



Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers

Release 10.2.x
Issue 5
March 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya 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 to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction	16
Purpose	16
Change History	16
Changes to platform support	17
Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)	17
Supported gateways	17
Safety labels and security alert labels	18
SAT Command syntax	18
Contention between simultaneous commands	19
The busyout and release commands	20
Displaying a list of every busied-out maintenance object in the system	20
Alarm and error categories	20
Common SAT command parameters	21
Common output field descriptions	22
Error messages	23
Common Error Codes	23
Chapter 2: Maintenance command descriptions	25
aar analysis	25
list aar analysis	25
aar route-chosen	26
list aar route-chosen	26
access-endpoint	27
busyout access-endpoint	27
release access-endpoint	27
status access-endpoint	28
test access-endpoint	29
administered-connection	30
disable administered-connection	30
enable administered-connection	30
status administered-connection	30
aevcs	31
reset aevcs link	31
status aevcs cti-link	31
status aevcs interface	32
status aevcs link	33
test aevcs-server	33
alarms	34
display alarms	34
test alarms	36
amw all	39

clear amw all.....	39
analog-testcall.....	39
test analog-testcall.....	39
announcement.....	40
add announcement.....	40
display announcement.....	40
erase announcement.....	40
list announcement.....	41
list int-annc-sources.....	41
announcement-board.....	42
disable announcement-board.....	42
enable announcement-board.....	42
ars analysis.....	42
list ars analysis.....	42
ars route-chosen.....	43
list ars route-chosen.....	43
list ars route-chosen field descriptions.....	44
attendant.....	44
status attendant.....	44
audio-group.....	45
list audio-group.....	45
list usage audio-group.....	46
audits.....	46
clear audits.....	46
status audits.....	46
bcms.....	48
monitor bcms.....	48
board.....	52
busyout board.....	52
release board.....	53
reset board.....	53
test board.....	53
bri-port.....	54
status bri-port.....	54
bulletin-board.....	61
display bulletin-board.....	61
calltype route-chosen.....	62
list calltype route-chosen.....	62
campon-busyout.....	63
campon-busyout.....	63
capacity.....	64
display capacity.....	64
cdr-link.....	74

busyout cdr-link.....	74
release cdr-link.....	74
status cdr-link.....	75
test cdr-link.....	76
cleared-alarm-notif.....	77
status cleared-alarm-notif.....	77
communication-interface links.....	77
change communication-interface links.....	77
display communication-interface links.....	78
communication-interface processor-channels.....	78
change communication-interface processor-channels.....	78
display communication-interface processor-channels.....	80
conference.....	80
status conference.....	80
configuration.....	111
list configuration media-gateway.....	111
list configuration software-versions.....	111
coverage path.....	112
list coverage path.....	112
craft2.....	113
enable craft2.....	113
disable craft2.....	113
cti-link.....	113
busyout cti-link.....	113
change cti-link.....	114
list cti-link.....	115
list usage cti-link.....	116
release cti-link.....	116
test cti-link.....	116
customer-alarm.....	117
test customer-alarm.....	117
data-module.....	118
busyout data-module.....	118
release data-module.....	118
status data-module.....	118
test data-module.....	119
digit-string.....	120
list usage digit-string.....	120
directory.....	120
list directory.....	120
list directory source.....	120
disabled-MOs.....	121
list disabled-MOs.....	121

disabled-tests.....	121
display disabled-tests.....	121
ds1-facility.....	122
busyout ds1-facility.....	122
test ds1-facility.....	122
ds1-loop.....	123
test ds1-loop.....	123
eda-external-device-alm.....	124
list eda-external-device-alm.....	124
test eda-external-device-alm.....	124
errors.....	125
clear errors.....	125
display errors.....	125
ess.....	129
disable ess.....	129
enable ess.....	130
status ess clusters.....	131
ethernet-options.....	133
get ethernet-options.....	133
list ethernet-options.....	134
set ethernet-options.....	134
events.....	135
display events.....	135
extended-user-profile.....	136
change extended-user-profile.....	136
display extended-user-profile.....	137
extension-type.....	137
list extension-type.....	137
failed-ip-network-region.....	138
display failed-ip-network-region.....	138
test failed-ip-network-region.....	138
file.....	139
remove file.....	139
filexfer.....	139
enable filexfer.....	139
firmware download.....	140
change firmware download.....	140
hardware-group.....	140
cancel hardware-group.....	140
resume hardware-group.....	141
status hardware-group.....	141
health.....	143
monitor health.....	143

status health.....	143
history.....	144
list history.....	144
notify history.....	147
cmdHistoryLogConfig.....	147
hunt-group.....	148
display hunt-group.....	148
list hunt-group.....	148
initcauses.....	148
display initcauses.....	148
integ-annc-board.....	150
list usage integ-annc-board.....	150
integ-annc-brd-loc.....	150
change integ-annc-brd-loc.....	150
ip-media-parameters.....	151
display ip-media-set.....	151
ip-interface.....	158
change ip-interface.....	158
ip-network-region.....	158
change ip-network-region.....	158
list ip-network-region.....	158
status ip-network-region.....	159
duplicate ip-network-region.....	160
ip-stations.....	160
reset ip-stations.....	160
ip-synchronization.....	162
status ip-synchronization.....	162
isdnpri-testcall.....	164
clear isdnpri-testcall.....	164
list isdnpri-testcall.....	164
status isdnpri-testcall.....	165
test isdnpri-testcall.....	166
journal-link.....	167
status journal-link.....	167
journal-printer.....	168
busyout journal-printer.....	168
release journal-printer.....	168
test journal-printer.....	169
led.....	170
test led.....	170
license.....	170
test license.....	170
link.....	171

busyout link.....	171
status link.....	171
test link.....	173
locations.....	174
list locations.....	174
location-parameters.....	174
list location-parameters.....	174
logging-levels.....	175
change logging-levels.....	175
display logging-levels.....	176
login-id.....	176
reset login-id.....	176
logins.....	177
status logins.....	177
marked-ports.....	177
list marked-ports.....	177
mct-history.....	178
list mct-history.....	178
measurements.....	179
list measurements aca.....	179
list measurements ds1.....	179
list measurements ip codec.....	181
list measurements ip dsp-resource.....	183
list measurements ip signaling-groups.....	195
media-gateway.....	196
add media-gateway.....	196
change media-gateway.....	200
display media-gateway.....	200
list media-gateway.....	201
reset media-gateway.....	202
status media-gateway.....	203
test media-gateway.....	204
Media Server.....	205
list media-server	205
add media-server.....	207
change media-server.....	208
display media-server.....	209
remove media-server.....	210
status media-server.....	211
meet-me-vdn.....	215
reset meet-me-vdn.....	215
mg-announcements.....	215
status mg-announcements.....	215

