700 for connection to the S6200/S6800. Note its node-name.
3. Add one or two signaling groups. For each Signaling Group, set the:
   - **Group Type** to “sip”
   - **Near-end Node Name** to value set in step 2, i.e. “CLAN”. This value is resolved through the hosts file on the Communication Manager.
   - **Far-end Node Name** to the same setting used in step 1, i.e. SES. This value is resolved through the hosts file on the Communication Manager.
   - **Near-end Listen Port** to “5061” for TLS or to “5060” for non-TLS.
   - **Far-end Listen Port** to “5061” for TLS or to “5060” for non-TLS.
   - **Far-end Network Region** to the codec set referred to in step 1.
   - Verify the **Transport Method** is set to “TLS” or “TCP”.

Signaling Group screen

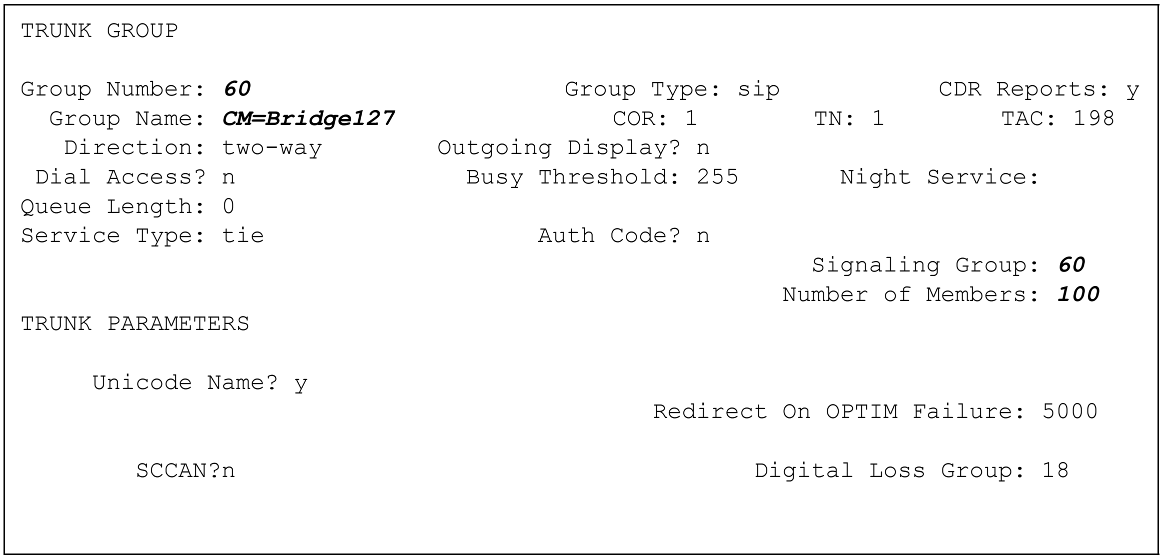
```
add signaling-group

 Group Number: 60       Group Type: sip
                        Transport Method: tls







Near-end Node Name: C-LAN1             Far-end Node Name: ses
Near-end Listen Port: 5061               Far-end Listen Port: 5061
       Far-end Network Region:
       Far-end Domain:

       Bypass If IP Threshold Exceeded? n


       DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
                                          IP Audio Hairpinning? y
 Session Establishment Timer(min): 3
```

4. Add one or two Trunk groups:
   - The **Group Number** is the Trunk Group Number.
   - The **Signaling Group** is the group associated with the Trunk Group.
   - The **Number of Members** for each group is the number of SIP channels supported on this trunk.

   Note:

   If the Number of Members is set to “0”, you will not be able to administer the members for this trunk group correctly.

Trunk Group screen

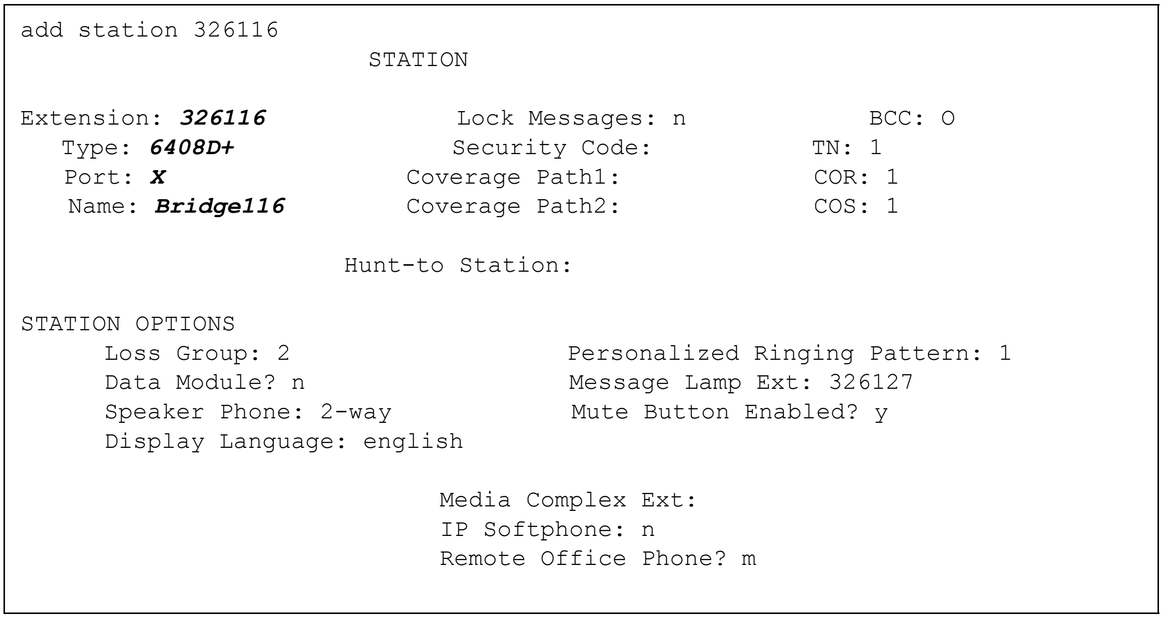


```
TRUNK GROUP

Group Number: 60                      Group Type: sip           CDR Reports: y
  Group Name: CM=Bridge127               COR: 1        TN: 1        TAC: 198
   Direction: two-way       Outgoing Display? n
 Dial Access? n               Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                                       Signaling Group: 60
                                                     Number of Members: 100
TRUNK PARAMETERS

     Unicode Name? y
                                            Redirect On OPTIM Failure: 5000

        SCCAN?n                                    Digital Loss Group: 18
```

5. Add a **Station Extension.** On the **Station screen**:

- Set the **Extension** to the entention number associated with the S6200/S6800.
- Set the **Type** to “6408D+”
- Set the **Port** to “X”.
- Set the **Name** to the bridge name associated with the server, i.e, “Bridge116” in the following figure.

Station screen



```
add station 326116
                        STATION

Extension: 326116             Lock Messages: n             BCC: 0
   Type: 6408D+               Security Code:           TN: 1
   Port: X                 Coverage Path1:             COR: 1
   Name: Bridge116         Coverage Path2:             COS: 1

                       Hunt-to Station:

STATION OPTIONS
      Loss Group: 2                   Personalized Ringing Pattern: 1
      Data Module? n                  Message Lamp Ext: 326127
      Speaker Phone: 2-way            Mute Button Enabled? y
      Display Language: english

                             Media Complex Ext:
                             IP Softphone: n
                             Remote Office Phone? m
```

6. Associate the station with the trunk.

- Set the **Application** to “OPS” for off-pbx extensions.
- Set the **Trunk Selection** to the trunk used for this extension, “60“in this example.
- On Page 2, set the **Mapping Mode** to “Both” to match all settings.

Appendix B: Integration with Communications Process Manager

This appendix describes the configuration settings that are required when Meeting Exchange is integrated with Avaya's Communications Process Manager.

Overview

Communications Process Manager initiates a Notify and Conference Server request to recipients when an external application sends an error trap. Recipients are requested to join an ad hoc exception conference on Meeting Exchange. When a notified user answers the phone, the service provides contextual information and asks the caller if they want to join the exception conference. Callers who accept are placed into the conference. The service attempts to first place moderators into the conference, then notifies other users via phone, email, or Short Messaging Service (SMS). If a moderator cannot be found, the service attempts to contact a moderator periodically until either a moderator joins the conference or the conference expires. The conference ends after all participants disconnect.

Note:

An Ad Hoc conference expires after 30 minutes if no one joins.

For more information about Communications Process Manager, see *Avaya Communications Process Manager Release 2.0 Administration and Configuration Guide*, Document 04-601159.

Accessing an Ad Hoc Conference

Callers can join an ad hoc conference in one of three ways:

- They can accept the invitation and be placed into conference
- They can respond through the Communications Process Manager User Portal and provide a callback number to have Communications Process Manager call them and place them into conference.
- They can call into Communications Process Manager to join the conference.

Process Table Configuration: (processTable.cfg)

Table 13 defines the required configurations in processTable.cfg for integration with Communications Process Manager.

Table 13: processTable.cfg with Communications Process Manager

process Name	ipcKey Number	ProcessExe	ipAddress	route	process Args
initipcb	110	noexecute	0.0.0.0		
bridget700	100	noexecute	0.0.0.0	dspEventmsDispatcher, netEvents/sipAgent	
comms Process	111	/usr/dcb/bin/serverComms	0.0.0.0		
sipAgent	101	/usr/dcb/bin/sipagent	0.0.0.0		
ms Dispatcher	102	/usr/dcb/bin/msdispatcher	0.0.0.0	netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer	
media Server	103	/usr/dcb/bin/softms	0.0.0.0	appEvents/msDispatcher,netEvents/msDispatcher	1
notifyService	113	noexecute	127.0.0.1:10235		
snmpAgent	120	noexecute	0.0.0.0		

System Configuration (system.cfg)

Verify the following settings are correct in system.cfg

```
MyListener=sips:6000@135.35.53.50:5061;transport=tls

#if this setting is populated will Overwrite the contact field in
responses
respContact=sip:6000@135.35.53.50:5061;transport=tls

#Adhoc conference parameters
AdhocConferenceURIPattern=<sip:adhocDirect$1;5061@$2;transport=tls>
AdhocMinPortsAvailable=20
AdhocDefaultConferenceSize=5
#Sipping Notification Interval (1-5)
sippingNotification=1

#Set if outbound proxy is configured
outboundProxyRoute=<sip:135.64.29.108:5061;transport=tls;lr>
```

Conference Profiles (conferenceProfiles.cfg)

The bridgeTranslator uses conferenceProfiles.cfg to map conference profiles to the conferencing server. The configurable parameters are:

Table 14: conferenceProfiles.cfg integration

Parameter	Definition	Options
ModHang	Moderator Hang Up	on/off
VMailFilter	Voice Mail Filter	on/off
EntryExitAnn	Entry/Exit Announcement	on/off

Verify the following conference profile settings:

Table 15: Conference Profile Settings

FactoryName	ModHang	VMailFilter	EntryExitAnn
ReservationSetup	on	on	on
ReservationSetupNoVMB	on	off	off

URItoTelnum.tab

The default configuration for adhocDirect in URItoTelnum.tab allows for dialing out to ad hoc conference participants only:

Table 16: Default ad hoc Configuration

TelnumPattern	TelnumConversion	comment
"*adhocDirect@*"	$2	diamond_adhoc_conf_support

To enable participants to dial in to an ad hoc conference via SIP INVITE:

1. Change TelnumConversion for adhocDirect to include a DNIS number similar to 5555$2.
2. Replace 5555 with a valid DNIS entry that has been configured in with a function of DIRECT.

SES Proxy

The SES Proxy should include a pre-defined host map with the following entries routed to the conferencing server:

- "sip:ReservationSetup*"
- "sips:ReservationSetup*"
- "sip:AdhocDirect*"
- "sips:AdhocDirect*"

For detailed instructions on configuring an SES Proxy with Meeting Exchange, see SIP Enablement Server (SES) and Meeting Exchange on page 45

Tip:

There is no requirement to define proxies on Meeting Exchange for registration.

Ad hoc Conference Properties

The following properties define an ad hoc conference as provided on the conferencing server:

- A SIP invite from Communications Process Manager creates a new reservation with a passcode for the ad hoc conference
- The conference is valid immediately after the reservation is created
- The reservation is valid for 24 hours as long as it is active
- The conference instance will be removed if no callers join within 30 minutes
- Ad hoc conferences use on demand ports

Security

To provide a secure conference instance, Meeting Exchange is configured to listen only on Transport Layer Security (TLS) traffic. The current deployment of Communications Process Manager, SES, and Meeting Exchange includes certificates signed by Avaya Certificate Authority.

A SIP Refer is allowed only if the P-Asserted-Identity SIP header of Communications Process Manager matches the same header in the invite to the conferencing server.

NotificationCtrlServer

NotificationCtrlServer is a new process (/usr/dcb/bin) to support conference event subscription through SIP. It is not required to be running and if it is not, SIP Subscribe messages are expected. Currently this process always starts when the bridge starts up and logs in as the first operator through BCAPI.

It receives Subscribe messages from the SIP Agent through commsProcess and sends Notify messages through the SIP Agent with an xml body.

Currently participant entry and exit notifications are sent once every "notification interval", with a default setting of 1 second.

Troubleshooting

Set the following debug logging to troubleshoot the SIP Agent and notificationCtrlServer when working with Communications Process Manager:

Sip Agent

- ipcbdbg f sipAgent t
- ipcbdbg f eventHandler t

The output logs are in /usr3/ipcb/log/debug.log

notificationCtrlServer

1. Go to: /usr/dcb/bin/notificationCtrlServer/MXLog.xml
2. Locate: com.avaya.conferencing.notificationctrlserver
   - Change the priority to "debug"
3. Restart the process

The output logs are in /usr3/ipcb/log/notificationCtrlServer.log

Appendix C: Configuration Files

This appendix describes the different configuration files that are required for the various S6200/S6800 Conferencing Servers media server configurations.

Process Table Configuration: processTable.cfg

The S6200/S6800 Conferencing Servers uses the process table to identify the location of the various processes that run on the system. The media server will not function unless the process table contains the appropriate information. This information is stored in /usr/ipcb/config to a file named, processTable.cfg.

To manually enter configuration settings for processTable.cfg, use the templates provided for each solution. To view the available templates, go to:

```
/usr/ipcb/config
```

To edit processTable.cfg settings for a standalone S6200 solution enter:

```
vi processTable_singleMS.cfg
```

To edit the settings for a solution with multiple S6200 servers, enter one of the two following commands, one for a solution with failover, one for a solution with no failover.

```
vi processTable_pyramid_appServerFailOver.cfg
```

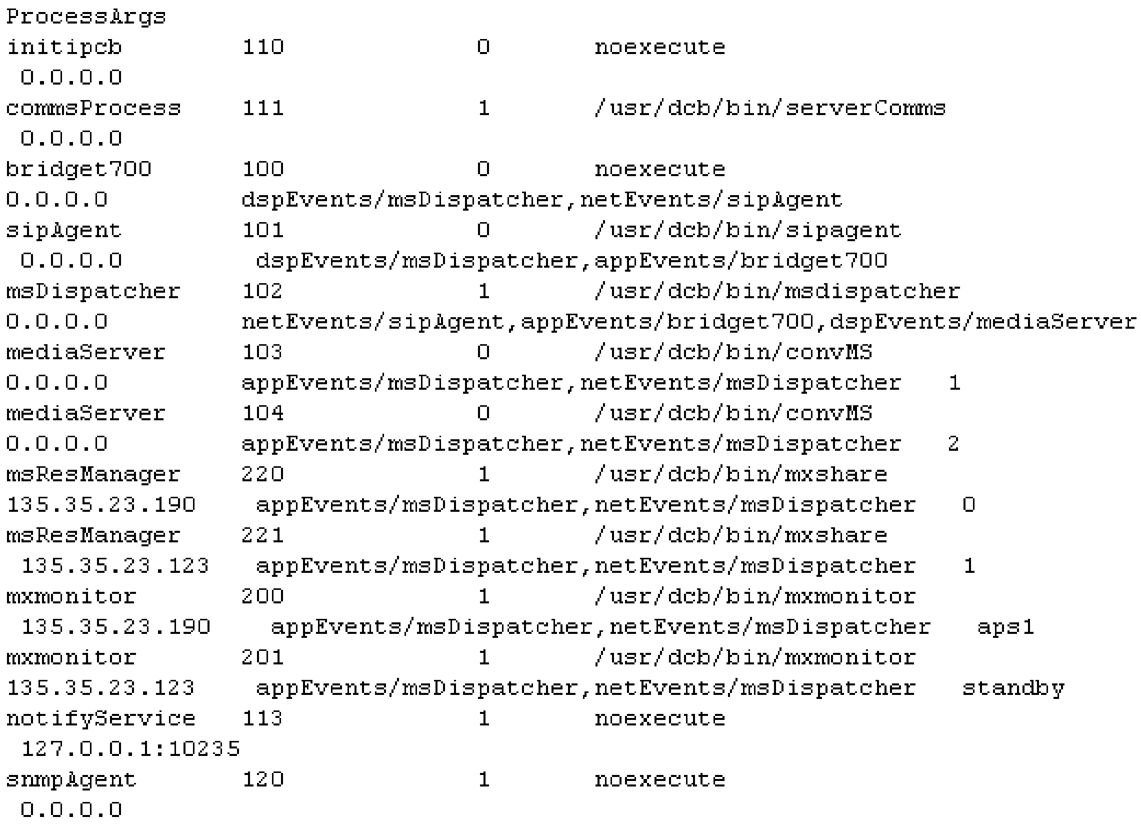
```
vi processTable_pyramid_noappServerFailover.cfg
```

To edit the settings for a solution with the S6800 media server, enter:

```
vi processTableConvedia.cfg
```

Settings for S6800 with MXShare and MXMonitor

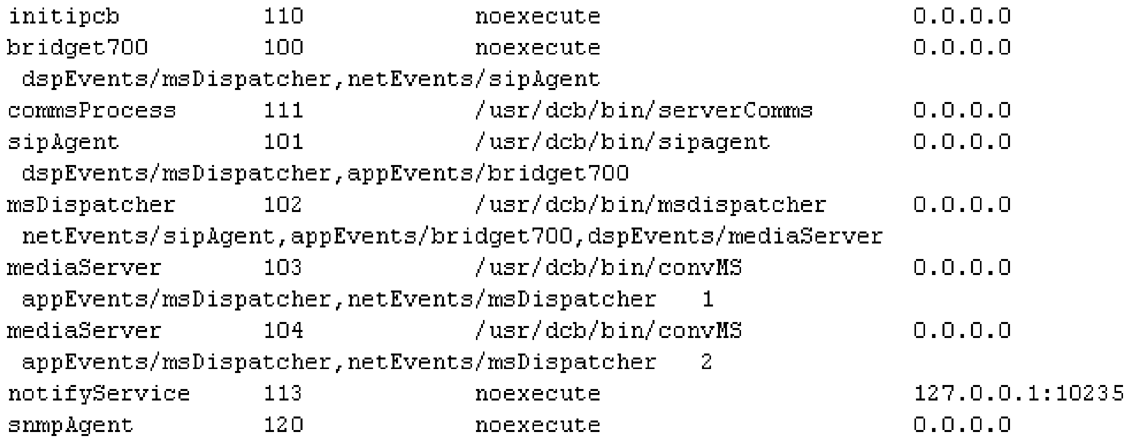
The following file contains IP Addresses of 0.0.0.0, which can be used as the local IP address of the Application Server. This configuration file can be edited to work on all Application Servers by adding the full IP Addresses for MXShare and MXMonitor. These settings are located at the bottom of the file.



```
ProcessArgs
initipcb        110             0       noexecute
 0.0.0.0
commsProcess    111             1       /usr/dcb/bin/serverComms
 0.0.0.0
bridget700      100             0       noexecute
0.0.0.0         dspEvents/msDispatcher,netEvents/sipAgent
sipAgent        101             0       /usr/dcb/bin/sipagent
 0.0.0.0         dspEvents/msDispatcher,appEvents/bridget700
msDispatcher    102             1       /usr/dcb/bin/msdispatcher
0.0.0.0         netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
mediaServer     103             0       /usr/dcb/bin/convMS
0.0.0.0         appEvents/msDispatcher,netEvents/msDispatcher   1
mediaServer     104             0       /usr/dcb/bin/convMS
0.0.0.0         appEvents/msDispatcher,netEvents/msDispatcher   2
msResManager    220             1       /usr/dcb/bin/mxshare
135.35.23.190    appEvents/msDispatcher,netEvents/msDispatcher   0
msResManager    221             1       /usr/dcb/bin/mxshare
 135.35.23.123   appEvents/msDispatcher,netEvents/msDispatcher   1
mxmonitor       200             1       /usr/dcb/bin/mxmonitor
 135.35.23.190    appEvents/msDispatcher,netEvents/msDispatcher   aps1
mxmonitor       201             1       /usr/dcb/bin/mxmonitor
135.35.23.123    appEvents/msDispatcher,netEvents/msDispatcher   standby
notifyService   113             1       noexecute
 127.0.0.1:10235
snmpAgent       120             1       noexecute
 0.0.0.0
```

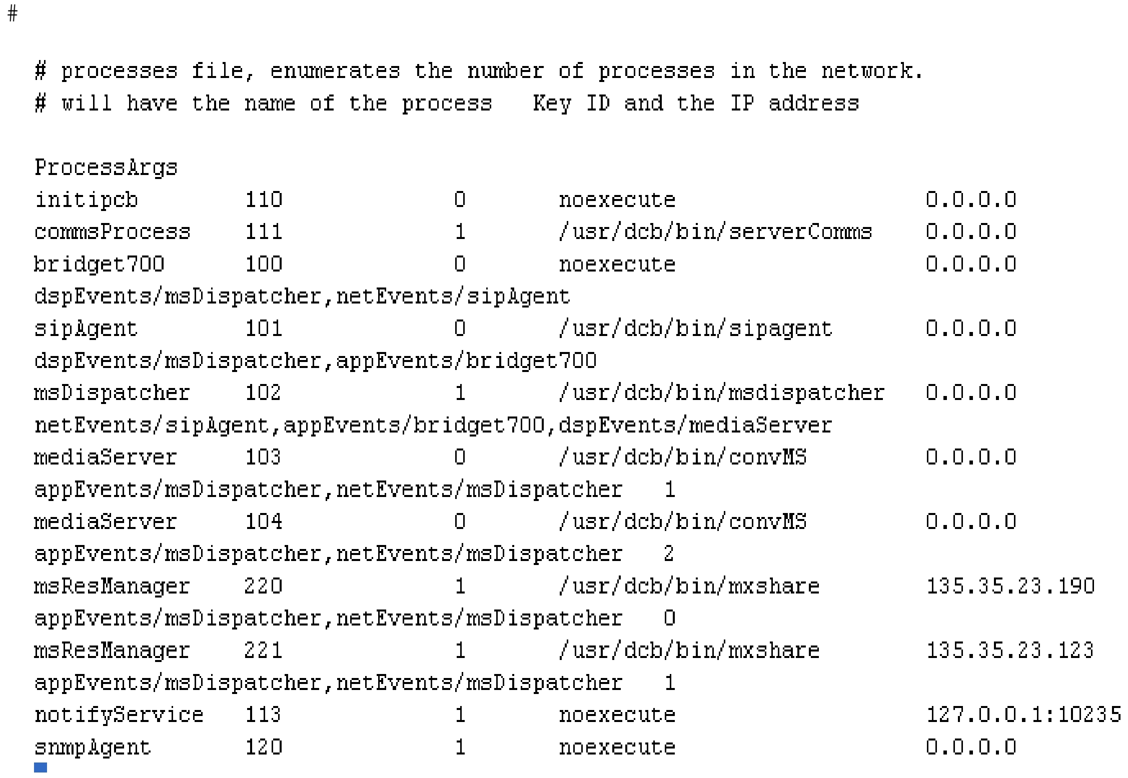
Settings for S6800 without MXShare/MXMonitor

The settings in this example file configure a system with two MPC cards with no MXShare or MXMonitor. Some lines in the following example wrap for clarity



```
initipcb          110            noexecute                       0.0.0.0
bridget700        100            noexecute                       0.0.0.0
 dspEvents/msDispatcher,netEvents/sipAgent
commsProcess      111            /usr/dcb/bin/serverComms        0.0.0.0
sipAgent          101            /usr/dcb/bin/sipagent           0.0.0.0
 dspEvents/msDispatcher,appEvents/bridget700
msDispatcher      102            /usr/dcb/bin/msdispatcher       0.0.0.0
 netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
mediaServer       103            /usr/dcb/bin/convMS             0.0.0.0
 appEvents/msDispatcher,netEvents/msDispatcher   1
mediaServer       104            /usr/dcb/bin/convMS             0.0.0.0
 appEvents/msDispatcher,netEvents/msDispatcher   2
notifyService     113            noexecute                       127.0.0.1:10235
snmpAgent         120            noexecute                       0.0.0.0
```

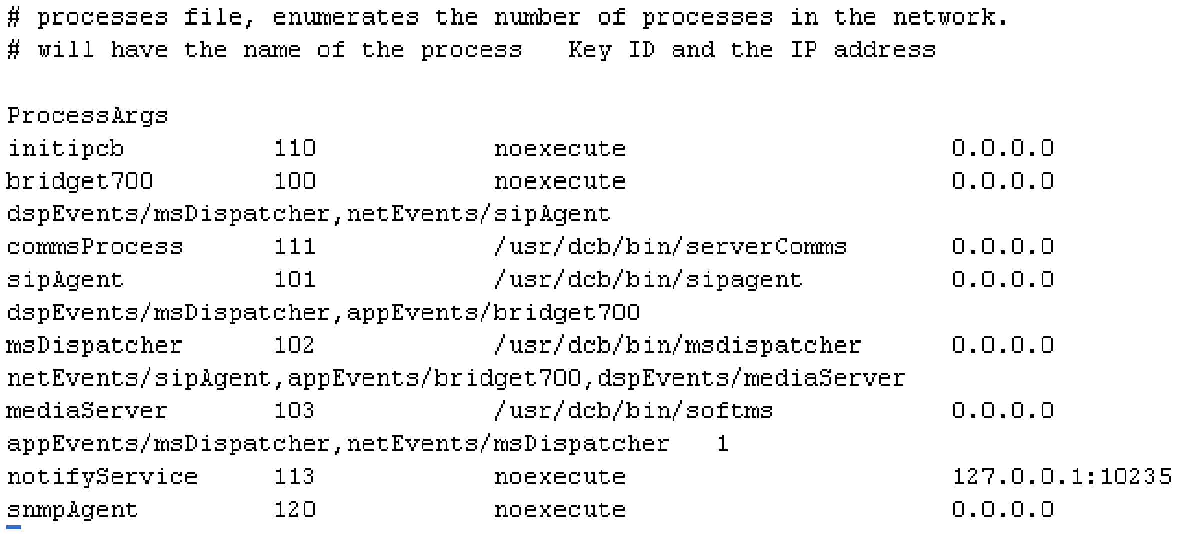
Settings for MxShare without MxMonitor



```
#

 # processes file, enumerates the number of processes in the network.
 # will have the name of the process   Key ID and the IP address

 ProcessArgs
 initipcb        110             0       noexecute                   0.0.0.0
 commsProcess    111             1       /usr/dcb/bin/serverComms    0.0.0.0
 bridget700      100             0       noexecute                   0.0.0.0
 dspEvents/msDispatcher,netEvents/sipAgent
 sipAgent        101             0       /usr/dcb/bin/sipagent       0.0.0.0
 dspEvents/msDispatcher,appEvents/bridget700
 msDispatcher    102             1       /usr/dcb/bin/msdispatcher   0.0.0.0
 netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
 mediaServer     103             0       /usr/dcb/bin/convMS         0.0.0.0
 appEvents/msDispatcher,netEvents/msDispatcher   1
 mediaServer     104             0       /usr/dcb/bin/convMS         0.0.0.0
 appEvents/msDispatcher,netEvents/msDispatcher   2
 msResManager    220             1       /usr/dcb/bin/mxshare        135.35.23.190
 appEvents/msDispatcher,netEvents/msDispatcher   0
 msResManager    221             1       /usr/dcb/bin/mxshare        135.35.23.123
 appEvents/msDispatcher,netEvents/msDispatcher   1
 notifyService   113             1       noexecute                   127.0.0.1:10235
 snmpAgent       120             1       noexecute                   0.0.0.0
```

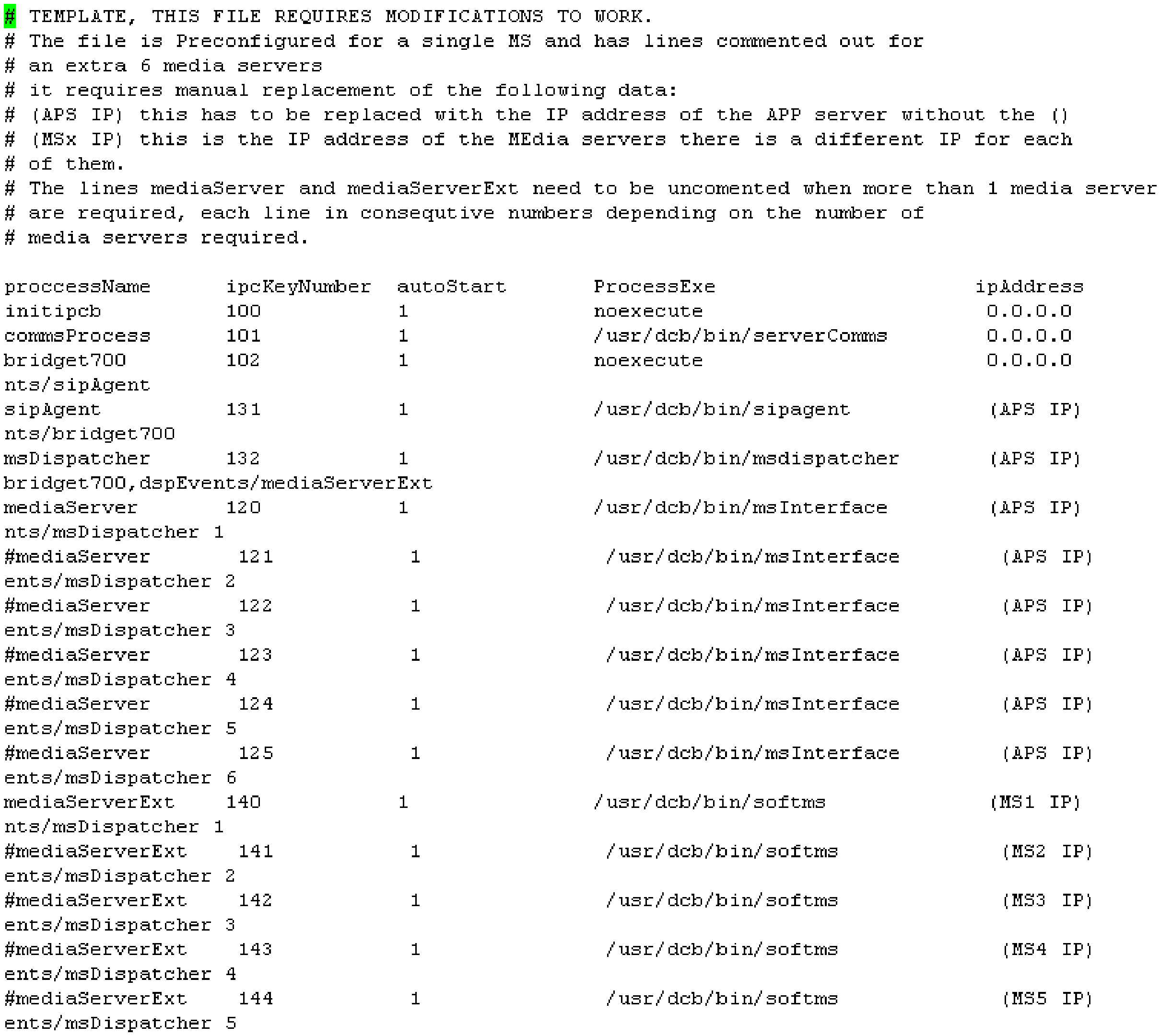
Settings for the standalone S6200

The file below shows the configuration for softms, the application media server. No external hardware is required.



```
# processes file, enumerates the number of processes in the network.
# will have the name of the process   Key ID and the IP address

ProcessArgs
initipcb          110            noexecute                      0.0.0.0
bridget700        100            noexecute                      0.0.0.0
dspEvents/msDispatcher,netEvents/sipAgent
commsProcess      111            /usr/dcb/bin/serverComms       0.0.0.0
sipAgent          101            /usr/dcb/bin/sipagent          0.0.0.0
dspEvents/msDispatcher,appEvents/bridget700
msDispatcher      102            /usr/dcb/bin/msdispatcher      0.0.0.0
netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
mediaServer       103            /usr/dcb/bin/softms            0.0.0.0
appEvents/msDispatcher,netEvents/msDispatcher   1
notifyService     113            noexecute                      127.0.0.1:10235
snmpAgent         120            noexecute                      0.0.0.0
```

Settings for the multiple S6200 solution



```
# TEMPLATE, THIS FILE REQUIRES MODIFICATIONS TO WORK.
# The file is Preconfigured for a single MS and has lines commented out for
# an extra 6 media servers
# it requires manual replacement of the following data:
# (APS IP) this has to be replaced with the IP address of the APP server without the ()
# (MSx IP) this is the IP address of the MEdia servers there is a different IP for each
# of them.
# The lines mediaServer and mediaServerExt need to be uncomented when more than 1 media server
# are required, each line in consequtive numbers depending on the number of
# media servers required.

proccessName      ipcKeyNumber  autoStart       ProcessExe                     ipAddress
initipcb          100           1               noexecute                       0.0.0.0
commsProcess      101           1               /usr/dcb/bin/serverComms        0.0.0.0
bridget700        102           1               noexecute                       0.0.0.0
nts/sipAgent
sipAgent          131           1               /usr/dcb/bin/sipagent           (APS IP)
nts/bridget700
msDispatcher      132           1               /usr/dcb/bin/msdispatcher       (APS IP)
bridget700,dspEvents/mediaServerExt
mediaServer       120           1               /usr/dcb/bin/msInterface        (APS IP)
nts/msDispatcher 1
#mediaServer       121           1               /usr/dcb/bin/msInterface        (APS IP)
ents/msDispatcher 2
#mediaServer       122           1               /usr/dcb/bin/msInterface        (APS IP)
ents/msDispatcher 3
#mediaServer       123           1               /usr/dcb/bin/msInterface        (APS IP)
ents/msDispatcher 4
#mediaServer       124           1               /usr/dcb/bin/msInterface        (APS IP)
ents/msDispatcher 5
#mediaServer       125           1               /usr/dcb/bin/msInterface        (APS IP)
ents/msDispatcher 6
mediaServerExt    140           1               /usr/dcb/bin/softms             (MS1 IP)
nts/msDispatcher 1
#mediaServerExt    141           1               /usr/dcb/bin/softms             (MS2 IP)
ents/msDispatcher 2
#mediaServerExt    142           1               /usr/dcb/bin/softms             (MS3 IP)
ents/msDispatcher 3
#mediaServerExt    143           1               /usr/dcb/bin/softms             (MS4 IP)
ents/msDispatcher 4
#mediaServerExt    144           1               /usr/dcb/bin/softms             (MS5 IP)
ents/msDispatcher 5
```

System Configuration File: system.cfg

The system configuration is stored in the system.cfg file located in the /usr/ipcb/config directory. Use this file to set the IP address of the application server and the media server priority. The media server priority depends on the application server.