mg-return.....	216
enable mg-return.....	216
mis.....	217
busyout mis.....	217
release mis.....	217
modem-pool.....	218
release modem-pool.....	218
test modem-pool.....	218
moh-analog-group.....	219
list moh-analog-group.....	219
monitored-station.....	220
list monitored-station.....	220
mst.....	220
clear mst.....	220
change mst.....	220
disable mst.....	221
display mst.....	221
list mst.....	221
multimedia.....	223
list multimedia.....	223
network-region-group.....	224
list members network-region-group.....	224
list network-region-group.....	224
night-service.....	224
list night-service attendant.....	224
list night-service hunt-group.....	225
list night-service trunk-group.....	225
node-names.....	226
display node-names.....	226
nr-registration.....	226
disable nr-registration.....	226
enable nr-registration.....	227
status nr-registration.....	228
options.....	230
set options.....	230
off-pbx-telephone.....	233
status off-pbx-telephone station.....	233
list off-pbx-telephone station-mapping.....	234
periodic-scheduled.....	235
status periodic-scheduled.....	235
pin.....	236
change pin.....	236
reset pin.....	237

ping.....	237
ping.....	237
pms-down.....	239
list pms-down.....	239
pms-link.....	240
busyout pms-link.....	240
release pms-link.....	241
status pms-link.....	241
test pms-link.....	242
port.....	243
busyout port.....	243
clear port.....	243
display port.....	243
mark port.....	244
release port.....	244
test port.....	245
pri-endpoint.....	245
busyout pri-endpoint.....	245
release pri-endpoint.....	246
status pri-endpoint.....	246
test pri-endpoint.....	247
profile-base.....	248
display profile-base.....	248
psa.....	248
status psa.....	248
public-unknown-numbering.....	249
change public-unknown-numbering.....	249
display public-unknown-numbering.....	250
list public-unknown-numbering.....	250
registered-ip-stations.....	252
list registered-ip-stations.....	252
remote-access.....	253
status remote-access.....	253
remote-office.....	254
add remote-office.....	254
change remote-office.....	254
display remote-office.....	255
list remote-office.....	255
remove remote-office.....	255
status remote-office.....	255
security-violations.....	256
monitor security-violations.....	256
set-data.....	258

list set-data.....	258
shell.....	258
go shell.....	258
signaling-group.....	259
display signaling-group.....	259
list signaling-group.....	261
list usage signaling-group.....	262
remove signaling-group.....	263
set signaling-group.....	265
status signaling-group.....	265
test signaling-group.....	267
skill-status.....	268
list skill-status.....	268
socket-usage.....	269
monitor socket-usage.....	269
status socket-usage.....	270
sp-link.....	271
busyout sp-link.....	271
release sp-link.....	271
status sp-link.....	271
test sp-link.....	272
station.....	272
add station.....	272
busyout station.....	272
change station.....	273
list station.....	273
release station.....	274
status station.....	274
test station.....	287
survivable-processor.....	288
list survivable-processor.....	288
suspend-alm-orig.....	289
disable suspend-alm-orig.....	289
enable suspend-alm-orig.....	289
list suspend-alm-orig.....	290
synchronization.....	290
change synchronization.....	290
disable synchronization.....	291
display synchronization.....	291
enable synchronization.....	292
list synchronization.....	292
set synchronization.....	293
sys-link.....	293

list sys-link.....	293
system.....	294
monitor system.....	294
reset system.....	296
System-parameters customer-options.....	299
display system-parameters customer-options.....	299
system-parameters ip-options.....	300
change system-parameters ip-options.....	300
display system-parameters ip-options.....	300
system-parameters maintenance.....	300
change system-parameters maintenance.....	300
display system-parameters maintenance.....	305
system-parameters ms-recovery-rule.....	305
change system-parameters ms-recovery-rule.....	305
terminal.....	306
erase terminal.....	306
test-number.....	307
disable test-number.....	307
enable test-number.....	307
test-schedule.....	308
display test-schedule.....	308
testcalls.....	309
list testcalls.....	309
tftp-server.....	312
change tftp-server.....	312
display tftp-server.....	312
time.....	313
display time.....	313
set time.....	313
trace.....	314
list trace media-gateway.....	314
list trace ras.....	315
list trace station.....	315
list trace tac.....	316
list trace vdn.....	316
list trace vector.....	317
traffic.....	317
monitor traffic.....	317
translation.....	318
save translation.....	318
trunk.....	319
busyout trunk.....	319
monitor trunk.....	319

release trunk.....	320
status trunk.....	320
test trunk.....	323
trunk-group.....	324
list trunk-group.....	324
list measurements trunk-group summary last-hour.....	324
tsc-administered.....	324
status tsc-administered.....	324
test tsc-administered.....	325
tti.....	325
status tti.....	325
tti-ip-stations.....	327
list tti-ip-stations.....	327
user-profile.....	327
change user-profile.....	327
display user-profile.....	327
duplicate user-profile.....	330
export user-profile.....	331
import user-profile.....	331
list user-profiles.....	332
remove user-profile.....	333
user-profile-by-category.....	333
add user-profile-by-category.....	333
change user-profile-by-category.....	334
display user-profile-by-category.....	334
video-bridge.....	334
status video-bridge.....	334
vector.....	336
list usage vector.....	336
list vector.....	336
Chapter 3: Linux bash commands.....	337
Linux Commands.....	337
Introduction.....	337
Chapter 4: Related Media Gateway CLI Commands.....	385
set mgc list.....	385
Chapter 5: Resources.....	386
Communication Manager documentation.....	386
Finding documents on the Avaya Support website.....	388
Accessing the port matrix document.....	388
Avaya Documentation Center navigation.....	389
Training.....	390
Viewing Avaya Mentor videos.....	391
Support.....	391

Using the Avaya InSite Knowledge Base.....	391
Appendix A	393
PCN and PSN notifications.....	393
PCN and PSN notifications.....	393
Viewing PCNs and PSNs.....	393
Signing up for PCNs and PSNs.....	394

Chapter 1: Introduction

Purpose

This document provides information about the Avaya Aura® Communication Manager commands that monitor, test, and maintain the hardware components of an Avaya server or gateway system. You can use the commands to test, troubleshoot, and fix problems that could severely disrupt call processing.

The commands can be run from the Communication Manager web interface. For more information about using the web interface, see *Administering Avaya Aura® Communication Manager*.

System Access Terminal (SAT) commands apply to a number of servers and gateways and display different results depending on the configuration of the system. Some commands apply to only certain servers.