Settings for S6800 with MXShare

The Media Server Priority depends on the Application Server.

Application Server	Explanation
APS1	The application server uses the first two resources available in the pool
APS2	APS 1 uses the first two available resources, so this application server uses the next two available resources.

The following is an example:

```
##############################################################################
# DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#1. Change the "IPAddress" to the IP Address of this machine
#2. Change the "MyListener"
#3. Change the "MediaServerPriority" to 1 if APS1 - Takes MPC 1&2
#4. Change "numMediaServers" to 2 so it will take 2 MPC resources from the pool of
available recources
##############################################################################
# ip address of the server
IPAddress=10.20.30.1
# request we will be listening to
MyListener=sip:6000@10.20.30.1
# if this setting is populated will Overwrite the contact field in responses
respContact=
MaxChannelCount=2000
# diff serv this value will appear on the TOS field of the IP packet
DiffServTOSValue=0
# vlan value
EthernetVlanValue=0
#refresh timer settings, to refresh the sessions that are connected
#recomended value is to set both at 180 3 minutes refreshes
sessionRefreshTimerValue=1800
minSETimerValue=1800
# Not used for Unixware MeetingXchange
MaxMeetingCount=400
MaxConferenceCount=500
MaxOperatorCount=10
# configuration for the media sharing process to know how many media

# MXShare
MediaServerPriority=1
numMediaServers=2
```

Tip:

In addition, set up the MPCs in `mediaServerInterface.cfg`. In the example below. The example has two as shown in the numMediaServer values.

```
# SCC-1
NFSServerIPAddress=135.35.23.190
# MPC-2
MediaServerIP_1=135.35.23.92
MediaServerInterfaceSipListenPort_1=5050
# MPC-3
MediaServerIP_2=135.35.23.95
MediaServerInterfaceSipListenPort_2=5040
```

For each server, list the NFS Server IP, the Media Server IP, the MPC number assigned to the media server and the and the Listen Port for the media server as shown above.

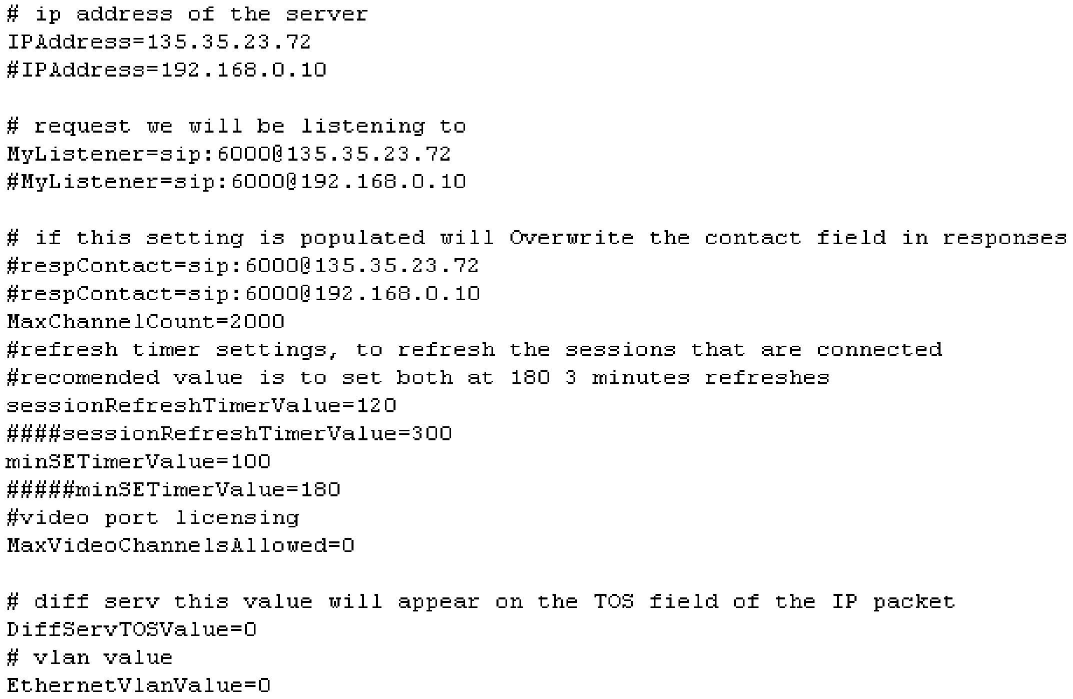
Settings for the standalone S6200

A system configured as an S6200 (application server), requires that the IP Address values be edited in the configuration file.

```
##############################################################################
# ip address of the server
IPAddress=10.20.30.1
# request we will be listening to
MyListener=sip:6000@10.20.30.1
# if this setting is populated will Overwrite the contact field in responses
respContact=
MaxChannelCount=600
# diff serv this value will appear on the TOS field of the IP packet
DiffServTOSValue=0
# vlan value
EthernetVlanValue=0
#refresh timer settings, to refresh the sessions that are connected
#recomended value is to set both at 180 3 minutes refreshes
sessionRefreshTimerValue=1800
minSETimerValue=1800
# Not used for Unixware MeetingXchange
MaxMeetingCount=400
MaxConferenceCount=500
MaxOperatorCount=10
```

Setting for the multiple S6200 solution

The following is an example of the system.cfg file for a solution with separate S6200 application and media servers.



```
# ip address of the server
IPAddress=135.35.23.72
#IPAddress=192.168.0.10

# request we will be listening to
MyListener=sip:6000@135.35.23.72
#MyListener=sip:6000@192.168.0.10

# if this setting is populated will Overwrite the contact field in responses
#respContact=sip:6000@135.35.23.72
#respContact=sip:6000@192.168.0.10
MaxChannelCount=2000
#refresh timer settings, to refresh the sessions that are connected
#recomended value is to set both at 180 3 minutes refreshes
sessionRefreshTimerValue=120
####sessionRefreshTimerValue=300
minSETimerValue=100
#####minSETimerValue=180
#video port licensing
MaxVideoChannelsAllowed=0

# diff serv this value will appear on the TOS field of the IP packet
DiffServTOSValue=0
# vlan value
EthernetVlanValue=0
```

Media Server Interface Configuration: Video Settings

Meeting Exchange®provides the capability for system wide video conferencing parameters. These parameters are negotiated with connecting video endpoints for incoming and outgoing video calls. Set video parameters in the video section of mediaServerInterface.cfg:

Table 17: Video Settings

Field	Definition	Setting
EnableVideoSupport	Defines whether video is available for the server	0= No video (default) 1= Video enabled
VideoSI	Video switching interval	1-10 seconds 2 = default
VideoSpeakerSees	Which speaker the video shows to the end user	current or previous previous = default
VideoSize	Support video resolution	CIF or QCIF CIF = default
VideoBandwidth	Supported codec size (kbit/s)	128,192, 256, 384, 512, 768 384 = default
VideoMPI	Minimum picture interval - the minimum time between encoding of pictures	1-32 4 = default

Set VideoSI (video switching interval) to the minimum number of seconds required for the video to switch to the active speaker. If the last switch happened 'SI' seconds ago and the active speaker has been speaking since then, the video switch will happen immediately after the active speaker switches. If the last video switch happened less then 'SI' seconds ago, the media server will wait at least 'SI' seconds before another video switch can occur.

The file is stored in /usr/ipcb/config on each application server. Each application server in ‘mxshare uses the same file settings with the exception of the NFS Server IP Address.

Note:

To see the video port capacity per MPC for your supported codec, see Table 5: Video Channel Limits with CMS 6000 on page 42

Hosts File Configuration

The hosts file is stored in /etc. Edit the hosts file to provide settings that allow the server to communicate with the CRS, other Application Servers, and Convedia Resources.

Tip:

The CRS host name is also referenced in the chdbased.reg file for communication. Put this value in the /etc/hosts file and verify that you can ping the address name (i.e. `ping autocrs`)

Important:

Verify to specify the fully qualified domain name for each server.

```
[crsdatasource]
installed=true
name=crsdatasource
version=0.1
address=autocrs
port=5050
user=ACS3
cabinet="3"

[sroot@mxsite1 admin]# pg /etc/hosts
127.0.0.1       localhost
#BRIDGES
135.35.23.123    auto-50.usae.avaya.com auto-50
#MPC SITE 1
135.35.23.92    mpc2.com mpc2
135.35.23.95    mpc3.com mpc3
#CRS - WITH FAILOVER ENTRIES
135.35.70.115   crstwo.usae.avaya.com crsmike
135.35.23.70    autocrs.usae.avaya.com autocrs
#4.1 MULTISITE NETWORK
135.35.23.102   crsmultisite1a.usae.avaya.com crsmultisite1a
135.35.24.102   crsmultisite2.usae.avaya.com crsmultisite2
135.35.25.102   crsmultisite3a.usae.avaya.com crsmultisite3a
135.35.23.107   crsmultisite1a.usae.avaya.com crsmultiste1a
135.35.23.107   newyorkbkcrs1.usae.avaya.com newyorkbkcrs1
# BEGIN - Edits by f_fixup_csHostsFile Thu Mar 15 17:31:12 EDT 2007
135.35.23.190   mxsite1.usae.avaya.com  mxsite1
192.11.13.6     serviceLan.usae.avaya.com       serviceLan
# END - Edits by f_fixup_csHostsFile
```

Modifying DTMF Input Settings (sFlowDigits.reg

The system accepts various DTMF input. Conferees and moderators press predetermined digits on their touch-tone telephones to use specific features. Figure 10 shows the standard settings for the DTMF input when the system is configured for the default call flow (sFlowDigits.reg).

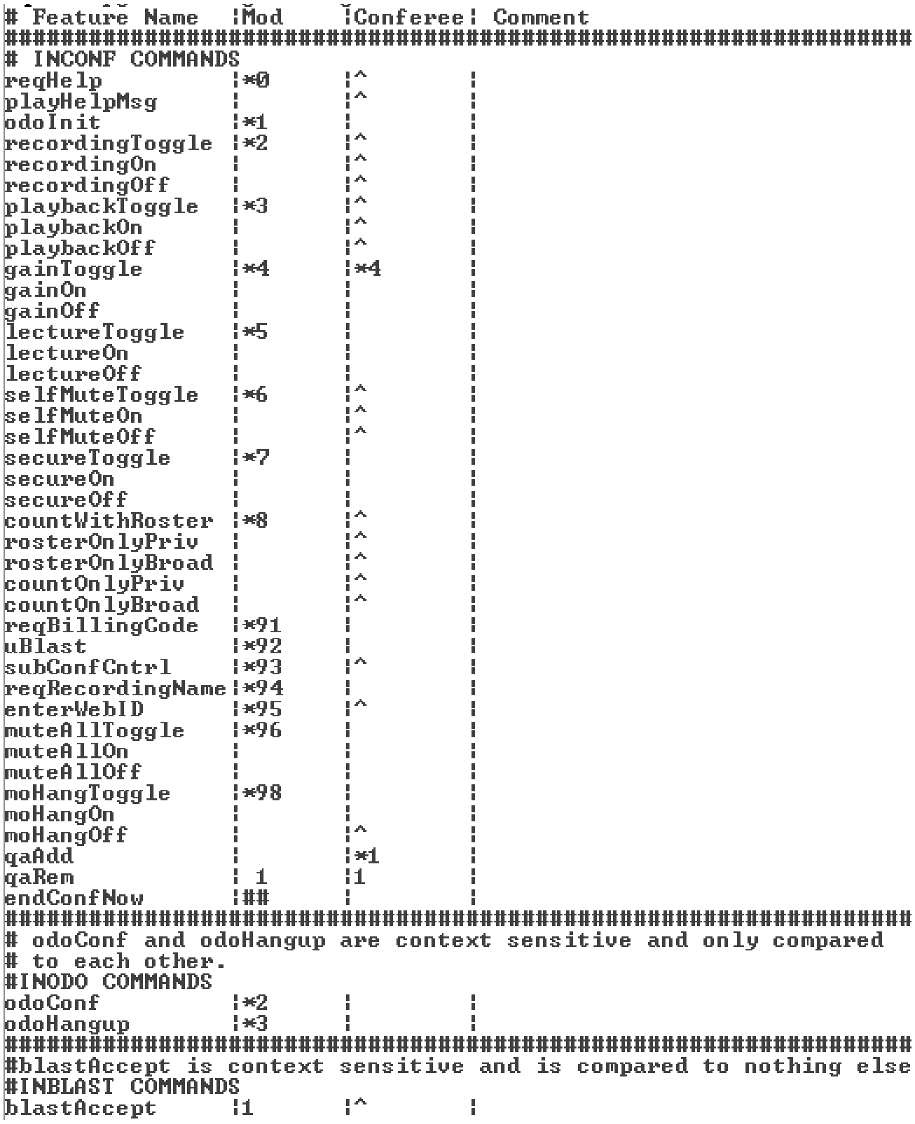
Note:

sFlowDigits.reg replaces digits.txt

If a customer requires different settings, use the following guidelines to modify the Command Initiation String (CIS) for both moderators and conferees:

- CIS can be from 0 to 4 digits in length
- Digits accepted: 0123456789*aAbBcCdD
- Sign ^ in conferee column indicates the command string is the same as for moderator
- If no digits are present, corresponding command/feature is disabled in sFlow
- Command names are case sensitive and may be used multiple times with different CIS
- White space, and # sign and comments are optional
- Two ’pipes’ (|) must be present
- The system checks for duplication of digits.

Figure 10: sFlowDigits.reg



```
# Feature Name  ¦Mod     ¦Conferee¦ Comment
#################################################################
# INCONF COMMANDS
reqHelp         ¦*0      ¦^       ¦
playHelpMsg     ¦        ¦^       ¦
odoInit         ¦*1      ¦        ¦
recordingToggle ¦*2      ¦^       ¦
recordingOn     ¦        ¦^       ¦
recordingOff    ¦        ¦^       ¦
playbackToggle  ¦*3      ¦^       ¦
playbackOn      ¦        ¦^       ¦
playbackOff     ¦        ¦^       ¦
gainToggle      ¦*4      ¦*4      ¦
gainOn          ¦        ¦        ¦
gainOff         ¦        ¦        ¦
lectureToggle   ¦*5      ¦        ¦
lectureOn       ¦        ¦        ¦
lectureOff      ¦        ¦        ¦
selfMuteToggle  ¦*6      ¦^       ¦
selfMuteOn      ¦        ¦^       ¦
selfMuteOff     ¦        ¦^       ¦
secureToggle    ¦*7      ¦        ¦
secureOn        ¦        ¦        ¦
secureOff       ¦        ¦        ¦
countWithRoster ¦*8      ¦^       ¦
rosterOnlyPriv  ¦        ¦^       ¦
rosterOnlyBroad ¦        ¦^       ¦
countOnlyPriv   ¦        ¦^       ¦
countOnlyBroad  ¦        ¦^       ¦
reqBillingCode  ¦*91     ¦        ¦
uBlast          ¦*92     ¦        ¦
subConfCntrl    ¦*93     ¦^       ¦
reqRecordingName¦*94     ¦        ¦
enterWebID      ¦*95     ¦^       ¦
muteAllToggle   ¦*96     ¦        ¦
muteAllOn       ¦        ¦        ¦
muteAllOff      ¦        ¦        ¦
moHangToggle    ¦*98     ¦        ¦
moHangOn        ¦        ¦        ¦
moHangOff       ¦        ¦^       ¦
qaAdd           ¦        ¦*1      ¦
qaRem           ¦ 1      ¦1       ¦
endConfNow      ¦##      ¦        ¦
#################################################################
# odoConf and odoHangup are context sensitive and only compared
# to each other.
#INODO COMMANDS
odoConf         ¦*2      ¦        ¦
odoHangup       ¦*3      ¦        ¦
#################################################################
#blastAccept is context sensitive and is compared to nothing else
#INBLAST COMMANDS
blastAccept     ¦1       ¦^       ¦
```

Steps to change command initiation strings in sFlowDigits.reg:

1. From the root prompt, open the sFlowDigits.reg file with the vi text editor.

   `vi /usr/dcb/dbase/admin/sFlowDigits.reg`

   The file includes the following default settings:

   *0 - Operator Help

   *1 - Initiate ODO dialout

   - *2 -Return to call with dialed line (as a result of ODO)

- *3 -Return to call without dialed line (as a result of ODO)

*2 - Toggle recording

*3 - Toggle playback

*4 - Toggle gain

*5 - Toggle lecture

*6 - Toggle self mute

*7 - Toggle security

*8 - Count with roster

*91 -Billing code prompt

*92 -Initiate uBlast

*93 -Subconference

*94 -Request recording file name

*95 -Enter WebId

*96 -Toggle mute all

*98 -Toggle moderator hang up

## -End conference

2. Modify the settings as required.
3. Save your changes and close the file.

```
wq!
```

4. Reboot the system to implement the changes.

Use the following utility to verify the changes:

```
cd /usr/dcb/bin
chksflowdigits
```

Tip:

System will run with valid command initiation strings and ignore ambiguous or duplicate strings.

Modifying DTMF Input Settings for Flex (flexflow_cfg.reg)

Systems configured for Flex call flows can be configured to accept various DTMF input to use special conference features. Modifications are made to the flexflow_cfg.reg file.

Note:

If a function is missing, or has an empty DTMF sequence, that function is disabled.

Follow this procedure to configure the DTMF:

Edit the flexflow_cfg.reg file with the vi text editor.

```
vi /usr/dcb/dbase/admin/flexflow_cfg.reg
```

The system displays the file, which contains two sections, InConference and AccountManagement. The sections may be in any order. Within each section, each line corresponds to a DTMF command. For example:

```
<function name> = <DTMF sequence to invoke>
```

An example file with default settings follows:

```
[InConference]
OperatorConference      = *0
OperatorIndividual      = 00
DialOut                 = *1
ConferenceRecord        = *2
ChangeEntryExit         = *3
LockConference          = *4
UnlockConference        = *5
MuteIndividual          = *6
UnmuteIndividual        = *7
ConferenceContinuation  = *8
PrivateRollCall         = *9
MuteGroup               = ##
UnmuteGroup             = 99
ParticipantCount        = *#
ListKeypadCommands      = **
DTMFConferenceHangup    = 77
GoToSubParent           = 93
PlayRecordFileNumber    = 94

[AccountManagement]
ChangeLeaderPIN         = 1
NameRecTones            = 2
QuickStart              = 3
AutoContinuation        = 4
Describe                = 9
```

5. Save the file.

Tip:

Use the /usr/dcb/bin/flexdigits utility to test the flexflow_cfg.reg file before putting it on a live bridge. This program will parse the input file, reporting any errors or warnings. To run the utility, use the name of the file as an argument. For example:

```
/usr/dcb/bin/flexdigits testFlexFlow_cfg.ini
```

MxMonitor for use with Convedia and MXShare/MXMonitor

Stored in /usr/ipcb/config, the mxmonitor.reg file contains the configuration information for the Application Servers and the Standby. This file is only required when an application server uses the mxMonitor

```
################################################################################
#    DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#1.List all systems in our [mxworkgroup]. Delete any entries not needed
#2.For [apsx] change the "cabinet=" value to the Bridge Ref number of the
corresponding AppServer
#3.Duplicate for all APS and STBY with their corresponding Bridge Ref number listed
on CRS Front End
################################################################################
[mxworkgroup]
aps1
standby
 [mxconfig]
trace=false
sipsource=crs
sipupdateperiod=60000
reqtimeout=300000
checkstatustimer=60000
numstatusrequests=2
[aps1]
process=aps1
role=active
cabinet=1
[aps2]
[standby]
process=standby
role=standby
cabinet=4
```

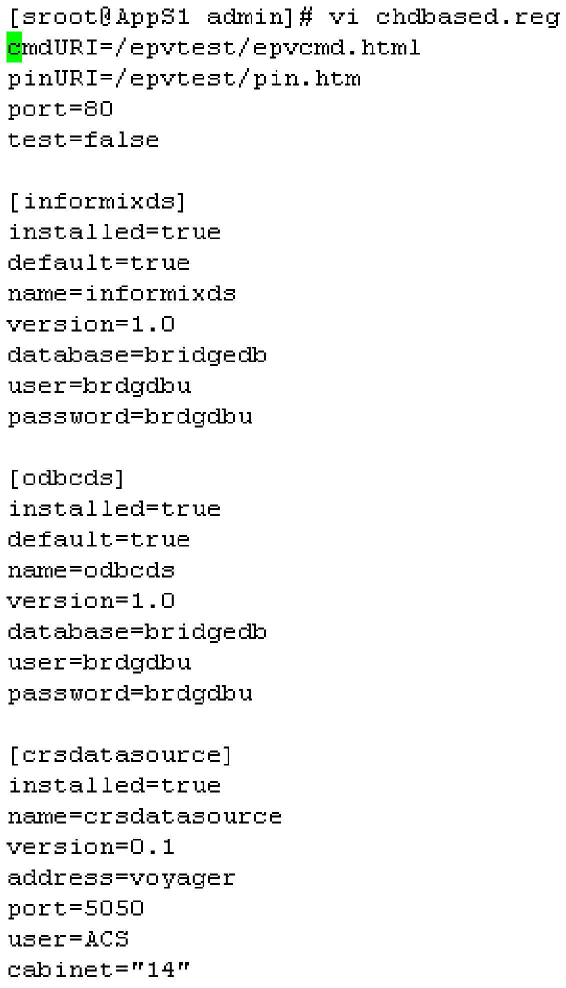
chdbased.reg settings for S6800 and MXShare/MXMonitor

When the mxMonitor is used on an application server, edit the chdbased.reg file to include the crsdatasource. Edit the settings in the crsdatasource to reflect the cabinet reference value from the CRS Front End. This file is located in /usr/dcb/dbase/admin.

```
# DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#1. Please change the "cabinet" value under [crsdatasource] to the
# actual CABINET ref value seen for this bridge IP address on the CRS Front End >
# System Administration Cabinets.
#2. Also make sure there is a username/password of
# ACS/acs System Administration > Logins
#3. Change the "address" to the host name of the CRS Server
##############################################################################
[datasources]
nullds
xmldatasource
odbcds
crsdatasource

[HKEY_DCB_ROOT.chdbased]
keepaliveperiod=30000
datasource=informixds
crsextend=false

[xmldatasource]
version=1.0
bridgeid=spectel10
installed=true
name=xmldatasource
address=localhost
URI=/epvtest
pingURI=/epvtest/ping.htm
port=80
test=false

[informixds]
installed=true
default=true
name=informixds
version=1.0
database=bridgedb
user=brdgdbu
password=brdgdbu
[odbcds]
installed=true
default=true
name=odbcds
version=1.0
database=bridgedb
user=brdgdbu
password=brdgdbu
```

```
[crsdatasource]
installed=true
name=crsdatasource
version=0.1
address=CRS
port=5050
user=ACS
cabinet="1"
```

Chdbased.reg settings for multiple 6200 solution



```
[sroot@AppS1 admin]# vi chdbased.reg
cmdURI=/epvtest/epvcmd.html
pinURI=/epvtest/pin.htm
port=80
test=false

[informixds]
installed=true
default=true
name=informixds
version=1.0
database=bridgedb
user=brdgdbu
password=brdgdbu

[odbcds]
installed=true
default=true
name=odbcds
version=1.0
database=bridgedb
user=brdgdbu
password=brdgdbu

[crsdatasource]
installed=true
name=crsdatasource
version=0.1
address=voyager
port=5050
user=ACS
cabinet="14"
```

Translation Table Configuration for Operator Dial In

Two files support operator dial in: telnumToUri.tab and uriToTelnum. Changes to these files required to support operator dial in are described in the following sections.

telnumToUri.tab

When operator dial in will be used on the system, edit the telnumToUri.tab stored in /usr/ipcb/config. No particular values are needed for the Operator Dial In feature.

Note:

Refer to Telephone number to URI translation table on page 49 for additional information.

```
# telnum to uri conversion table
##############################################################################
#    DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#1. For Operator Dial In, change "<sip:5200@*" "OP5200x1" accordingly where
currently
#   5200 is the dial in for Op1. Change both instances of 5200 to change.
#2. For 93???? = sip:$1@10.221.11.250, if 936543 is dialed
sip:936543@10.221.11.250 is sent
#3. For 10??? = sip:10@10.20.30.$1, if 10234 is dialed sip:10@10.221.10.234 is sent
##############################################################################
TelnumPatternTelnumConversioncomment
"1900"    sip:1900@10.20.30.54 ws54
"93????"  sip:$1@10.221.11.250two
"10???"   sip:10@10.20.30.$1 three
"6389"    sip:6389@10.20.30.133Lab_Avaya
"1234"    sip:1234@10.20.30.140 Lab_Cisco
"6229"    sip:6229@10.20.30.184 Lab_Pingtel
????      sip:$1@10.20.30.50 mediagateway
*         sip:$0@10.20.30.50 defaultmediagateway
```

UriToTelnum.tab

The following is an example of a UriToTelnum.tab file with settings configured for Operator Dial In. The file is located in /usr/ipcb/config.

Note:

For more information, refer to URI to telephone number translation table on page 50.

```
# request URI to telnum conversion table
# This table converts the Request URI in the SIP INVITE request to the
# appropriate value specified when a pattern is matched. For example, if the
# request Uri was "<sip:3333@10.220.10.4>" and one of the patterns was
# "<sip:*@*" a match would take place. If the conversion for that match was
# $1 then 3333 would be passed as the ddi for the call. If the conversion for
# that match were "0000" then 0000 would be passed as ther ddi for the call.
##############################################################################
#    DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#1. For Operator Dial In, change "<sip:5200@*" "OP5200x1" accordingly where
currently
#   5200 is the dial in for Op1. Change both instances of 5200 to change.
##############################################################################
TelnumPattern      TelnumConversion               comment
"<sip:5200@*"      "OP5200x1"                     Op1
"<sip:5201@*"      "OP5200x2"                     Op2
"<sip:5202@*"      "OP5200x3"                     Op3
"<sip:5203@*"      "OP5200x4"                     Op4
"<sip:5204@*"      "OP5200x5"                     Op5
"<sip:5205@*"      "OP5200x6"                     Op6
"<sip:5206@*"      "OP5200x7"                     Op7
"<sip:5207@*"      "OP5200x8"                     Op8
"<sip:5208@*"      "OP5200x9"                     Op9
"<sip:5209@*"      "OP5200x10"                    Op10
"sip:6389@*"       "6389@10.220.15.133"           Avaya
"*;dnis=*;*"       $2                             ddi_folwd_by_addtnl_prmtrs
"*;dnis=*"         $2                             ddi_not_flwd_by_addtnl_prmtrs
"*sip:*@*"         $2                             AvayaPhone
"sip:*@*"         $1                              ddibeforePaddressRequestUri
"<sip:*@*"         $1                             ddbeforeIPaddressinRequestUri
"<sip:*"           "1900"                         noddibeforeIPaddrinRequestUri
"sip:*"            "1900"                         noddibeforeIPaddrinRequestUri
"<sip:*"           "1900"                         noddibeforeIPaddrinRequestUri
*                  $0                             wildcard
```

Proxy Table Configuration for use with Operator Dial In

Location - /usr/ipcb/config/proxyConfigTable.cfg

The information in this configuration table is sent to the proxy. The CRS also sends information to the proxy and CRS data overrides data from this file. It is ok to have data in both files. The CRS data is to be changed dynamically where this file cannot.

```
#proxy configuration
###############################################################################
#    DIRECTIONS FOR USE WITH MEETINGXCHANGE 5.0 AND CRS
#    -------------------------------------------------
#1. The information in this config table will be sent to the proxy
#2. *NOTE -  the CRS also sends information to the proxy and CRS data overides data
#    from this file
#3. It is ok to have data in both files, the CRS data if to be changed dynamically
#   where this file is not
#4. *NOTE - No brackets<> around any values or else the values will not be sent to
#   the proxy correctly
#5. The below configuration will work for proxy registration for Operator Dial In,
#   changes will also
#   have to be made in the UritoTelnum.tab and TelnumtoUri.tab
#
###############################################################################

ProxyUri        Contact                 To                                From
usrName         passWord        refreshTime
sip:10.20.30.50        sip:5200@10.20.30.1   sip:5200@10.20.30.50
sip:5200@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5201@10.20.30.1   sip:5201@10.20.30.50
sip:5201@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5202@10.20.30.1   sip:5202@10.20.30.50
sip:5202@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5203@10.20.30.1   sip:5203@10.20.30.50
sip:5203@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5204@10.20.30.1   sip:5204@10.20.30.50
sip:5204@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5205@10.20.30.1   sip:5205@10.20.30.50
sip:5205@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5206@10.20.30.1   sip:5206@10.20.30.50
sip:5206@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5207@10.20.30.1   sip:5207@10.20.30.50
sip:5207@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5208@10.20.30.1   sip:5208@10.20.30.50
sip:5208@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5209@10.20.30.1   sip:5209@10.20.30.50
sip:5209@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5210@10.20.30.1   sip:5210@10.20.30.50
sip:5210@10.20.30.50   prxyusrname          prxypswd           180
sip:10.20.30.50        sip:5211@10.20.30.1   sip:5211@10.20.30.50
```

Verifying Network Configuration and adding NTP Servers

To verify the current LAN configuration and add NTP Servers if they are not already configured for your system, use the mx-ipChange.sh script.

```
cd /usr/dcb/bin

./mx-ipChange.sh
```

```
mx-ipChange.sh:
mx-ipChange.sh:    ============================================
mx-ipChange.sh:    NOTICE: SYSTEM REBOOT REQUIRED
mx-ipChange.sh:
mx-ipChange.sh:    A system reboot is required to update
mx-ipChange.sh:    the conferencing bridge IP configuration.
mx-ipChange.sh:
mx-ipChange.sh:    Additional warnings will be issued prior
mx-ipChange.sh:    to applying changes and prior to rebooting.
mx-ipChange.sh:
mx-ipChange.sh:    Type "Ctrl-C" within 10 seconds to
mx-ipChange.sh:    terminate this procedure.
mx-ipChange.sh:    =============================================
mx-ipChange.sh:

Current customer LAN configuration is:
Host name                        = testsystem
Domain name                      = du.rnd.avaya.com
IP_address                       = 135.64.21.107
Netmask                          = 255.255.255.0
Gateway                          = 135.64.21.1
Network Time Server(s)           = 135.64.25.1
Domain Name Server(s)            = 135.64.21.5
Domain Search List               = du.rnd.avaya.com
NIC bonding state                = enabled
NIC device                       = bond0
Domain name (default="du.rnd.avaya.com"). Enter h for help, q to quit:
```

Adding a Network Time Protocol Server

You can use the mx-ipChange.sh script to add up to three NTP Servers to your system. To add NTP servers in the configuration, start the mx-ipChange.sh script. Press Enter. Enter the IP addresses requested. At the Network Time Server prompt, you can enter up to three server IP addresses. If you have only one NTP server, enter the server address, and press Enter.

```
Domain name (default="du.rnd.avaya.com"). Enter h for help, q to quit:
du.rnd.avaya.com

Enter IP address 1 of 1 for New subnet mask     : 255.255.255.0
Enter IP address 1 of 1 for New gateway address : 135.64.21.1

Multiple query. Type return if you have fewer addresses to enter

Enter IP address 1 of 3 for Network Time Servers: 135.64.25.1
Enter IP address 2 of 3 for Network Time Servers:

Multiple query. Type return if you have fewer addresses to enter

Enter IP address 1 of 3 for DNS servers         : 135.64.21.5
Enter IP address 2 of 3 for DNS servers         :

DNS search domains (eg: yours.net mine.net)     : du.rnd.avaya.com
```

Note:

There is no Hostname or IP address configuration option when running this script.

Run the script to make the changes. The server will reboot automatically to install the new network configurations.

To verify the changes, open the script again. At the prompt, enter q to quit the program.

Creating a new IP Address

To change the IP address on a system, run the following script from `/usr/dcb/bin`:

```
ip_Change_Mx_Cs.sh
```

You must enter the old and new ip address after the script.

```
ip_Change_Mx_Cs.sh <old ip address> <new ip address>
```

Changing the hostname

To change the hostname on the system, run the following script from `/usr/dcb/bin`:

```
hn_Change_Mx_Cs.sh
```

This script prints out usage information.

Note:

When you make any of these changes, such as creating an IP address and changing the hostname, verify that core services start up after you make the changes.

Appendix D: Validating the System

Overview

This appendix provides guidance for validating communication between the CRS and the application servers.

This section describes how the installer can test for both application server failover and for CRS failover if there is a cluster. Additionally, a procedure outlines verifying the communication between the CRS and the application server.

Testing for application server failover

Once all of the application servers and the CRS are configured properly, the CRS is updated with the status of the bridges, displaying Active or Standby. This can be seen on the Bridges tab on the CRS Front End. If a failover occurs, the MxMonitor updates the CRS and the status of the failed and failover bridges changes on the display.

i

Testing application server to CRS communication

Communication between the CRS and the application server is a one-way process. The application server sends messages to the CRS. The application server can send either the GET_ACCESS_NUMBERS_LIST or the TAKE_OVER_BRIDGE message to the CRS.

- The GET_ACCESS_NUMBERS_LIST message is a request for the DDI Phone fields.
- The TAKE_OVER_BRIDGE message informs the CRS that one application server is taking over for another.

Note:

The CRS uses the TAKE_OVER_BRIDGE message to set a bridge as active or standby. The CRS does not remap DDI's or any other value, because the application servers govern this.