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers, and specifically by:

- Trained Avaya technicians
- Maintenance technicians dispatched to a customer site for troubleshooting an alarm or a user report
- Maintenance technicians located at a remote maintenance facility
- Assigned maintenance technicians of the customer

Change History

Issue	Date	Summary of changes
5	March 2026	Added the section: Changes to platform support on page 17
4	May 2025	Updated the following section: • enable filexfer on page 139
3	February 2025	Updated the following section: • list trace tac on page 316
2	April 2024	Updated the “list mct-history” section.
1	March 2023	Release 10.2

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the [End of sale G650 document](#) published on the Avaya Support website.

Supported gateways

The following table lists the supported gateways of Avaya Aura® applications.

Supported gateways	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
G430 Branch Gateway	Y	Y	Y	Y	Y
G450 Branch Gateway	Y	Y	Y	Y	Y
G650 Media Gateway	Y	Y	Y		

 Note:

From Avaya Aura® Release 10.2 and later, G650 Media Gateway is no longer functional.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems.

 Caution:

A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

 Warning:

A warning statement calls attention to a situation that can result in harm to hardware or equipment.

 Danger:

A danger statement calls attention to a situation that can result in harm to personnel.

 Security alert:

A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

SAT Command syntax

Each command consists of an action, an object on which the action is performed, and the required or optional qualifiers that modify the command. For example, in the `test station extension` [`short` | `long`] command:

- **test** is the action.
- **station** is the object.
- **extension** is a required qualifier.
- [**short** | **long**] are the optional qualifiers. A **pipe (|)** indicates the options: short or long.

You can abbreviate command words. The system recognizes a partially entered word when you type enough letters to distinguish the command from other valid entries. For example, you can type the `test alarms long clear` command as `t al l c`.

If you do not type enough letters, the screen displays a list of command words and qualifiers that match the abbreviation.

You can drop the leading zeroes from numeric entries. For example, you can type the cabinet number 03 as 3.

Press the **HELP** key to display the available commands and all valid qualifiers of the command.

The length of the hardware location differs for the various types of commands:

- `display media-gateway` requires a gateway number location. For example, `display media-gateway 233`.
- `test port` requires a location:
 - The gateway number, the media module number, and the port location. For example, `test port 5V90613`.

Contention between simultaneous commands

The following limits apply to maintenance and administration activities:

- Up to 21 users can log in to the system simultaneously.
- Up to 5 maintenance commands can run concurrently.
- Up to 10 administration commands can run concurrently.
- Only one command can run on a maintenance object or another system entity at a time. The restriction applies to the following commands:
 - `busyout`
 - `change`
 - `clear`
 - `recycle`
 - `release`
 - `remove`
 - `set`
 - `test`
- When an action command is running on a media module, the media module pack and all maintenance objects located on the pack are unavailable for other commands.
- Most commands require shared system resources to run. When the required resources are already in use, the command stops. Only one such command can run at a time.
- The display-only commands usually do not conflict with any other commands:
 - `display`
 - `status`

- `get`
- `monitor`

The busyout and release commands

The **busyout** command puts the object of the command in the maintenance-busy state. In the busyout state:

- The system removes the object from the active service, and the object is unavailable for call processing.
- The system drops the services that depend on the busied-out component. If the component supports a link, the system drops the link too.
- No scheduled or periodic background tests run on the object . Demand maintenance tests can be run on the object, but some tests require that the object be released to complete.
- The system logs a warning alarm with error type 18 for each busied-out object.
- To prevent the busyout of a particular bus, you must move dedicated tone time slots to the other half of the duplicated bus.

The **release** command releases the maintenance object from the maintenance busyout server and puts the server back into service. If you run the **release** command on an object that is not busied out, the command stops.

Displaying a list of every busied-out maintenance object in the system

Procedure

1. Type the `display errors` command .
2. Type `error type 18` in the **Error Type** field on the Hardware Errors Report screen.

Alarm and error categories

Use **display alarms** and **display errors** to generate reports for certain groups of maintenance objects.

Use the **Category** field of the input screen to restrict the report to the maintenance objects of a specific category. The **HELP** key displays a list of categories. You can use the other fields on the input screen to further customize the alarm and error report.

Common SAT command parameters

The following table lists the common command input parameters and their description:

Parameter	Meaning
schedule	Use schedule to specify a start time to run the command. When the command is executed, the output is sent to the system printer. schedule is available for the display, list, and test commands. • Enter list common-queue to display the commands that are queued for execution. • Enter remove common-queue job# to cancel a queued command. This command requires that the system printer is administered.
group#	The 1–3 digit trunk-group number.
group#/member#	The group number followed by a slash and a 1–3 digit member number of an individual trunk.
extension	The extension number assigned to the port or other maintenance object. The number of digits in an extension is determined by the system dial plan.
next	The next available number in the sequence.
repeat #	The number of times a test sequence is to be repeated.
short long	The type of test sequence to run for the maintenance object. The test sequence varies for each maintenance object. The short test sequence is always non-destructive and is the default.  Caution: For maintenance objects, long is destructive to call service.
clear	Used with test commands. clear repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests or until any test in the test sequence fails. If no alarms are active, the test sequence is run once. • long clear clears every alarm against the maintenance object if no errors are encountered. • short clear clears only alarms that are pertinent to the tests in the short test sequence.  Caution: If every test passes, long clear clears every error counter. If firmware counters are cleared while an actual problem exists, customer service can degrade due to calls being routed over faulty components.

Common output field descriptions

Output field	Field description
Port	Port location identifier. The port length differs for the various types of commands. A port circuit requires a full-length address such as 5V90613.
Maintenance Name	The name of the maintenance object as it displays in the alarm and error logs.
Alt. Name	The alternate name depends upon the type of the object. for example: • Station MO, Alt. Name = nnnnn (extension). • Trunk MO, Alt. Name = nn/n (trunk-group# / member#). • Personal CO MO, Alt. Name = P/23 (P/ personal CO line group #).
Test No.	The identification number of the test that is being run on the maintenance object as part of a <code>test</code> command. Descriptions of each test and related error codes appear under each maintenance object. For specific maintenance object information, see <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> .
Result	One of the following results: • PASS: The command successfully completed. For a <code>test</code> command, no errors were detected by the test. • ABORT: The command was prevented from completing. See Common Error Codes on page 23. • FAIL: A serious error was detected by the test. See Common Error Codes on page 23. • CONFLICT: Another user was testing this maintenance object. • DISABLED: The maintenance object or test was disabled by the <code>disable</code> command.
Error Code	Indicates the reason for a FAIL or ABORT result. For <code>test</code> commands that return a test result, consult the tables of test error codes under the relevant maintenance object in <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> . For <code>busyout</code> , <code>release</code> , and <code>reset</code> commands, see Common Error Codes on page 23.