For example, imagine an installation with four application servers, each numbered 1 to 4. Servers 1 to 3 are active and server 4 is standby. In the CRS, set up four bridges to correspond to each of the application servers. Make sure you use the corresponding ddi phones. When application server 1 wants its access numbers, it sends the GET_ACCESS_NUMBERS_LIST message with “1” as its parameter. The CRS returns a list of the ddi phone numbers for the bridge (application server 1). If application server 1 fails and application server 4 takes over, then application server 4 sends the TAKE_OVER_BRIDGE message to the CRS. Application server 4 now assumes the identity of application server 1 as far as communication with the CRS is concerned, i.e. it sends the GET_ACCESS_NUMBERS_LIST with a parameter of “1”, not “4”. As a result, when the CRS receives the TAKE_OVER_BRIDGE message, it does NOT remap DDI's.

Appendix E: Server Upgrade

This appendix describes the upgrade procedure for an upgrade from a prior Meeting Exchange 5.0 Release. This appendix contains the following sections:

Upgrade considerations

In a Pyramid configuration with external software media servers, the media servers can be upgraded first, one at a time. Call connections will be maintained, provided the call load is not high at the time of the upgrade.

For configurations with application server failover using mxmonitor, the standby server can be upgraded first, followed by the other servers one at a time, allowing them to fail over during upgrade. This will result in dropped calls, but the downtime will be limited to the time required to detect and fail over, approximately two minutes.

For installations with Avaya Plug-ins for for Microsoft Outlook, Microsoft Office Communicator, Microsoft Live Meeting, IBM Lotus Notes, or IBM Lotus Sametime, configurations are not copied across by default as part of the bridge upgrade. Therefore additional steps are required once the upgrade is complete to reconfigure. For more information, see step 34 in After upgrading on page 140.

The following upgrade path is supported:

- 5.0 > 5.0 Service Pack 2

To complete the steps described in this chapter, you must run the commands at `sroot` level.

Before upgrading

- Make sure that domain name is specified during install. Meeting Exchange requires the fully qualified hostname to be set during the software installation. Before proceeding with the upgrade, ensure that the domain name is in the `etc/hosts` file as required. If the `mx-ipChange.sh` script was run on the bridge, the domain information may have been modified. An example of domain information:

```
135.64.27.81    duqaMX5L-2781.du.rnd.avaya.com  duqaMX5L-2781
```

- Ensure that core services are running on your Meeting Exchange server:

  ```
  /opt/coreservices/lifecycle/bin/lc list
  ```

- Password expiry changes are not copied across as part of the upgrade. Prior to the upgrade, collect password expiry details. The key accounts are here:

  sroot/craft/dcbmaint/dcbadmin/dcbguest

  The command is:

  ```
  chage -l dcbguest
  ```

  After the upgrade, set password expiry changes (if required).

  Example: To turn password expiry off for `dcbadmin`, run command.

  ```
  chage -I -1 -m 0 -M 99999 -E -1 dcbguest
  ```

- The `syslog.conf` file is not copied across as part of the upgrade. If customizations have been made to this file, they will need to be implemented after the upgrade.

Backing up your current configuration

Use the following steps to back up existing data and configurations. Although backups run automatically on the server, Avaya strongly recommend that you manually back up existing data and configurations. Avaya considers it to be a mandatory step in the upgrade procedure.

The `usr3` directory is not overwritten as part of the upgrade, so it's not strictly required to perform this step. It is included as an additional precautionary measure.

1. Stop the conferencing server and informix.

   ```
   service mx-bridge stop

   service informix stop
   ```

2. Run the two standard bridge backup tools.

   ```
   /usr/dcb/bin/backup.sh

   /usr/dcb/dbase/bridgedb/batch_backup.sh \

   -full \

   -force \

   -directory /usr3/BACKUPS/autobackups
   ```

3. Manually tar additional elements:

   ```
   tar zcvf /usr3/BACKUPS/autobackups/extras.tar.gz \
   /opt/informix/etc/sqlhosts \
   /usr/brdgdbo \
   /usr/brdgdbu \
   /usr/dcbadmin \
   /usr/dcbguest \
   /usr/dcbmaint \
   /usr/ipcb \
   /usr/splibdbu \
   /etc/sysconfig/network-scripts/ifcfg-*
   ```

4. Copy the three backup sets created above from `/usr3/BACKUPs/autobackups` to another machine.
5. Restart the bridge and informix.

   ```
   service mx-bridge restart
   service informix restart
   ```

Upgrading Meeting Exchange

After performing the upgrade, additional manual steps are required to restore configurations from the prior release.

6. Mount the upgrade cd.

   ```
   mount /mnt/cdrom
   ```

   Alternatively, you can copy the iso image of the new build, for example MX 5.0.2.0.14 on the server.

   a. Open a WinSCP session with `craft` login.

   b. SCP the iso image to the `/home/craft` directory on the conferencing server.

   c. Log into the server

   ```
   cd /home/craft
   mount -o loop MX5.0.2.0.14.iso /mnt/cdrom
   ```

7. Install the Signing Authority certificates. The install-def-dev-certs-linux file is stored at the same location as the `ISO` image of the new build.

- Open a WinSCP session to the conferencing server to SCP the attached file `install-def-dev-certs-linux` to the server: `scp bridge IP.`

  ```
  cd /home/craft
  ```

  ```
  chmod 777 install-def-dev-certs-linux
  ```

  ```
  ./install-def-dev-certs-linux
  ```

8. List all software images currently stored on the system up to a maximum of three.

   ```
   cinstall -q
   ```

9. List the release available on the CD. This information is used in the **-b** and **-x** steps to follow.

   ```
   cinstall -q file:/mnt/cdrom
   ```

10. Check all partitions.

    ```
    cpartition
    ```

    Note:

    > **cpartition -a** lists the currently active build, **cpartition -s** lists the current standby build.

11. Download the release onto the system disk, for example MX-5.0.2.0.14.

    ```
    cinstall -b MX-5.0.2.0.14 file:/mnt/cdrom
    ```

    If the system disk repository is full, you may not be able to download the release. If you cannot download the release, you can remove software files from the repository. To see a list of files in the repository, enter:

    ```
    cinstall -q
    ```

    To remove the oldest software files, for example, MX-5.0.0.0.18, enter:

    ```
    cinstall -e MX-5.0.0.0.18
    ```

12. Eject the CD when the **cinstall -b** step completes successfully.

    ```
    eject
    ```

13. Upgrade the Standby partition to the new release from the disk’s repository.

    ```
    cinstall -x MX-5.0.2.0.14
    ```

14. Do not reboot the system at this stage.

15. Backup the `/etc/services` new default file so that it can be referenced later. The `/etc/services` file is copied across during upgrade, therefore newly added default ports are not saved:

    ```
    cp /root2/etc/services /usr3/NewDefaultservices.txt
    ```

    ```
    diff /etc/services /root2/etc/services | cat > /usr3/
      Diffservices.txt
    ```

    This command will highlight changes in the new services file and you may need to merge the two versions to include new features with your own previous port allocations.

16. Backup the new default `/usr/dcb/dbase/admin` files so that they can be referenced later. The existing files are copied across during the upgrade. For Meeting Exchange, files being transferred are detailed in: `/etc/opt/ecs/backup/mx_backup_ds.conf`. The purpose of this step is to ensure that there is a copy of the new default files available on the system after the upgrade. This copy is for reference only.

    ```
    mkdir /usr3/adminNew
    ```

    ```
    cp /root2/usr/dcb/dbase/admin/* /usr3/adminNew
    ```

17. Verify that the boot partition contains new software.

    ```
    cpartition
    ```

    Example output of this command:

    ```
    /dev/sda6       active  MX-5.0.1.0.18
    /dev/sda1       standby MX-5.0.2.0.14
    /dev/sda6       boot    MX-5.0.2.0.14
    ```

18. Reboot the bridge.

    ```
      reboot
    ```

    The system boots into the new software, as displayed in the `boot` partition.

19. To verify that the configuration is complete, run the following command and wait for the message: `MeetingExchange Server configured successfully`:

    ```
    tail -f /var/disk/logs/S94mx-runOnce*
    ```

    The completion of the configuration can take between 30 and 45 minutes.

20. Verify that the standby partition is now active.

    ```
    cpartition
    ```

21. Make the current active/standby/boot partition configuration permanent for subsequent reboots. All subsequent reboots will boot into the new release:

    ```
    cpartition -p
    ```

22. Verify the current partition status:

    ```
    cpartition
    ```

23. Verify that coreservices is fully up by running the following 3 commands:

    ```
    /opt/coreservices/lifecycle/bin/lc list
    ```

    This command should list 12 services all with status of STARTED.

    ```
    /opt/coreservices/dss/bin/dss list -h localhost -p 31050
    ```

    This command should list 21 services.

    ```
    /opt/coreservices/dss/bin/dss list -h localhost -p 50000
    ```

    This command should list 2 services.

24. If core services is not fully started, as detailed above, stop it:

    ```
    service wdinit stop
    ```

25. Verify that the tomcat5 process has been stopped.

    ```
    service tomcat5 status
    ```

    If the tomcat5 process has not stopped, try stopping the service:

    ```
    service tomcat5 stop
    ```

    If the tomcat5 process has still not stopped, search for the process ID and kill it.

    ```
    ps -ef | grep -i tomcat5
    kill -9 <process ID>
    ```

26. Start core services.

    ```
    service wdinit start
    ```

27. Wait until those 3 commands, listed above in step 23 in cp /root2/usr/dcb/dbase/admin/* /usr3/adminNew on page 139, show that it is fully initialized. This process takes 4 or 5 minutes.

After upgrading

28. After the upgrade, new default `/usr/ipcb/config` files have been installed. Any previous configurations will need to be reapplied (for example, `system.cfg` - tls configuration). The old `/usr/ipcb/config` parameters are stored in `/root2/usr/ipcb/config`. Do not copy old configuration files across. Edit the new default files as new parameters may have been introduced in this release. Files typically customized are:

    - `system.cfg`
    - `telnumToUri.tab`
    - `UriToTelnum.tab`
    - `processTable.cfg`

- `mediaServerInterface.cfg`
- `softMediaServer.cfg`
- `mxmonitor.reg`

Before you perform this step, stop the bridge as follows:

```
service bridge stop
```

After you perform this step, start the bridge, as follows:

```
service mx-bridge restart
```

29. After the upgrade, customized stored procedures need to be reapplied. To find out if any stored procedures have been applied, you must ask the Meeting Exchange System Administrator at the customer site.
30. After the upgrade, the new default firewall rules are active. Any customizations need to be reapplied. The old firewall rules remain stored in:

    ```
    /root2/etc/firewall/conf/mx_firewall.rules
    ```

    The new rules are stored in:

    ```
    /etc/firewall/conf/mx_firewall.rules
    ```

    After making any changes, restart `iptables`:

    ```
    service iptables restart
    ```

31. Reapply the `dcbguest/dcbmaint/dcbadmin` password expiry settings, if required.

    For example, to turn password expiry off for `dcbadmin`, run this command.

    ```
    chage -I -1 -m 0 -M 99999 -E -1 dcbadmin
    ```

32. Reapply `syslog.conf` customizations if required. The location of the original file is:

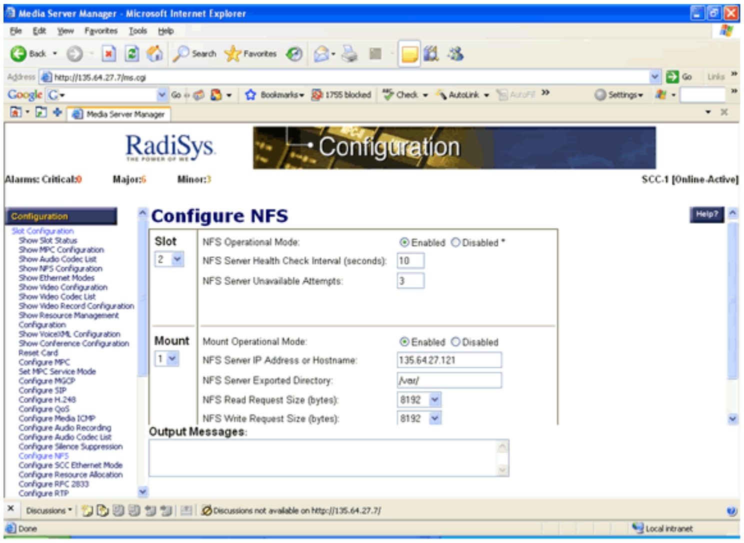
    ```
    /root2/etc/syslog.conf
    ```

33. This step applies to S6800 systems only. After upgrading the system, verify that the mounts on the MPC are updated by checking the alarms. To update the mounts; Enable and disable the mounts on the S6800 server:

    a. Log into the S6800 user interface.

    b. Select **Configuration** > **Node Configuration** > **Configure NFS**. The **NFS Configuration** screen opens.

Figure 11: NFS Configuration Screen



http://135.64.27.7/ms.cgi

Alarms: Critical:0 Major:6 Minor:3 SCC-1 [Online-Active]

Configure NFS

Slot: 2

NFS Operational Mode: ● Enabled ○ Disabled *

NFS Server Health Check Interval (seconds): 10

NFS Server Unavailable Attempts: 3

Mount: 1

Mount Operational Mode: ● Enabled ○ Disabled

NFS Server IP Address or Hostname: 135.64.27.121

NFS Server Exported Directory: /var/

NFS Read Request Size (bytes): 8192

NFS Write Request Size (bytes): 8192

Output Messages:

Discussions not available on http://135.64.27.7/

c. In the **Mount** section, change **Mount Operational Mode**, to **Disabled**.

d. Save the changes

e. Change **Mount Operational Mode** back to **Enabled**.

f. Save the changes.

g. Follow these steps for all mounted MPCs.

34. For installations with Avaya Plug-ins for Microsoft Outlook, Microsoft Office Communicator, Microsoft Live Meeting, IBM Lotus Notes, or IBM Lotus Sametime, see the *Meeting Exchange 5.1 IBM Lotus Installation and Configuration Guide* and the *Meeting Exchange 5.1 Microsoft Installation and Configuration Guide* for information on how to reconfigure the bridge after upgrade. Both of these guides are available on support.avaya.com.

Sample SOAP configuration

The `/usr/share/tomcat-5.5.9/conf/server.xml` needs to be configured with the IP address of the CRS. The previous file is backed up to `/root2/usr/share/tomcat-5.5.9/conf/server.xml`.

a. Navigate to `/usr/share/tomcat-5.5.9/conf/server.xml` and apply the CRS IP in the below statement.

```
url="jdbc:sqlserver://<CRS IP>:1433;databaseName=BSRes2"
```

b. Restart the service:

```
service wdinit restart
```

Sample Outlook configuration

a. Install Outlook Conference Scheduler.

```
rpm - qa | grep outlook
```

```
rpm - Uvh outlook-plugin.xxxxxx.rpm
```

```
service outlook-plugin restart
```

b. Configure the file `/usr/ipcb/outlook/configuration.xml`. The previous file will be backed up to `/root2/usr/ipcb/Outlook/configuration.xml`. Typical configurations include audionumbers and features.

For example, for audionumbers:

```
<audionumbers>Internal:35682,Local:01-2075682,International:+353-
  1-2075682</audionumbers>
```

For features, enable the parameters.

```
webconference="1"
```

```
showjoinconferencebutton="1"
```

c. Restart the outlook plugin service:

```
service outlook-plugin restart
```

35. If your installation of Meeting Exchange uses UserTransactionLogs, restart syslog to start logging:

```
service syslog restart
```

36. Check that all processes are up and that you can make a call to the bridge:

```
dcbps
```

Rolling back to a previous version

37. Verify current partition status:

```
cpartition
```

38. Make the current standby partition active upon the next reboot:

```
cpartition -o
```

39. Reboot the bridge.

```
reboot
```

40. Verify active/standby/boot status.

```
cpartition
```

41. Make the active partition permanent.

    ```
    cpartition -p
    ```

Appendix F: Troubleshooting

Describes common problems and suggested resolutions.

General Issues

This section discusses general problems and also problems that are common to the operating system.

Identifying Installation Problems

The installation script, ipcb_cdinst.sh, maintains a complete recording of the installation (and any reinstallations). The file is stored in /usr/ipcb/ipcb_cdinst.sh.log. Check the following logs for installation issues:

- /usr/dcb/logs - for daily logs
- /usr3/ipcb/logs - for mx logs
- /var/adm

Setting Network Drivers to 100 Full Duplex

If the network drivers for your server are set to Auto, they must be reset to 100 Full Duplex.

⚠ **Important:**
Do not use a network connection when making this change. Connect to the server via modem.

```
cd /etc/sysconfig/network-scripts/
more ifcfg-eth0
```

Connecting to a Gigabit Switch

If your network has a gigabit connection, set your server ports as shown in: Gigabit Connections on page 15.

Correcting Uptime Reporting

When you reboot a Dell™ 1950 server, the system uptime report may not be accurate. Ensure that the uptime is reported accurately.

Obtaining Debug Information

For issues, most problems require that you use Linux commands and edit configuration files.

The S6x00 log files provide a key source of information. The following table will help you to locate core and log files on the different servers.

Table 18: S6x00 Core and Log File Directories

Application	Core and log file directory
bridgeTranslator	/usr/dcb/bin
initipcb	/usr/dcb/bin
Platform log file	/usr3/ipcb/log/
sipagent	/usr3/runtime/sipagent_logs0 for the first file, and /usr3/runtime/sipagent_logs1 for the second file, and so on. **Note:** Log files in usr/dcb/bin/ are linked to the corresponding file in /usr3/runtime/
softms	/usr/dcb/bin
CS700 legacy applications	/usr/dcb/bin for most processes
System log file	/usr/dcb/logs

For specific advice , refer to the following sections which describe specific symptoms.

Table 19 lists commands that can assist you with resolving problems.

Table 19: Common Linux Commands

Type this command:	To:
df -k	determine if the system is running low on disk space.
ifconfig -a	list Ethernet interfaces
hostname	find the computer’s name
ipcs -qa	find the number of IPC messages used by each queue. The number in the "QNUM" column represents the number of messages waiting in a queue.
kill	stop a process.
man -k <*topic*>	search for help on a topic.
netstat -s	get detailed statistics, including dropped packets, for all protocols; IP, UDP, ICMP, etc.
ping <*ip address*>	test connectivity to another system on the network.
ps -eaf	list running processes.
sar 5 5	List Linux version plus list available CPUs
uname -a	determine which kernel is running
uptime	identify the length of time a computer has been running
who	determine which users are logged onto the computer.
who -b	view the last reboot,

Table 20 lists log files that can be helpful in diagnosing common problems.

Table 20: Log Files

Directory	File	File description
/usr/dcb/	logs	Daily log files for Meeting Exchange.
/usr3/ipcb/	log	Daily log files for MX software.
/var/lock/subsys	syslog	log file containing messages and errors.

Setting up Debug

System log files are located /usr3/ipcb/log

- debug.log
- dcbsched.log > system.log

To turn on logging information for softms:

```
ipcbdbg f mediaserver t
```

To enable/disable for a particular process, you need to specify the associated process name, provided in /usr/ipcb/config/processTable.cfg

Note:

Logging returns to the WARN level when the process is restarted.

To turn off logging information for softms:

```
ipcbdbug f all w
```

IP Trace Packet Utilities

Run the following utilities to trace packets:

- Ethereal - mirrors all ports in a complete system
- tcpdump - for S6200 and S6800 signalling

  Captures SIP signalling and RTP audio stream

Restart a Program

Normally, let the bridge software automatically start and stop its processes. However if you need to manually restart a process, you will need to manually stop the process first.

Use the "kill" command to stop a process. This command requires the process ID number. To obtain the process ID number, use the "ps -ef" command to list processes and locate the one you want to stop.

To start the process, you can either let the init process automatically restart it, or for debugging purposes you can type the command to start the process.

⚠ **WARNING:**
Manually starting a process is not recommended because there may be required command line parameters. Therefore manually starting a process should be done in consultation with the development staff.

Unable to create new files

Systems that are unable to create new files will exhibit the problem in a number of ways. Typically the system may not be able to perform these functions:

- Save recording files
- Write new log messages
- Open a new window
- Edit a file

Administrators can use the df command with the k switch to determine if the system is running low on disk space.

```
df -k
```

When the system is more than 80% full, free up space by removing old log or core files.

Software version

The software version information is stored in the version.xml file located in /usr/dcb/bin. This file lists the version of:

- Meeting Exchange
- Bridge software included in the release
- Linux

System Configuration Problems

This section describes problems related to installation or configurations.

Slow System Performance

When the system's response time is slow, take these actions:

1. Check the amount of free CPU time using this command:

   ```
   sar 5 5
   ```

   Idle time should be 50% or more. If the idle time is less than 50%, list all running processes by typing:

   ```
   ps -eaf
   ```

   Note:

   The idle percentage is an unreliable way of determining the system load. A better indicator, is to verify that DTMF digits are handled promptly by making a test call to the system.

2. Look for the processes which use the most cumulative CPU.
3. To check CPU memory, run the following command:

   ```
   top
   ```

   ⚠ **Important:**

   The system may be trying to handle more calls than is optimal when the softms process is using the most CPU time.

4. Ensure the system is running a minimum amount of other software.

   For best performance, the server running should be dedicated to use as a VoIP bridge. Do not use the system to run other enterprise applications, such as billing, or server applications such as file, print, database, web, application, etc.

   It is not recommended that shared disks, tapes, or other devices be connected to a VoIP system.

System does not Accept Calls

Follow this procedure:

1. Telnet to the system to make sure it is on the network and running.
2. Concantenate processTable.cfg

   ```
   cat /usr/ipcb/config/processTable.cfg
   ```

3. Change directories to /usr/dcb/bin:

   ```
   cd /usr/dcb/bin
   ```

4. List the currently running processes using the dcbps command.

   ```
   dcbps
   ```

5. Verify that the listed processes include:
    - bridgeTranslator
    - sipagent
    - appropriate media server process(es):
        - softms for software based DSP
6. Restart processes, if needed

    ```
    service mx-bridge restart
    ```

7. Verify that each process has a unique key ID.
8. Verify that each media server in the cluster has a unique number.
9. Verify the IP address of each media server

    Tip:

    With a single server system, list the IP of the server as 0.0.0.0 to prevent IP errors and to prevent the need to change the IP at any time.

10. Verify that Autostart is set to 0 when configuring with a separate application server. Set Autostart to 1 when configuring as a standalone server.
11. Check the log files stored in /usr/dcb/logs for reasons why the system is not accepting the calls. Some clues might include processes which are repeatedly stopping and restarting or SIP stack errors.

    ```
    cd /usr/ipcb/config
    ```

12. Look for core files. Type `cores` to determine if new core files exist.
13. Change directories

    ```
    cd /usr3/ipcb/log
    ```

    Tail the daily log to look for errors.

    Tip:

    Daily log files (/usr/dcb/logs) are on the application server only. /usr3/ipcb/log is on both the application and the media server.

14. Verify system.cfg is correctly configured.
15. Check the SIP call flow using a network trace.

Processes are running but calls do not connect

Once you verify the correct processes are running on the server, if calls still do not connect, check the following:

1. Verity the SIPAgent is running

2. Change directories to system.cfg
   - Verify that the correct transport, tls or tcp, is identified in MyListener and respContact
3. Check for errors

   ```
   tail -f /usr3/ipcb/log/system.log
   ```

   ```
   tail -f /usr3/ipcb/log/debug.log
   ```
4. Change directory to /usr3/runtimeSIPAgent_log0. Look in pdtrc.log for errors
5. Check the UDP port for the transport. Port is 5060 for tcp and 5061 for tls

   ```
   netstat -a
   ```

   ```
   grep 5060 (or 5061)
   ```
   - Verify that the switch is sending a call to the server
6. Type **ifconfig -a**
   - Verify that the local IP address shown here matches system.cfg
7. Verify that the server can ping the gateway and itself
8. Run a network trace

Caller hears busy signal

A network busy signal can result if there is a transport mismatch between the conferencing server and the Communication Manager. Verify that the transport setting, tls or tcp, is the same for both.

Caller hears fast busy

Check the folllowing files if callers report hearing a fast busy when dialing into the server.

1. Verify that media server resources are available:

   ```
   cd /usr3/ipcb/log
   ```

   ```
   grep regstring
   ```
   - Verify the number of registered media servers ar shown and that they have the correct IDs. If the information is not correct, go to processTable.cfg msInterface to verify media server count.
2. Check log files. Message 486 reports that the system is out of resources.

VoIP programs restarted

You can search the log file for the date you suspect the program restarted. For example, if you suspect that the VoIP programs restarted on July 28, follow these steps.

```
cd /usr3/ipcb/log
```

```
grep start system.log.Jul28
```

1. Look for messages in the log which say "INIT started process…" and the date and time that occurred.

Backing up Configuration Files

Use the Administration menu to access the restore option.

1. Start the administration client, by typing this command:

   ```
   dcbadmin 115
   ```

2. Select Administrator Menu > File Management > Backup/Restore.
3. Select Backup.
4. Select MeetingXchange.
5. Wait for the message stating, “Backup of sip_config is complete. Press any key to exit.”
6. Press any key.

   Note:

   The system store backup files in /usr3/BACKUPS/usr/dcb/ipcb_config. The currently used versions of the files are in /usr/ipcb/config. There is a link from /usr/ipcb/config to /usr/dcb/ipcb_config.

Restoring Configuration Files

Use the Administration menu to access the restore option.

1. Start the administration client, by typing this command:

   ```
   dcbadmin 115
   ```

2. Select Administrator Menu > File Management > Backup/Restore.
3. Select Restore.
4. Select MeetingXchange.
5. Wait for the message stating that the restore was successful.

Note:

Backup files are stored in /usr3/BACKUPS/usr/dcb/ipcb_config. The currently used versions of the files are in /usr/ipcb/config. There is a link from /usr/ipcb/config to /usr/dcb/ipcb_config.

Network Problems

This section describes some common network-related problems.

Debug a Network Problem

Use these guidelines to determine the cause of a problem on the network.

1. Make sure the network cable is firmly seated in both the server and the switch.
2. Verify that the LAN is set to 100 Full Duplex on both the server and the switch.
3. Ensure the software media server can communicate with the network by logging on to a bridge and using the “ping” command to test communication with another computer on the network. If you get an error saying “Network is unreachable” refer to the procedure Network is unreachable on page 155 before continuing.
4. Verify the IP address of both computers which are experiencing communication problems. Use the "ifconfig -a" command. Ignore the "lo" loop back device" and look for "inet" parameter for the "net0" device.
5. Use "netstat” while trying to communicate with the system. If communication is working, the system should display a line describing a socket from the source computer to the destination (bridge computer). If successful, the state of the socket is "ESTABLISHED".

   Note:

   This step applies to TCP/IP communication, not UDP.

   If you are debugging VoIP configuration then refer to System does not Accept Calls on page 150.
6. View /var/adm/syslog file to see if there are any errors related to network communication problems.

   If all the configuration files and parameters look favorable, then there may be a message format difference between the sending and receiving computers.

   You will need to debug that you need some type of packet sniffer program or computer. See the tip for the symptom "How can I capture of monitor IP traffic?"

   If you have not located the problem, gather all the information, and send it to the developers for further investigation.

Network is unreachable

Verify network connectivity by following this procedure:

1. List all Ethernet interfaces, by typing this command:

   ```
   ifconfig -a
   ```

   This command should return more than "lo"" loop back. When it returns only the loop back, or displays the message "Network is unreachable", then install the driver for your Ethernet interface.

   When the command returns:"eth0", "net0", or another network interface that has the state "DOWN", refer to "Need to configure Network interface"

   a. Confirm that the Ethernet cable is firmly connected to the back of the server and to the router/switch/hub.

   b. Verify the port on the router/switch/hub is enabled and correctly configured.

   When the command returns:"eth0", "net0", or another network interface that has the state If the state is "Up":

   c. Verify the IP address of the interface is correct.

   d. Test communication with other computers in the network by using the ping command. For example:

   ```
   ping 10.221.10.254
   ```

2. If the problem remains, reboot the server.
3. If the problem remains after rebooting, contact support.

How can I capture or monitor IP traffic?

Use a second system to monitor IP traffic. The system should run Ethereal or tcpdump. Connect this system to a mirrored port on the Ethernet switch/router/hub. That port should be a mirror of all traffic sent to the VoIP system.

SIP Agent failures

SIP agent fails when the proxy server is not available to register the bridge.

Problems

This section provides procedures for troubleshooting common audio problems.

No Audio

When a call appears to connect, but no audio is heard, follow this procedure:

1. Check the SIP phone configuration used by the person who reported the problem.
2. Verify the correct media server program is running on the server:
   - convMS for Convedia
   - softms for the S6200 media server
3. Check the system configuration file, system.cfg. If a hardware media server is in use, check those configuration files as well. Refer to Chapter 2: Configuration for details.
4. Use a packet sniffer program to verify the RTP packets are delivered to the system.
5. External hardware media servers only:
6. Verify the hardware media server is connected to the network and operating correctly. Refer to the manufacturer's documentation for the hardware media server. Static Heard in Conference

When participants hear static in a conference:

1. Follow the procedure for Slow System Performance on page 150.
2. Verify that the correct codec is in use by using a software phone that can display the code.
3. Double-check the router and network configuration to verify that RTP packets get the correct quality of service and are not being delayed by data traffic

After entering code, line disconnects or no audio is heard

If callers hear the annunciator greeting when dialing in, but there is dead air after they enter code:

1. Check /usr3/ipc/logs for error messages
2. Check system.cfg. Ensure that no IP is listed in MyListener and respContact if Communication Manager is not a part of the solution
3. Check User Transaction Logs (/usr/dcb/ulogs) to verify that DTMF is being passed
4. Check rtpm for memory being used and to determine if large numbers of calls are being sent to the server simultaneously

5. Use a packet sniffer program to verify the RTP packets are delivered to the system

Static Heard in Conference

When participant hear static in a conference:

1. Follow the procedure for Slow System Performance on page 150.
2. Verify that the correct codec is in use by using a software phone that can display the code.
3. Double-check the router and network configuration to verify that RTP packets get the correct quality of service and are not being delayed by data traffic.
4. Use a packet sniffer program to verify the RTP packets are delivered to the system.
   - Check SIP messages
   - Look at STP for port and IP address of media server. Check UDP traffic on the media server port. Extract both outgoing and incoming audio with the network trace program.
5. Try to record the static. If no static is heard on the recording, the issue originates with the output. If the static is heard on the recording, the issue originates with the input.
6. If static is heard during a conference, use Line Listen from the operator display to isolate the issue.
7. Verify that the conferencing server is set to Full Duplex.
8. Verify that the SIP Agent switch is set to Full Duplex.

Tip:

The conferencing server supports Full Duplex only.

Dialout Issues

This section provides tools for troubleshooting dialout issues.

1. If the conferencing server is configured with a Communication Manager, verify that the transport method has been added to the telnumToURI table.
   - Verify that the correct transport, tcp or tls, is listed in the table
2. If the conferencing server is not configured with a Communication Manager, verify that the CLAN address is in the telnumToURI table.
3. Verify that the correct IP is being called
4. Verify the error code in /usr/ipc/logs
5. Verify that you can ping the gateway

6. For non-CRS solutions, verify the proxy server IP address in ProxyConfigTable.cfg
   - Verify that Session Timer is set to 300
   - Verify settings in mxmonitor.reg, chdbased.reg, and processTable.cfg

Server Failover

The following sections provide some tools for systems configured for server redundancy (see Server Redundancy on page 57.

Failover failure

If a server does not automatically fail over as expected:

1. Verify that mxmonitor has servers set up as active and standby in processTable.cfg
2. Verify that all media servers are registered
3. Verify that the information for each application server in mxmonitor.reg matches that in chdbase.reg

Determining a server’s status

There are two methods available to determine whether a server is acting as an application server (APS) or as a standby (STBY) server.

On the application server, type this command:

```
pg /usr/dcb/logs/date <- where date is today’s date.
```

The server status is displayed as either STBY or APS.

Alternately, you can list the server’s status by typing these commands:

```
pg /usr/dcb/logs/date | grep MXMONITOR <- where date is the current
  date.
dcbps
```

When there are two ConvMS processes started, then the server is an APS. If there are no ConvMS or sipagent started, then it is the STBY

Preventing failover

Occasionally you may need to make configuration changes that require a reboot, and you do NOT want the system to fail over to the standby application server.

Follow this procedure:

1. Issue the command “uninitdcb” on both the APS (the one you are making the changes to) and STBY. This command ensures that the other two APS remain up and functioning.
2. Issue the command “initdcb &” on both the APS (the one you are making the changes to) and STBY. This command starts all processes with the any configuration file changes.

   Note:

   Issue this command on the APS first, although it should not make a difference. After issuing the command, both application servers should work as configured (APS or STBY).

Appendix G: System Log Messages

Describes messages and logs generated by S6200/S6800 Conferencing Servers.

System Messages

The following messages may appear across the top of the operator screen. The appropriate action for each situation is described.

Table 21: System Messages and Recommended Responses

Message	Meaning	Action
Seizure On Line [001–575]-Expected Wink, Outgoing Call Aborted.	System configured for wink start dialout supervision. Operator-initiated blast or dialout line has seized in (answered) but no wink was received.	Contact the phone network provider to verify dialout supervision type (wink or delay and reconfigure dialout supervision for Delay if necessary.
Could Not Create Unattended Conference: All Confs. In Use	Although a valid conference code was entered, all conferences are in use or have not been cleared.	From the operator console, run a Conference Clear_all on all empty conferences to free them up for use. If no conferences are empty, check to see if any conferences have exceeded their time limit and ask them to hang up.
Incoming Call On Line [001–575], Operator Access Canceled	Call came in on an accessed line before operator dialed a number on that line (System returns operator to main menu.)	Access another line for dial out.
Incoming Call, Blast Dial Canceled on Line [001–575]	Call came in on line reserved for blast before system dialed out on the line.	The system hunts for an additional line. It may be necessary to free up lines if the system is full.
Insufficient Channels To Complete Blast	More channels specified for blast than are currently available.	Attempt to free up sufficient lines by purging disconnects or politely interrupting conferees who have exceeded their time limit.
		1 of 2

Table 21: System Messages and Recommended Responses (continued)

Message	Meaning	Action
No Annunciator Available For Blast	Blast does not begin as all annunciators are busy.	Wait a few seconds for an annunciator to become available and try again.
Empty Blast List Or No Items Selected	There are several possibilities: Operator blasted empty list or list without phone numbers. Operator requested Blast/reBlast with all items excluded. Operator requested reBlast but all lines are already in conference. Any combination of the above.	View dial list to determine nature of error and try again.
WARNING: Only 30 more minutes available for digital record!	Only one 30-minute segment remains for digital record.	Delete obsolete digital record files to free disk space.
WARNING: FINAL 30 minutes of digital record time!	Someone is using the final 30-minute segment for digital record. Future digital record requests will be denied.	Delete obsolete digital record files to free disk space.
NOTICE: Disk Full. Digital Record Stopped!	While a digital conference record was in progress, the remaining disk space was consumed. The system stopped recording and will deny future digital record requests.	Delete obsolete digital record files to free disk space.
Setting up conference <name> use diallist <listname>	An attended conference is scheduled to begin.	None.
		2 of 2

Log Message Codes

The following sections describe the error messages associated with specific codes in the system log files. If you need more information concerning a particular error, contact Avaya Customer Support.