Error messages

Error Message	Meaning
All maintenance resources busy; try again later	Every available maintenance resource is in use.
Command resources busy; Press CANCEL to clear, and then resubmit	A resource problem exists. Restart the command.
Error encountered; can't complete request	The command cannot be executed, because of corrupt software. Follow the escalation procedures.
Hardware-group command aborted with cancel command entered from another terminal	The test hardware-group command which is running in the foreground was successfully canceled with the cancel hardware-group command from another terminal.
'login id': 'command' has a command conflict	The command is in conflict with another executing command. The login id of the conflicting user and the conflicting command is shown.
Port/Board invalid	The format for the board location is incorrect.
save translations has a command conflict	An update of the standby server is in progress.

Common Error Codes

Error Code	Command Result	Description/Recommendation
	ABORT	System resources are unavailable to run the command. Try the command again at one-minute intervals up to 5 times.
0	ABORT	Internal system error. Retry the command at one-minute intervals up to 5 times.
1005	ABORT	A DS1 interface media module could not be reset because it is supplying the online synchronization reference. Use set sync to designate a new DS1 interface media module as the online reference, then try the reset again.
1010	ABORT	An attempt was made to busyout an object that was already busied out.
1011	ABORT	An attempt was made to release an object that was not first busied out.

Table continues...

Error Code	Command Result	Description/Recommendation
1015	ABORT	A reset of this media module requires that every maintenance object on it be in the out-of-service state. Use busyout board to place every object on the media module in the out-of-service state, and try the reset again.
1026	ABORT	The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use set tdm PC to switch the control channel and system tones to the other TDM bus.
1426	ABORT	The port cannot be released because the gateway has the Emergency Transfer Mode set. The user must use the command line interface of the gateway to clear the mode.
2012 2500	ABORT	Internal system error.
2100	ABORT	System resources to run this command are unavailable. Try the command again at one-minute intervals up to 5 times.
62524 62525 62526	ABORT	Maintenance is active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains many administered stations or trunks with installed media modules that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again.
	NO BOARD	The media module is not physically installed.
	FAIL	See the applicable maintenance object information in <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> .
	PASS	The requested action successfully completed. If the reset command was used, the media module is now running and must be tested.

Chapter 2: Maintenance command descriptions

aar analysis

list aar analysis

Use `list aar analysis` to view the parameters that the Automatic Alternate Routing (AAR) table uses to route a call.

Syntax

```
list aar analysis [start] [route] [location n|all] [node] [to-node] [count] [schedule]
```

start	This is an optional parameter. The digit string from which the system starts listing the aar analysis data.
route	This is an optional parameter. The route number that Communication Manager uses for the dialed string. The parameter value can be one of the following: • 1 to 2000 • r1 to r32 • p1 to p2000
location	This is an optional parameter. The location of the extension. The parameter value can be one of the following: • 1 to 2000 • all
node	This is an optional parameter. The first node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.
to-node	This is an optional parameter. The last node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.
count	This is an optional parameter. The number of stations that you want the system to display.

schedule This is an optional parameter. The time at which you want the system to print the output.

Field descriptions

Field	Description
Location	The location of the extension.
Dialed String	The dialed string that matches with the dialed string entry in the AAR Digit Analysis table.
Total Min Max	The minimum and maximum number of digits that you have administered to match with the dialed string.
Route Pattern	The route pattern that Communication Manager uses for the dialed string.
Call Type	The type of call for each dialed string.
Node Number	The destination node number in a private network when the system uses Node Number Routing or Distributed Communication System (DCS).
ANI Req'd	The value of this field denotes if R2-MFC and Russian MF ANI calls require ANI.

aar route-chosen

list aar route-chosen

Use the **list aar route-chosen** command to check the parameters that the Automatic Alternate Routing (AAR) table uses to route a call to a number. Using AAR, the system automatically selects the most desirable and least expensive route for calls over the trunk facilities at the customer's end.

Syntax

```
list aar route-chosen x [location n|all][partition n][schedule]
```

x The dialed number.

location n Optional. The location number. The parameter value includes:

- **1 to 2000**
- **all**

The default value is **all**.

partition n Optional. The partition group number. The parameter value ranges from **1** to **8**.

schedule Optional. The start time for the command.

Field descriptions

Field	Description
Location	The location entered on the command line.
Partitioned Group Number	The partitioned group number entered on the command line. The default value is 1 .
Dialed String	The dialed string matching with the dialed string entry in AAR Digit Analysis table.
Total Min Max	The minimum and maximum lengths matching with the minimum and maximum length entries from the AAR Digit Analysis table.
Route Pattern	The pattern number used to route the call.
Call Type	The call type matching with the call type entry from the AAR Digit Analysis table. For more information on call type, see <i>Avaya Aura® Communication Manager Screen Reference</i> .
Node Number	The node number matching with the node number entry from the AAR Digit Analysis table.
Actual Outpulsed Digits by Preference	The digits transmitted when you choose each of the preferences in the route pattern.

access-endpoint

busyout access-endpoint

Use the **busyout access-endpoint** command to busy out an access endpoint.

For more details on busyout commands, see [Busyout and release commands](#) on page 20.

Caution:

busyout access-endpoint command drops an active call on the endpoint.

Syntax

```
busyout access-endpoint extension
```

extension The extension of the access endpoint that needs to be busied out.

release access-endpoint

Use the **release access-endpoint** command to release all ports from the busy state. Communication Manager performs the periodic and scheduled tests and completes the background initialization testing on the released ports.

The **Port** field displays the port address of the released access endpoint.

For more information about busyout and release commands, see [Busyout and release commands](#) on page 20.

Syntax

```
release access-endpoint extension
```

extension The extension of the access endpoint that needs to be released.

status access-endpoint

Use the **status access-endpoint** command to check the operational status of an access endpoint.

Syntax

```
status access-endpoint extension
```

extension The extension of the access endpoint.

Field descriptions

Field	Description
Extension	The extension number of the access endpoint.
Port	The physical location of the port, including media gateway, slot, and circuit, to which the access endpoint is connected.  Note: For the wideband access endpoint, the location is the starting port.
Communication Type	The type of communication that the channel supports. Values of this field include: • 56k-data • 64k-data • voice-band-data • voice-grade-data • wideband
Width	The width of the access endpoint For communication types 56k-data, 64k-data, voice-band-data, and voice-grade-data, the width is 1 For communication type wideband, the width is the number of DS0s that make up the access endpoint

Table continues...

Field	Description
Service State	The operational status of the access endpoint channel. Values of this field include: • in-service or active • in-service or idle • out-of-service • maintenance-busy • disconnected
Connected Ports	The location of any facility or endpoint to which this access endpoint is connected.

test access-endpoint

Use the **test access-endpoint** command to perform the hardware diagnostic tests on all the port circuits associated with an access endpoint.

Syntax

```
test access-endpoint extension [ short | long | repeat n | clear ]
```

extension The extension of the access endpoint. The number of digits is determined by the dial plan.

short Perform a series of non-destructive diagnostic tests.

long Perform a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and non-destructive tests.

repeat n The number of times to repeat the test sequence.

clear Repeat the test sequence until the alarm is cleared or until a single test in the sequence fails.

Examples

```
test access-endpoint 25012
test access-endpoint 45002 sh
test access-endpoint 45892 l
test access-endpoint 24389 sh r 4
test access-endpoint 34899 l r 6
test access-endpoint 93483 r 2
test access-endpoint 10022 c
```

administered-connection

disable administered-connection

Use the **disable administered-connection** command to stop scheduled and periodic testing and to stop processing of inline errors for all or selected administered connections.

To view the administrative information for administered connections, use the **list administered-connection** and **display administered-connection** commands.

Syntax

```
disable administered-connection [ a-c# | all ]
```

a-c# The number assigned to the administered connection during administration.

all Disable all administered connections.

Example

```
disable administered-connection all
disable administered-connection a-c1
disable administered-connection a-c2
```

enable administered-connection

When maintenance is disabled using the **disable administered-connection** command, use the **enable administered-connection** command to re-enable scheduled and periodic testing and inline error processing on a specified administered connection or every administered connection.

Using administered connection commands, you can isolate the results of certain maintenance processes by preventing interference.

To view administrative information for administered connections, use the **list administered-connection** and **display administered-connection** commands.

Syntax

```
enable administered-connection a-c # | all
```

a-c# The number of the administered connection assigned during administration.

all Enable all the administered connections.

status administered-connection

Use the **status administered-connection** command to see the operational status of an administered connection.

Syntax

```
status administered-connection a-c #
```

a-c# The number of the administered connection assigned during administration.

status administered-connection field descriptions

Field	Description
Connection Number	The number assigned to the administered connection.
Enabled	The status that shows whether the administered connection is enabled.
Originator	The extension of the access or data endpoint that initiates the connection.
Destination	The destination address used to route the administered connection.

aesvcs

reset aesvcs link

Use the **reset aesvcs link** command to reset an AESVCS link. This command closes the socket connection and the AES server attempts to reconnect.

For more information on links, see the **status link** command.

Syntax

```
reset aesvcs-link n/n
```

n/n The AESVCS server number and the AESVCS link number.

Example

```
reset aesvcs link 01/01
```

status aesvcs cti-link

Use the **status aesvcs cti-link** command to see the status of all the CTI links associated to AES servers on the AE Services Administration page of the IP Services screen administered using the **change ip-services** command. These links provide connectivity to ASAI adjuncts, which are connected to an Ethernet LAN.

For more details on links, see the **status link** command.

Syntax

```
status aesvcs cti-link
```


status aesvcs cti-link field descriptions

Field	Description
CTI Link	The CTI link number. The field value range is 1–16.
Version	The negotiated ASAI protocol version.
Mnt Busy	The status indicating whether maintenance is busy. Values include <i>y/n</i> . If the value is <i>y</i> , the link has been busied out using the busyout cti-link command. Use the release cti-link command to release the busied out link.
AE Services Server	The name of the AES server on the AE Services Administration page of the IP Services screen administered using the change ip-services command.
Service State	The status of the TCP/IP tunnel connection and CTI link. Values include down/established .
Msgs Sent	The number of ASAI messages sent during a specified 30-minute window collection period.
Msgs Rcvd	The number of ASAI messages received during a specified 30-minute window collection period.

status aesvcs interface

Use **status aesvcs interface** command to see the status of the interfaces on which Communication Manager checks for AESVCES server connections.

Syntax

```
status aesvcs interface
```

status aesvcs interface field descriptions

Field	Description
Local Node	The name of the AESVCS interface as administered on the IP Services screen using the change ip-services command.
Enabled	The status whether the interface is enabled, as set on the Enabled field on the IP Services screen using the change ip-services command.
Number of Connections	The number of active AESVCS server connections on the interface.
Status	The current status of the interface: - Disabled — the <i>Enabled</i> field is set to <i>n</i> on the IP Services screen administered using the change ip-services command for the interface. - Intfce-down — the interface is not functioning and cannot accept incoming communications. - Listening — the interface is running and AESVCS servers can connect over it.

status aesvcs link

Use the **status aesvcs link** command to see the status of all the active sockets associated with AES servers. The sockets are administered on the AE Services Administration page of the IP Services screen using the **change ip-services** command.

For more information on links, see the **status link** command.

Syntax

```
status aesvcs link
```

status aesvcs link field descriptions

Field	Description
Srvr/Link	The AES server ID from the AE Services Administration page and the AE Services link number. The field value range is 1–16.
AE Services Server	The name of the AES server.
Remote IP	The IP address of the AESVCS link (AESV-LNK) connection on the AES server.
Remote Port	The TCP/IP port of the AESVCS link connection on the AES server.
Local Node	The node name of the interface on which the AES server is connected and the v6 addresses of the node.
Msgs Sen	The number of ASAI messages sent during the 30-minutes moving window collection period.
Msgs Rcvd	The number of ASAI messages sent during the 30-minutes moving window collection period.

test aesvcs-server

Use the **test aesvcs-server** command to run diagnostic tests on the specified AESVCS server and any associated AESVCS links (AESV-LNK).

Syntax

```
test aesvcs-server 1-16 [ short | long ] [ repeat # | clear ] [schedule]
```

1–16 The AES server number 1–16.

short Perform a series of non-destructive diagnostic tests.

long Perform a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and non-destructive tests.

repeat # The number of times to repeat the test.

clear Repeat the test sequence until any active alarms against the AES server are cleared by the passing of tests, or until any test in the sequence fails.

schedule Specify a start time for the command.

Example

```
test aesvcs-server 4 long repeat 3
```

alarms

display alarms

Use the **display alarms** command to see the hardware alarm report. Use this report to select the alarms to be displayed.

The system creates the hardware alarm reports from the logs of the maintenance subsystem that monitors the system hardware and logs problems as errors or alarms. The type of alarm indicates the impact of the problem. Following are the types of alarms:

- **Warning alarm** — Indicates a problem that is important to log or external to the system, but does not cause a noticeable degradation of service.
- **Minor alarm** — Indicates a problem that can disable a local area of the system and noticeably degrade the system.
- **Major alarm** — Indicates a problem that widely degrades the system and impairs service. The system places a call to INADS.

A resolved alarm is a problem that has been corrected, and the alarmed component of the system is functioning correctly again. The system stamps resolved alarms with the date and time the problem was corrected. The system handles any errors associated with the alarms as **resolved**.