Each message is in a 6-line format. The first line of each message is blank, and the sixth line contains a single semicolon:

1 - ;

2 - systemName_nodeName date&time

3 - AsequenceNumber.messageNumber REPT AUTO

4 - /* processName fileName lineNumber messageType/UNIXerrorString

5 - m*essageString* */

6 - ;

Message strings may be truncated to maintain an 80-character line limit. The messages themselves are numbered on the following pages, with each message followed by a short paragraph describing its meaning. Variable data is represented according to the percentage (%) conventions described below. When the set of variable strings is known and limited, the choices are included in the message and separated by forward slashes (/).

Conventions used in the messages:

% = variable

%d = decimal number

%s = string

%x = hexadecimal number (0x%X)

0000–0999: Status Messages

<table>
<tr><th>Message Code</th><th>Message</th><th>Meaning</th></tr>
<tr><td>0100</td><td>DCB SYSTEM RESTARTED</td><td>Someone ran a system shutdown ,and the system restarted at the specified time. Typically followed by diagnostics and cold restart messages.</td></tr>
<tr><td>0103</td><td>%s alarm clear on %s: %s</td><td>Indicates a network (T1) alarm has been cleared. Variables are alarm type, alarm location (Trunk), alarm classification
<table>
<tr><th>Alarm Type</th><th>Alarm Classification</th></tr>
<tr><td>Red/Carrier</td><td>Major/Service Affecting</td></tr>
<tr><td>Yellow/Remote Carrier</td><td>Major/Service Affecting</td></tr>
<tr><td>Blue/AIS</td><td>Non-Alarmed/Service Affecting</td></tr>
<tr><td>Not Installed</td><td>Non-Alarmed/ Non-Service Affecting</td></tr>
<tr><td>Maint./Local Maintenance</td><td>Non-Alarmed/Service Affecting</td></tr>
<tr><td>Limit/Out of Frame</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Slip</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Bipolar Violations</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/CRC Errors</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Errored Seconds</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Sync./Loss of Primary</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Sync./Loss of Secondary</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Sync./No Synchronization</td><td>Critical/Service Affecting</td></tr>
</table>
Alarm Location: “T1 Card N Board X” where N=1–3 and X=A–B; or “T1 Auxiliary Trunk”</td></tr>
</table>

<table>
<tr><th>Message Code</th><th>Message</th><th>Meaning</th></tr>
<tr><td>0104</td><td>%s alarm set on %s: %s</td><td>Indicates a network (T1) alarm has been set. Variables are alarm type, alarm location (Trunk), and alarm classification.
<table>
<tr><th>Alarm Type</th><th>Alarm Classification</th></tr>
<tr><td>Red/Carrier</td><td>Major/Service Affecting</td></tr>
<tr><td>Yellow/Remote Carrier</td><td>Major/Service Affecting</td></tr>
<tr><td>Blue/AIS</td><td>Non-Alarmed/Service Affecting</td></tr>
<tr><td>Not Installed</td><td>Non-Alarmed/
Non-Service Affecting</td></tr>
<tr><td>Maint./Local Maintenance</td><td>Non-Alarmed/Service Affecting</td></tr>
<tr><td>Limit/Out of Frame</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Slip</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Bipolar Violations</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/CRC Errors</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Limit/Errored Seconds</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Sync./Loss of Primary</td><td>Minor/Non-Service Affecting</td></tr>
<tr><td>Sync./Loss of Secondary</td><td>Minor/Non-Service Affecting</td></tr>
</table>
Alarm Location: “T1 Card N Board X” where N=1–3, X=A–B; or “T1 Auxiliary Trunk”</td></tr>
<tr><td>0108</td><td>Administrator database updated</td><td>An administrator changed the settings for the auxiliary terminal (Operator Configuration).</td></tr>
<tr><td>0109</td><td>Annunciator conference %d indicates %s still has active channels</td><td>Annunciator message has completed but all the channels could not be moved into the Enter Conference. This is an internal software error and may be preceded with Message 0126 (No Transition...)</td></tr>
</table>

Message Code	Message	Meaning
0110	Blast dial list %d (%s) - insufficient channels available	A blast/reblast has been requested but insufficient user channels are available. The channels are either in use for other calls, still disconnecting from previous calls, or are out of service/faulted.
0111	Blast dial list %d (%s) item %d (%s) - channel %d in use	Blast could not be initiated on a channel due to an internal processing error or a network glare condition.
0112	Blast dial list %d (%s) - no annunciator available	A blast/reblast has been requested but all annunciators are in use for other calls or digital conference record/playback.
0113	Blast dial list %d (%s) - no items marked for dialing	A blast/reblast has been requested but either the blast list is empty or all items have been deselected.
0114	Channel %d in %s state without annunciator	An attempt has been made to place a channel into an annunciator conference but there is no annunciator playing the requested message. This indicates an internal processing error.
Systems with multiple DNIS calls moving from the input conference to an annunciator conference may receive 0114 errors. In fact, the system **does** play annunciator messages to the channels.		
0115	Channel database updated	Database updated.
0116	Channel database updated - remote operator channel removed	Database updated.
0117	Continuous annunciator indicates done - call progress channels present	The continuous annunciator has terminated unexpectedly. Either an internal processing error or file system/ hard disk error.
0118	Cannot find channel %d in conference %d	Whenever a channel is placed into a conference, it is always moved from one conference to another. This error indicates that the channel could not be found in its previous conference. The channel still ends up in the new conference. This error indicates that the internal database has been corrupted.
0119	DSP %d semaphore %d not available	The host attempted to obtain the specified semaphore while the semaphore was locked by the specified DSP.

Message Code	Message	Meaning
0120	DSP %d installed, supports network line %d	During initialization, the specified DSP was detected.
0121	Error defining alarm in alarm database	The system has attempted to define an alarm but the alarm definition table is full. Internal debug error only, should not occur in production software.
0122	Event %d out of sequence on channel %d	A DSP event was not received in the correct sequence. This usually indicates that the host was expecting notification from a DSP that one annunciator buffer was ready and instead received notification about the other.
0123	Initiating network device cold restart	Indicates that the network devices (trunks) in the system are being restarted. Cold indicates that the trunks will be re-initialized.
0124	Initiating network device warm restart	Indicates that the network devices (trunks) in the system are being restarted. Warm indicates that the current states of the trunk will not be affected.
0125	No transition found for channel %d, message 0x%X, state %s	Indicates a T1/Call Handler state transition error. An event has occurred on a channel which is not defined for the state that the channel is in. The channel, event, and channel state are variables. To fully understand the meaning of the message a thorough knowledge of the T1 and Call Handler state machines is required.
0126	No transition found for channel %d, message 0x%X, state %s	Indicates a T1/Call Handler state transition error. An event has occurred on a channel which is not defined for the channel's current state. The channel, event, and channel state are variables. To fully understand the meaning of the message, a thorough knowledge of the T1 and Call Handler state machines is required.
0127	DSP node %d - got DSP controlled semaphore %d	During DSP testing, the host was able to obtain control of the specified semaphore, which was expected to be controlled by the specified DSP.

Message Code	Message	Meaning
0128	Previous call not terminated or multiple start call on channel %d	A new call has been declared on a channel; but the previous call has not been terminated. Internal debug error only; should not occur in production software.
0129	Received unknown event 0x%d	The specified event was received from a DSP, but is not defined.
0130	Recursive execution of state machine (%s)	Internal debug error only, should not occur in production software.
0131	Request for annunciator %d in *failed/active* mode	A request to use the specified annunciator was received when the annunciator was already in use or was not usable due to a previously reported failure.
0132	Request for channel %d on failed DSP node	A request was received to access a channel on a DSP that had previously failed.
0133	System database updated	Database updated.
0134	System time has been reset	Database updated.
0135	Timer lost, source process %d tag 0X018X, operation %s	Memory allocation error in the Timer process.
0136	Warm restart requested but network device not configured	A system re-initialization was started, but when the system came up the network boards had reset. This could occur during the re-initialization due to board installation problems.
0139	Operator database updated	Database updated.
0141	Network database updated	Database updated.
0142	Possible %d CDR(s) Lost For Channel %d	Indicates an internal queuing problem has occurred and CDRs/CODRs may have been lost. Will only occur under an extreme load condition.
0143	Auxiliary Channel %s Unavailable	Indicates that channels on the FDAPI have gone out of service.
0144	Auxiliary Channel %s Available	Indicates that channels on the FDAPI have come into service.

Message Code	Message	Meaning
0146	Unattended database group *name, message:* file created file deleted group config. updated %d codes added %d codes changed %d codes deleted	Database updated.
0147	Possible %d CODR(s) Lost For Conference %d	Indicates an internal queuing problem has occurred and CDRs/CODRs may have been lost. Will only occur under an extreme load condition.
0148	Conference activity screen window is full	Conference has so many CDRs associated with it, that the maximum number of lines has been reached.
0149	Duplicate DTMF Digits in digits.txt, %s and %s	Indicates that the 'digits.txt' file has been modified and that an error has occurred in the definition of the indicated digits. Two digit events are defined to have the same DTMF digit
0150	Digit Collection Error, Channel %d, Status %d , Digits %d	Indicates that insufficient DNIS digits have been collected. The channel, collection status (Timeout, Error), and digits collected are variables.
0151	Call Branding Database Updated.	Database updated.
0152	Socket connected to host '*host-name'* at IP address *IP-addr*	A LAN process has accepted a socket connection to host *host-name* at IP address *IP-addr*.
0153	Closing socket connection to host '*host-name'* at IP address *IP-addr*	A LAN process is purposely closing a socket connection to host *host-name* at IPaddress *IP-addr.* Either the LAN process is being shut down or an error has occurred on the socket connection. A previously logged error message from the LAN process may indicate the reason.
0154	Lost socket connection to host '*host-name'* at IP address *IP-addr*	A LAN process lost a socket connection to host *host-name* at IP address *IP-addr.* Either the indicated host closed the connection or the connection timed out due to a LAN hardware problem

Message Code	Message	Meaning
0155	Received bad ‘*cmd-string’* command from host ‘*host-name’* at IP address *IP-addr*	A LAN process received an invalid ASCII text command *cmd-string* over a socket connection from host *host-name* at IP address *IP-addr*. *Cmd-string* is either an invalid command or it has an invalid format or length and cannot be processed.
0156	:Closing socket, IP address *IP-addr* not found in ‘/etc/hosts’ file	A LAN process closed a socket connection to a remote host at IP address *IP-addr* because no entry was provided in the /etc/hosts file for that host to be allowed access to that service.
0157	Bad Parameters Passed For DigConf. Rec/Play	Incorrect information entered by operator and not trapped in operator screen.
0158	Could Not Allocate Annunciator For DigConf. Rec/Play	Operator requested DigRP channel but it was allocated for another function after the request and before it was put into conference.
0159	DigRP Channel %c - Already In Use	Indicates that a DigRP channel was not stopped before it was moved to another conference.
0160	Could Not Return DigRP Annunciator %d to Annunciator Conf.	Indicates an internal DigRP processing/ database error condition.
0161	Bad DigConf. Rec/Play Mode, DigRP Channel %c, Conf. %d	Indicates an internal DigRP processing/ database error condition.
0162	Error Starting DigConf. Rec/ Play, DigRP Channel %c, Conf. %d	Indicates an internal DigRP processing/ database error condition.
0163	Error Stopping DigConf. Rec/ Play, DigRP Channel %c, Conf. %d	Indicates an internal DigRP processing/ database error condition.
0164	DigRP Request %s on DigRP Channel %c - Not In Use	Indicates an internal DigRP processing/ database error condition.
0165	DigRP Request %s on DigRP Channel %c - Not Found	Indicates an internal DigRP processing/ database error condition.
0166	Error Executing DigRP Request %s on DigRP Channel %c	Indicates an internal DigRP processing/ database error condition.
0167	Flexible Annunciator Message Database Updated	An administrator updated the flexible annunciator message database.

Message Code	Message	Meaning
0168	LAN configuration updated.	An administrator changed the LAN configuration.
0174	Rebuilt conference scheduler shared database.	This message follows 0134 on a system running the Conference Scheduler (administrator resets system date/time) or 0146 (administrator activates Conference Scheduler). The system updates the scheduler database after these events.

1000–1999: User/Usage Messages

Table 22: User/Usage Messages

Message Code	Message	Meaning
1001	USAGE: %s <terminal %d (1-%d)>	Process was spawned with insufficient command line arguments.
1003	USAGE: %s <display %d 1-10>	Tells how to run %s from the command line.

2000–2999: Process Interface Messages

Table 23: Process Interface Messages

Message Code	Message	Meaning
2000	*MakeNull/Add/Peek/ Delete* link list failure	The specified software operation with respect to link lists failed.
2001	Cannot start/stop timer	An attempt to start or stop a timer provided by the timer process or to create a queue for such timers failed.
2002	Reply_dial_done error	A failed attempt to inform the call handler that a previous request to dial a number was completed.
		1 of 3

Table 23: Process Interface Messages (continued)

Message Code	Message	Meaning
2003	Report_DSP_fail error	A process was unable to inform the call handler that a DSP failed.
2004	Report_digits error	The event process was unable to inform either the call handler that DNIS digits have been received or the command process that DTMF digits have been received.
2005	Cmd_dial_done error	A failed attempt to report to the command process that dialing is completed.
2006	Cmd_tone_done error	A failed attempt to report to the command process that a tone is completed.
2100	Error message has unknown source key 0x%d	The log process has been requested to enter a log message from an unknown process with the specified source key.
2101	Received unknown command 0x%d	A process received a message to perform an unknown or unsupported operation with the specified command number.
2102	Undefined message type 0x%X received from process %d	Indicates a message has been received by a process that could not be processed.
2104	Unknown delayed command (0x%d) for channel %d	The command process does not recognize the specified command that it saved for delayed processing on the specified logical channel number.
2200	Poll returned unexpected 0x*XX* event	A process detected an unexpected event while polling for data to be received or sent. *XX* indicates the hexadecimal value of the unexpected event.
2201	Process terminating - unable to obtain information for hostname '*host-name*'	A LAN process terminated trying to set up a listener for a particular LAN service because it was unable to obtain IP address information regarding hostname *host-name* from the /etc/ hosts file.
		2 of 3

Table 23: Process Interface Messages (continued)

Message Code	Message	Meaning
2202	Process terminating - '*service-name*' service not found in '/etc/services' file	A LAN process terminated trying to set up a listener for a particular LAN service because it was unable to obtain port assignment information regarding service *service-name* from the /etc/services file.
2203	CDR sequence error for *MM/DD*: last=*NNNNN*, current=*NNNNN*	The "autocdr" LAN process was not able to sync up with the call handler after sending data from a CDR file for that current day of *MM/DD*. last=*NNNNN*, indicates the last sequence number read from the CDR file and current=*NNNNN*, indicates the current sequence number received from the call handler to be sent next.
		3 of 3

3000–3999: UNIX System Error Messages

These are UNIX *directory, file, fork/exec, alloc, shm, lock, prio, rtalarm,* and *ipc* errors.