Syntax

```
display alarms [ schedule ]
```

schedule Specify a start time for the command.

display alarms field descriptions

Field	Description
Alarm Types	Enter y or n in the alarm type fields to specify the type of alarm to display on the report. You can choose a combination of: • active or inactive alarms. • major, minor, or warning alarms. • resolved or unresolved alarms.

Table continues...

Field	Description
Interval	Enter m, h, d, w or a to display alarm records for the last month, last hour, last day, last week, or all. • From: Display alarm records from the time specified by mm/dd/hh:mm, where mm is the month, dd is the day, hh is the hour and mm is the minute. If no From date is defined, the report includes every alarm active since a month before to the current time. • To: Display alarm record to the time specified by mm/dd/hh/mm, where mm is the month, dd is the day, hh is the hour, and mm is the minute. If no To date is entered, any alarm that is active after the From date is used.
Equipment Type	Identify the equipment type that you want on the report. If there is no input to these fields, the system defaults to every type. • Gateway: Display every alarm associated with a particular gateway. • Board Number: Display every alarm associated with a particular media module. Alarms for a media module are referenced by media gateway. • Port: Display every alarm associated with a particular port on a media gateway. Alarms for a port circuit are referenced by port location Mediagateway#-mediamodule#-circuit. • Category: Enter a category to restrict the report to maintenance objects in a specific category. The Help key displays a list of categories. • Extension: Alarms associated with an extension number. • Trunk (group/member): Display every alarm associated with a particular trunk group or trunk-group member.

Input for display alarms

Enter **display alarms** to display the Alarm Reports options screen. Select different options on this screen for the type of report you want to see and press **Enter**.

Table 1: Alarm Report field descriptions

Field	Description
Port	The location of the alarmed object.
Maintenance Name	Name of the MO as it is in the alarm and error logs.

Table continues...

Alt. Name	Alternate name depends upon the type of the object. For example: • Station MO, Alternate Name = nnnnn (extension) • Trunk MO, Alternate Name = nn/n (trunk-group#/member #) • Personal CO line MO, Alternate Name = P/xx (P/personal CO line group #)
Alarm Type	Major, Minor, or Warning is an indicator of the seriousness of the alarm.
Service State	Service state of the station and trunk ports: • RDY — ready for service • OUT — out of service • IN — in service • [Blank] — No associated service state
Ack	Headings 1 and 2 identify the first and second OSS telephone numbers, respectively. The entries in the column below ACK indicate the acknowledged alarm state: • y — alarm has been acknowledged • n — alarm has not been acknowledged • c (cleared) — alarm was first acknowledged, then resolved and cleared • [Blank] — no attempt was made to report the alarm If the user disables the alarm origination with change system-parameters maintenance, then the Ack field is blank regardless of the true acknowledged state of the alarm.
Date Alarmed	Day, hour, and minute of alarm.
Date Resolved	Day, hour, and minute of resolution. 0 for active alarms.

Feature interactions for display alarms

If the alarm origination is disabled by **change system-parameters maintenance**, the Ack field is blank regardless of the true acknowledge state for the alarm.

If **second-as-backup** is entered in the Alarm Origination to OSS Numbers field, the column under the heading 2 will be blank for the alarms that the switch has not attempted to send to the second OSS telephone number. For the alarms that the switch has attempted to send to the second OSS telephone number, the column will be **y**, **n**, or **c**, depending on the acknowledgment status of the alarm. After the call to the first OSS telephone number is successful, for the alarms that the switch has attempted to send to OSSN2, the column will be consistent with the column under heading 1.

test alarms

Use **test alarms** to test the hardware associated with active alarms in the alarms log.

test alarms provides a query screen to help the user narrow the selection of alarmed objects. After the screen is filled out, press **Enter** to test the hardware associated with the selected alarm log entries. The results in standard test output and status information are on the message line as the command progresses.

Several alarms may be logged against a single maintenance object, each alarm representing a different problem. Even if there are multiple entries in the alarm log for a single object, **test alarms** tests each physical object once.

Syntax

```
test alarms [ auto-page ] [ failures ] [ step ] [ short | long ] [ repeat # | clear ]
```

auto-page	Continue testing and displaying test results by providing a new screen every time the SAT screen is filled with test results. The screen does not scroll to accommodate new results. If the auto-page option is not specified, when the SAT screen is filled with test results testing stops until the user enters the Page key to continue or the Cancel key to halt the testing.
failures	Show failures on the SAT screen. All passes will not be displayed on the output screen. Hardware failures, aborts, conflicts, and PN-down failures.
step	Step to the next or previous alarm without testing the current alarm. Alarm information is displayed with a prompt for a keypress. Enter: • CANCEL to cancel the command • ENTER to test the currently displayed alarm • NEXT ALARM (function key) to move to the next alarm • PREV ALARM (function key) to move to the previous alarm without testing the currently displayed alarm Press NEXT ALARM (function key) or PREV ALARM (function key) at any time during the command, even during test results. If the NEXT ALARM or PREV ALARM is pressed during a test, the test is aborted, testing of the current alarm stops, and the next alarm or previous alarm is displayed. If the first alarm is displayed, and the PREV ALARM is pressed, then the last alarm is displayed. If the last alarm is currently displayed, and NEXT ALARM is requested, the first alarm is displayed.
short	Run a series of nondestructive diagnostic tests.
long	Run a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
repeat #	Number of times to repeat the test, between 1 and 100.
clear	Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

test alarms options

After entering **test alarms**, you are presented with an options screen for alarm selection. The following fields are displayed on the test alarms screen.

Table 2: test alarms field descriptions — Hardware Test Alarm Query

Field	Description
ALARM TYPES	The type of alarm or combination of alarms to be tested, specified by <i>y</i> or <i>n</i> in the alarm type fields.
REPORT PERIOD	Test alarms for records for the last hour (<i>h</i>), last day (<i>d</i>), last week (<i>w</i>) or all (<i>a</i>).
From	Specifies error records starting from the time specified by <i>mm/dd/hh/mm</i> (month/day/hour/minute). If no <i>From</i> date is entered, errors from the earliest record in the log are displayed.
To	Specifies every error record up to the time specified by <i>mm/dd/hh/mm</i> . If no <i>To</i> date is entered, every error up to the current date is displayed.
Equipment Type	To limit the report to a specific group of components, enter the location of a type of equipment in one of the following fields. If no entry is made, errors for the entire system are displayed. • Gateway — Enter the gateway number. • Category — Enter a category to restrict the report to maintenance objects in a specific category. The HELP key displays a list of categories. • Extension — Enter the extension number of a port. • Trunk (group/member) — Enter a trunk-group number, or a trunk-group and member number separated by a slash (for example, 78 or 78/1).

test alarms output

The responses, with output, on a test-by-test basis with one line of data displayed for each test result. With the failures option, only the tests that failed.

Table 3: test alarms field descriptions — Alarm Entry

Field	Description
Port	The location of the alarmed object (Media-gateway-slot-circuit). The alarm log use the same identifier.
Maintenance Name	The name of the MO as it is displayed in the alarm and error logs.
On Board	Whether the fault detected is on the associated media module, or an off board element connected to the media module.
Alt Name	Extension numbers or trunk-group numbers.

Table continues...

Field	Description
Alarm Type	Major, minor, or warning is an indicator to the seriousness of the alarm raised.
Service State	RDY (ready for service), OUT (out of service), or IN (in service) is the current service state of the station and trunk ports shown.

amw all

clear amw all

Use `clear amw all` to clear the message waiting light on an extension.

Syntax

```
clear amw all n
```

n Extension number.

analog-testcall

test analog-testcall

Use `test analog-testcall` to use the Automatic Transmission Measurement System (ATMS) to originate test calls over analog trunks. ATMS collects performance measurements on the test call and compares them to administered thresholds. Detail and summary reports of these measurements are generated with `list testcalls`.

You can specify testing of an entire trunk group or an individual trunk using either group or member addresses or port and media module location. The type of test call, the number of the testing line on the far-end switch and various other parameters must be administered on the Trunk Group screen before the command can run.

The `test analog-testcall` test aborts when attempting a test call on these trunk groups:

- ISDN-PRI
- SIP
- DID
- Any incoming trunk group (transmission tests can be run on outgoing trunks)

ATMS, `test analog-testcall`, and the measurement reports are described in Automatic Transmission Measurement System (ATMS) in 'Automatic Transmission Measurement System'

in *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Syntax

```
test analog-testcall trunk# / member# | port location | supervision | no-selftest |  
no-return-loss | no-st-or-rl [ repeat # ] [ schedule ]
```

announcement

add announcement

Syntax

```
add announcement [ext]
```

ext extension for adding the announcement.

Use the **add announcement** for the following types of announcement:

- Integrated
- Integrated-mus
- integrated-rep

display announcement

Syntax

```
display announcement [ext]
```

ext extension of the announcement to be displayed.

Use the **display announcement** for the following types of announcement:

- Integrated
- Integrated-mus
- integrated-rep

erase announcement

Use the **erase announcement** command to delete the announcement files from a gateway location, whether the announcement files are backed up to a compact flash or internal flash. For example, when you run the command **erase announcement 6v9**:

- If the backup device in the gateway location 6v9 is the internal flash on a gateway, all the announcement files on the internal flash (as well as the RAM) are erased.

- If the backup device in the gateway location 6v9 is a Compact Flash inserted in a G430 or G450 Release 2 (or later), all the announcement files in the `/annc/backup` directory on the Compact Flash (as well as the RAM) are erased.

Syntax

```
erase announcement [gateway number] [module number]
```

list announcement

Use the `list announcement` command to see announcement information listed by the extension.

Syntax

```
list announcement [ext x] [to-ext x] [count n] [type x] [schedule]
```

- ext x** Lists information for a specific extension. Also use `list announcement x`.
- to-ext x** Lists information for all announcement beginning with one extension and ending with another when used with the parameter `ext x`
- count n** Lists *n* number of announcements.
- type x** Lists all announcements of a specific type.
- schedule** Specifies a start time for the command.

The last column of `list announcement` command displays the number of sources. For example, if the audio group has three music sources then, the **Num of Sources** column shows 3.

list int-annc-sources

Syntax

```
list int-annc-sources [gateway x] [module X]
or
list int-annc-sources [media server x] [schedule]
```

- gateway x** x can have value 1 — 250.
- module x** x can have value 1 — 250.

Use the `list int-annc-sources` command to produce the output for all VAL, GW VAL and Avaya Aura® Media Server (MS) announcement sources.

announcement-board

disable announcement-board

Use the `disable announcement-board` command to disable an announcement board on your system.

The **Maximum Media Gateway VAL Sources** fields on the system-parameters customer-options screen must be set to enable/disable announcement-board. For information on administering announcement boards, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
disable announcement-board x
```

enable announcement-board

Use the `enable announcement-board` command to enable an announcement board on your system.

The **Maximum Media Gateway VAL Sources** fields on the system-parameters customer-options screen must be set to enable/disable announcement-board. For information on administering announcement boards, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
enable announcement-board x
```

ars analysis

list ars analysis

Use `list ars analysis` to view the parameters that the Automatic Route Selection (ARS) table uses to route a call.

Syntax

```
list ars analysis [start] [route] [location n|all] [node] [to-node] [count] [schedule]
```

start	This is an optional parameter. The digit string from which the system starts listing the ars analysis data.
route	This is an optional parameter. The route number that Communication Manager uses for the dialed string. The parameter value can be one of the following: • 1 to 2000 • r1 to r32 • p1 to p2000

- location** This is an optional parameter. The location of the extension. The parameter value can be one of the following:
- 1 to 2000
 - all
- node** This is an optional parameter. The first node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.
- to-node** This is an optional parameter. The last node in the list that you want the system to display. The parameter value can be in the range of 1 to 999.
- count** This is an optional parameter. The number of stations that you want the system to display.
- schedule** This is an optional parameter. The time at which you want the system to print the output.

Field descriptions

Field	Description
Location	The location of the extension.
Dialed String	The dialed string that matches with the dialed string entry in the ARS Digit Analysis table.
Total Min Max	The minimum and maximum number of digits that you have administered to match with the dialed string.
Route Pattern	The route number that Communication Manager uses for the dialed string.
Call Type	The type of call for each dialed string.
Node Number	The destination node number in a private network when the system uses Node Number Routing or Distributed Communication System (DCS).
ANI Req'd	The value of this field denotes if R2-MFC and Russian MF ANI calls require ANI.

ars route-chosen

list ars route-chosen

Use `list ars route-chosen` to see the parameters used by ARS to route a call to a specific number.

Syntax

```
list ars route-chosen x [ location n | all ] [ partition n ] [ schedule ]
```

- x** Dialed number
- location n** Optional. The location number. The parameter value includes
- **1 to 2000**
 - **all**
- partition n** Optional. The partition group number. The parameter value ranges from **1** to **8**.
- schedule** Optional. Specify a start time for the command.

list ars route-chosen field descriptions

Output field	Field description
Location	Entries are displayed for phones dialing from the specified location. The default is all.
Partitioned Group Number	Partitioned Group Number as entered on the command line. The default is 1.
Dialed String	The matched entry in the ARS Digit Analysis table.
Total Min Max	Minimum and maximum length of the string matched in the ARS Digit Analysis table.
Route Pattern	Route pattern used to route the call.
Call Type	The call type as matched on the AAR Digit Analysis table. See Avaya Aura® Communication Manager for full explanation of this field.
Node Number	Node number as matched on the ARS Digit Analysis table.
Location	Entries are displayed for phones dialing from this location. If there are no matching entries in the telephone's location, Communication Manager tries the entries for location all.
Actual Outpulsed Digits by Preference	Digits outpulsed when you choose each of the preferences in the chosen route pattern.

attendant

status attendant

Use **status attendant** to see the operational state of the specified attendant console.