Table 24: Unix System Error Messages

Message Code	Message	Meaning
3000	Cannot change to *name* directory	The process cannot change to the specified directory. The directory may be missing or have the wrong permissions.
3001	Cannot open *name* directory	The process cannot open the specified directory. The directory may be missing or have the wrong permissions.
3002	Cannot get current working directory	An error was returned from the c function getcdw (3c).
3100	Cannot load DCB database	Process had an error attempting to read in the .dat files.
3105	Cannot save DCB database	One of .dat files had a general write error.
		1 of 4

Table 24: Unix System Error Messages (continued)

Message Code	Message	Meaning
3106	Cannot access `*name*'	A process cannot determine the status of the specified file.
3107	Cannot move file from *source* to *destination*	A file cannot be moved from one name and/or directory to another. Permission may be wrong, the directory may be missing, or the name invalid.
3108	Cannot open *name*	The specified file cannot be opened. It may be missing or have the wrong permissions.
3109	Failed to load '*name'* file	The specified file cannot be downloaded to a DSP.
3110	File not COFF format	A file to be downloaded to a DSP has the wrong format for downloading.
3111	Cannot read *name*	The specified file cannot be read.
3112	Cannot seek *name*	An attempt to move to a desired position in the specified file failed.
3114	Cannot write *name*	An attempt to write the specified file failed.
3115	Cannot get/set controls for *device*	An attempt to read or write control information for the specified device failed.
3117	Cannot extend RTFS file *name*	An attempt to increase the size of the specified real-time file failed.
3118	Cannot *write/read* RTFS file *name*	An attempt to perform the specified operation on the named file failed.
3200	Cannot execute *process*	An attempt to start execution of the specified process failed.
3201	Cannot start *name* process	An attempt to start execution of the specified process failed. A previous log message gives more details.
		2 of 4

Table 24: Unix System Error Messages (continued)

Message Code	Message	Meaning
3202	Failed to create process for *name*	The specified process could not be created for execution.
3203	Process '%s %d' %s	Receive a SIGCLD signal on specified process.
3204	Process '%s %d' Respawning Too Rapidly	The system terminated respawning of a dead process.
3304	Cannot initialize alarm database	An attempt to initialize the alarm database failed.
3305	Cannot map dual-port memory	A failed attempt to write the reference memory using the dual-port memory defining DSo timeslots for use by the transmit PLD on the MVIP bus.
3306	Out of memory for announcement %d	No memory was available for use by the specified announcement.
3307	Out of memory	No memory was available for internal use by a process.
3400	Cannot initialize shared memory	Could not initialize (latch onto) the shared database. System probably not running.
3401	Cannot initialize shared database	An error occurred while trying to latch onto the shared database.
3402	Cannot open shared database	A process was unable to access the shared database.
3501	Rt_lock error	A process was unable to lock itself into memory for quick response to external events.
3600	Cannot set real time priority	An attempt to specify the priority of a process failed.
3700	Cannot set/cancel real time alarm	A request for a real time alarm failed.
3802	Cannot receive IPC message	Interprocess communication failed when a process attempted to receive a message.
		3 of 4

Table 24: Unix System Error Messages (continued)

Message Code	Message	Meaning
3805	Cannot send message to *process*	Interprocess communication failed when a process attempted to send a message to the specified process.
3900	Process terminating - *func-name* function call failed	A LAN process terminated trying to set up a listener for a particular LAN service due to either inadequate system resources or a system/software error when trying to execute *func-name*.
3901	Error receiving data from host '*host-name'* at IP address *IP-addr*	A LAN process received an error while trying to read socket data from host *host-name* at IP address *IP-addr*. This error may occur due to either inadequate system resources or a LAN hardware/software problem.
3902	Error sending data to host '*host-name'* at IP address *IP-addr*	A LAN process received an error while trying to send socket data to host *host-name* at IP address *IP-addr*. This error may occur due to either inadequate system resources or a LAN hardware/software problem.
		4 of 4

4000–4999: Hardware and Device Messages

Table 25: Hardware and Device Messages

Message Code	Message	Meaning
4000	Annunciator ready event %d failed for channel %d	An attempt to report to the annunciator process that the specified buffer is ready for the logical channel failed.
4001	Cannot get attributes for output device	A TCGETA call to ioctl returned an error.
4007	Error %d: [%s] during network driver operation: %s	Indicates that a network driver error occurred. This occurs only when the network software loses synchronization. with the network driver (for example, after system reinitialization).
4008	Cannot set attributes for output device	A TCSETAF call to ioctl returned an error.
4009	Cannot configure analog board	An attempt to configure the analog board failed.
4010	Cannot get DSP memory address	An attempt to get the physical address at which DPM is mapped from the DSP driver failed.
4011	Cannot get DSPs installed	An attempt to determine the installed DSPs from the DSP driver failed.
4012	Cannot get active DSP nodes	An attempt to determine the active DSPs from the DSP driver failed.
4013	Cannot get/return interrupt vector	An attempt to acquire or return control of an interrupt vector for testing purpose failed.
4014	Cannot initialize alarms	Failed to set real-time I/O operation to allow the read/write access necessary to placate the deadman timer.
		1 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4015	Network %s failure	A library call to (enable or disable) a network card returned failure. Will always follow a 4007 when logged from maintenance.
4016	Cannot get/set DSP register for board %d	A request to the DSP driver to read or write a register on the specified DSP board has failed.
4019	Put_(in) active error	An attempt to set a DSP node active or inactive has failed.
4020	Read_intr error	The event process failed to read a interrupt message from the DSP driver.
4100	*device* diagnostic failed	The diagnostic for the specified device failed.
4101	*device* diagnostic passed	The diagnostic for the specified device was completed with no problems found.
		2 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4103	DSP reports error %d on channel %d	A DSP reported error on the specified logical channel number. Recognized errors are: 1 - ILLEGAL_COMMAND .set 1. This command never gets reported. If an illegal command is detected, the system ignores it and goes to the next channel. 2 - RECORD_ERROR .set 2. The DSP encountered an error during a record operation. 3 - PLAY_ERROR .set 3. The DSP encountered an error during a playback operation. Possible causes include: - Non annunciator channel is asked to play or record. - Annunciator channel is asked to play/record when it is already so doing. - Annunciator channel tries and fails to grab a semaphore while playing/recording. 4 - DTMF_CHAR_ERROR .set 4. The DSP detected an invalid character in the digit array.
4104	DSP node %d diagnostic failed	The diagnostic for the specified DSP failed.
4105	Failure detected on DSP node %d	A process reported that the specified DSP failed.
4106	Invalid data (0x%d) for channel %d	The host found that a DSP contains the indicated invalid event buffer tail index for the specified logical channel number.
4107	Network %d failed- switch: %c, memory: %s, stream” %d, channel %d	The memory diagnostic for the specified network failed for the indicated switch, memory, stream, and channel.
		3 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4108	Network in service - %s channel(s) [%s] restored	Indicates a network trunk has come into (gone out of) service. The channel types (for example, User or Remote Operator) and channel numbers are variables.
4109	Network out of service - %s channel(s) [%s] removed from service	Indicates a network trunk has come into (gone out of) service. The channel types (for example, User or Remote Operator) and channel numbers are variables.
4110	Unexpected DSP command 0x%d on annunciator %d	An announcement or playback has been requested on the indicated annunciator which is busy with the specified command.
4111	DSP node %d: expected 0x%d got 0x%d at 0x%d	During DSP testing, the specified DSP expected to read one value, but got another, at the specified address. If expected value and read value do match, the host received the correct value on the second read.
4112	DPM corrupted	A process has detected that one of the circular buffers maintained in dual-port memory was corrupted. The command process or the init process found a problem with the head of the remove-talker buffer, or the event process found a problem with the head of the event buffer.
4113	DSP node %d - not running	During DSP testing, the specified DSP was not started as desired.
4114	DSP node %d - not responding to *test*	The downloaded DSP test code does not respond for the specified test.
4115	DSP node %d *test*: Undefined response: 0x%d	The downloaded DSP test code gave an undefined response to the specified test.

4 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4116	DSP Board %d cannot set MVIP reference memory	An attempt to write the reference memory for the specified DSP board via the dual-port memory defining DS0 time slots for use by the transmit PLD on the MVIP bus failed.
4117	DSP Board %d fails MVIP *RX/TX* ping pong test	The specified MVIP control test failed for the specified DSP board.
4118	DSP node %d - minimum MVIP *RX/TX* frame count %d, got %d & %d	The specified DSP failed the MVIP frame count test. The received counts should have been at least as much as the specified amount and be different by no more than one.
4119	DSP node %d interrupts: Sent %d, DSP got %d, Host got %d	During DSP testing, the host sent the specified number of interrupts to the DSP. The number received by the DSP and the number received by the host in return are also specified.
		5 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4120	*name* %d path error code %d	During connectivity testing of the named path, the error specified by the two digit code was detected. The first digit identifies a problem encountered in the test: 1 - The digits received identify the wrong channel path. 2 - An unknown event was received from a DSP. 4 - An unexpected command was detected in the channel used for testing. 8 - A DSP required for the test has failed or is not present. Any other hexadecimal number recorded for the first digit is the sum of the above digits for the problems indicated. The second digit indicates the number of DTMF digits detected over the specified path. Three digits must be received that correctly identify the channel path being tested.
4121	DSP %d MVIP Ref Memory: Wrote 0x%d, got 0x%d at 0x%d	During testing of the specified DSP, the host wrote the specified value and read a different value at the specified memory address.
4122	DSP node %d *test* command: Wrote 0x%d, got 0x%d	During the specified DSP test, the specified command was written, but the DSP got a different one or did not recognize the command.
4123	DSP node %d *test* parameter: Wrote 0x%d, got 0x%d	During the specified DSP test, the specified parameter was written, but the DSP got a different one or did not recognize the parameter.
		6 of 7

Table 25: Hardware and Device Messages (continued)

Message Code	Message	Meaning
4124	DSP %d *test* Mem: After %d cycles, DSP wrote 0x%d, got 0x%d at 0x%d	After the specified number of cycles of the specified DSP memory test, the DSP wrote the specified value and got a different one at the specified location.
4125	DSP node %d Transmission: Sent 0x%d, got 0x%d at 0x%d	During the specified MVIP transmission test, the DSP sent the specified byte and received a different value at the specified word address.
4126	*device* diagnostic completed	A diagnostic for the specified device has been completed. Problems, if any, have already been logged.
4127	MVIP Connection Initialization Failed, Result %d	Initialization of the T1/MVIP switch connection failed with the specified result code.
4128	DSP node %d: responded to %d at 0x%d	During DSP testing, the specified DSP node responded to a write request that was intended for the specified DSP response node at the specified location.
4129	DSP node %d: reports a missing frame sync	The specified DSP reported that it missed frame synchronization while performing other work. This is not a serious condition unless it happens repeatedly within the same second or two on the same DSP.
4130	ESQL. %d. %s.	An embedded SQL error occurred in either sqlsd (the SQL server daemon) or pdbadmin. The first string contains either the SQL statement that failed or the function name in which the error occurred. The next two arguments are provided by Informix. The first is an Informix error code that can be looked up in Informix documentation.
		7 of 7

Application Server Errors

The following sections describe errors which are unique to the S6200/S6800 Conferencing Servers

Debug Process Errors

Message: DEBUGPROCCESS Couldn't find interface for %s

Meaning: Can not find information for named process in processTable.cfg.

Corrective Action: Either load backup copy of processTable.cfg or manually add the information for the missing process.

SIP Utility Messages

Message: Can't print a message of %d chars

Meaning: The software can handle user input messages that are 2-5 bytes, but not other lengths.

Corrective Action: No action required. The user should try to enter the expected number of digits.

Message: Media Server is not in the process table

Meaning: The media server process was not found in processTable.cfg

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add a media server process.

Message: Error Couldn't find appsendto interface

Meaning: Could not find the process to which the media server sends messages.

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add the to which the media server sends messages

Message: Error Couldn't find DSP send to interface

Meaning: Could not find the process which handles network events.

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add the process

Message: Error Couldn't find the init process Key

Meaning: Could not find the IPC message queue ID in processTable.cfg

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add the process

Message: Error Creating IPC on start up: %s,strerror(errno)

Meaning: Failed to create an IPC message queue. The message contains the error number which is defined in /usr/include/sys/errno.h

Corrective Action: Make sure the software is running as root. If you logged in as another user to manually stop or start the software, you must first “su root”. If that is not the problem, the system may be out of resources. The safest way to fix that is to reboot.

Message: ERROR: msgctl() failed. errno=%d. qid=%d\n, errno, id

Meaning: Failed to increase the size of an IPC message queue

Corrective Action: Make sure the software is running as root. If you logged in as another user to manually stop or start the software, you must first “su root”. If that is not the problem, the system may be out of resources. The safest way to fix that is to reboot.

Message: ERROR: msgctl() failed. errno=%d. qid=%d\n, errno, id

Meaning: Failed to read the seize of an IPC message queue.

Corrective Action: Make sure the software is running as root. If you logged in as another user to manually stop or start the software, you must first “su root”. If that is not the problem, the system may be out of resources. The safest way to fix that is to reboot.

Message: ERROR: msgsnd() failed. errno=%d. destKey= 0x%x q=%d total send errors %d\n,

Meaning: Failed to send an IPC message.

Corrective Action: Log in and use the “ipcs -qa” command.

Look for the message queue with the matching key.

Determine if the queue is full. If it is, then restart that process or the server software.

If the message queue doesn't exist, then restart the process which reads messages from that queue.

The system may be out of messages.

Message: [%d] Unknown event queue to process[%d].

Meaning: An IPC message contains an unknown message queue ID

Corrective Action: Check the configuration in processTable.cfg. Make sure the event queue and process are listed. Then check the process is running using the “dcbps” command line utility. If that looks good, then restart the software.

Message: No entry for the process%s “,interface.c_str()

Meaning: There was no record in processTable.cfg for the named process

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add the information for the missing process.

INIT Messages

Message: %s is not in the process table ,IPCBINIT_PROC_NAME

Meaning: There was no record in processTable.cfg for the named process.

Corrective Action: Either load a known good backup copy of processTable.cfg or manually edit it to add the information for the missing process.

Message: started process=<%s> with pid=<%d>. Args=<%s/%s>

Meaning: This is only an error if proceeded by a message saying a process ended (killed, aborted, exited, etc

Corrective Action: If a process is frequently restarting, it could be caused by: 1. Lack of some resource, 2. A timeout, 3. Internal error. Restart the software

Message: unable to start process=<%s>

Meaning: The executable file for the process may not exist, or it may not be set to be executable, or you may have manually started the software as a normal user when you should start the software with "root" permissions.

Corrective Action: 1. Look for the name of the executable program in processTable.cfg.

2. Go to /usr/dcb/bin to see if the executable file exists.

3. See if the file is owned by "root" and the permission for the file includes an "x" for the file owner.

4. See if the system is out of virtual memory using the SCO administration utilities. If it is out of memory, then reboot

Message: process <%s> not responding after %d tries

Meaning: A process is not replying to poll messages, probably because it is overloaded, or locked.

Corrective Action: The software should automatically restart the process to recover. If not,

1. The system may be overloaded. Use the "ipcs -qa" message to see if the message queue has many messages in it. If that is the case, a faster CPU and more RAM may help.

2. There could be an internal error in that process.

Message: select() error=%d

Meaning: There was an error in the "select" command which is used to delay a few seconds. The error message includes an error code which is defined in /usr/include/sys/errno.h

Corrective Action: Look up the error code in /usr/include/sys/errno.h. Then take the corrective action implied by the error code.

Message: sleeping for another %x seconds

Meaning: The process is waiting for the specified period. This is not an error.

Corrective Action: None

Message: unknown queue id responded %d, recvdQueueID

Meaning: The program got a message with an unknown message queue ID.

Corrective Action: This may be caused by an internal software error.

Message: restarting process=<%s>,

Meaning: A process was automatically restarted. That is done to recover when a process ends unexpectedly, or when the init process kills a process that appears to be frozen.

Corrective Action: 1. The system may be overloaded. Use the “ipcs -qa” message to see if the message queue has many messages in it. If that is the case, a faster CPU and more RAM may help.

2. There could be an internal error in that process.

Message: Killed process=<%s> with pid=<%d>

Meaning: A process was killed. Either because:

1. The process failed to respond to poll messages which implies it is either overloaded or stuck.

2. The system is shutting down.

Corrective Action: Look for previous messages to see the sequence of events. If there are previous messages about this process not responding, then that process could either be overloaded or stuck. If the process repeatedly dies and restarts, try restarting the software. If that fails to resolve the problem, try rebooting the machine.

Message: Can't kill missing process=<%s> with pid=<%d>

Meaning: The init process tried to kill a process that doesn't exist. Usually that means the process aborted or exited already

Corrective Action: Normally no action is needed. The init process should automatically restart the process.

Message: Error %d when killing process=<%s> with pid=<%d>

Meaning: A system error occurred when killing a process.

Corrective Action: Look up the error code in /usr/include/sys/errno.h. Take the corrective action implied by the error code.

Message: Error %d in waitpid, errno

Meaning: A system error occurred when trying to determine why a process ended.

Corrective Action: Look up the error code in /usr/include/sys/errno.h. Then take the corrective action implied by the error code.

Message: Process %s id %d exited normally with exit status %d

Meaning: A program exited with the specified code. Normally a zero means the program ended normally while a nonzero number means an error occurred.

Corrective Action: This message is only an error if a program ends when it is not expected to end. This message is normal when the system is shutting down.

Message: Process %s id %d killed by signal %d

Meaning: A program was killed by init or some other process, or by a signal generated by the process that died. The signal that killed the process is listed.

Corrective Action: Look up the signal in /usr/include/sys/signal.h. If the signal is SIGABRT, SIGBUS, or SIGSEGV that is an internal Avaya error so contact Avaya support. The SIGTERM or SIGKILL signals are used by the init process. To see if those are related to a problem you need to look at the sequence of messages related to this process. If there are messages about a process not responding, then use the recommended corrective action for that.

Message: Process %s id %d stopped by signal %d

Meaning: A program was stopped by the specified signal. Normally a program is stopped by sending it a suspend signal. That is normally done from a shell and is not expected when the software is running in the background.

Corrective Action: Look up the signal in /usr/include/sys/signal.h. If the signal is SIGABRT, SIGBUS, or SIGSEGV that is an internal system error.

The SIGTERM or SIGKILL signals are used by the init process. To see if those are related to a problem you need to look at the sequence of messages related to this process. If there are messages about a process not responding, then use the recommended corrective action for that.

Message: invalid message=%x

Meaning: The message type in the message is wrong.

Corrective Action: This is probably caused by either in internal error or an incompatible mixture of different processes.

Index