Syntax

```
status attendant console #
```

console # Console number assigned to the attendant.

Description

This information can help in trouble diagnosis and in locating facilities to which the attendant console is connected.

status attendant field descriptions

Field	Description
Console Number	Number assigned to the attendant
Port	Port location of the attendant (Media-Gateway-slot-circuit)
Service State	In-service/idle, in-service/active, out of service, or disconnected
Usage State	Idle or active
Maintenance Busy State	y/n Is maintenance testing the object?
Connected Ports	Port locations to which the attendant is communicating (Media-Gateway-slot-circuit).

audio-group

list audio-group

Use `list audio-group` to list all audio groups and see how many members (audio sources) are in each group.

For more information on the Audio Groups screen, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list audio-group { [ 1-Max ] ( number n | ( to-number n ) | count n ) } [ schedule ]
```

1-Max	audio group number to list.
number <i>n</i> to-number <i>n</i>	range of audio group numbers to list.
count <i>n</i>	number of audio groups to see on the page.
schedule	Specify a time for the command to run.

list audio-group field descriptions

Field	Description
Group	Number of the Audio Group
Name	Name of the Audio Group
Number of Sources	Number of members (audio group sources) in the audio group

list usage audio-group

Use **list usage audio-group** to see all extensions that refer to the specified audio group.

For more information on the Announcements/Audio Sources screen, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list usage audio-group n [ schedule ]
```

n	Audio group number.
schedule	Specify a time to run the command.

audits

clear audits

Use **clear audits** to clear cumulative and peak hour data collected for each data relation audit. The **clear audits** command clears old data to display the data that is collected since the last **clear audits** when **status audits** is run.

Syntax

```
clear audits [cumulative] [peak-hour]
```

cumulative	The data collected for the peak hour since the last reboot or the last time the clear audits command was run.
peak-hour	The data collected since the last reboot or the last time the clear audits command was run.

status audits

Use **status audits** to see the results of Data Relation Audits that are built into the switch. Data Relation Audits check for inconsistencies between selected data items in the switch and report inconsistencies. Data Relation Audits are useful during development and testing phases of projects to discover software errors. On field, Data Relation Audits help the switch to recover from data corruption before the service is interrupted.

The status audits command displays the date and time that the requested interval begins, the number of times that the full sequence of audits executes (audit cycles), and status information about each audit that detected a problem or aborted during the interval. The status information contains:

- The name of the audit.

- The number of times an audit ran and corrected an error.
- The number of times an audit ran and detected an irreparable error.
- The number of times an audit ran and aborted.
- For cumulative: The date and time that the audit first detected a problem.
- For cumulative: The time of the most recent error detected by the audit.

Audit data information cumulates from the last reboot or the last **clear audits** cumulative command, and for peak hours since the last reboot or the last **clear audits** command.

The status audits screen does not automatically update, but reflects the system at the time of request.

Syntax

```
status audits [cumulative] [peak-hour]
```

cumulative The data collected for the peak hour since the last reboot or the last time the **clear audits** command was run.

peak-hour The data collected since the last reboot or the last time the **clear audits** command was run.

status audits field descriptions

Field	Descriptions
Start Date	• For cumulative: The date and time of the last reboot or the last time the clear audits cumulative command was run. • For peak-hour: The date and time of the beginning of the peak hour since the last reboot or when the last clear audits command is run.
# of Audit Cycles Completed	The number of audit cycles completed in the specified interval (0–999999). Asterisks indicate numbers that exceed 999999. The switch executes audits in a set order. After all audits are executed, the switch restarts the sequence. Individual audit values can be larger if the switch is partially through another audit cycle. Audit cycle numbers do not apply to these audits that execute as part of scheduled maintenance.
Audit Name	The audit name that detected an error or aborted. A few audits do not run in the normal audit sequence. Instead, they execute as part of scheduled maintenance and are marked with "(SCH)" following the audit name.

Table continues...

Field	Descriptions
# Cycles Fixed Data	The number of times the audit was run in a specified interval and found a fixable problem. Asterisks are used from numbers that exceed 65534.
# Cycles Could Not Fix Data	The number of times the audit was run in a specified interval and found a problem that could not be fixed. The audited switch data is inconsistent when this happens. Asterisks are used for numbers that exceed 65534.
# Cycles Audit Aborted	The number of times that the audit was run in a specified interval and aborted due to an internal error. Asterisks are for numbers that exceed 65534.
First Error	The date and time when the audit first detected fixed data, could not fix data, or aborted problems since the last clear audits cumulative command.
Most Recent Error	The date and time when the audit last detected fixed data, could not fix data, or aborted problems since the last clear audits cumulative command.

bcms

monitor bcms

Use **monitor bcms** to see a summary of Basic Call Management System (BCMS) conditions for agents and splits. The online status report is automatically updated every 30 seconds. You can also update the online status report on demand by pressing **UPDATE**. Press **CANCEL** and terminate the login to cancel monitor bcms.

Syntax

```
monitor bcms split split# | system split# | skill skill# | vdn vdn#
```

split *split#* Status of a particular split and the number of the split (ACD hunt group number).

system *split#* Status of the split queue and cumulative split information for every split measured by BCMS, and the numbers of the split (ACD hunt group numbers) separated by spaces and/or split number ranges separated by a hyphen (-).

skill *skill#* Status of a particular skill group and the number of the group.

vdn *vdn#* Vector directory number

Example

```
monitor bcms system
monitor bcms split 1
```

monitor bcms field descriptions

Field	Description
Date	The current date and time. Updated every 30 seconds or when UPDATE is pressed.
SPLIT NAME	The name of the split being reported. If no name is administered, the split extension appears as "EXTxxxxx". Splits appear in split number order.
CALLS WAIT	The number of calls currently waiting in this split's queue. Direct Agent Calls are preceded by an asterisk. This field is real-time status data.
OLDEST CALL	The amount of time that the oldest call has waited in queue. Real-time status data.
AVG SPEED ANS	The average time required for an answer in this split during the current period, including time in queue and time ringing at the agent's voice terminal. Intraflow calls (those that overflow from one ACD split to another split) will not have queue time from previous splits included in the average. The calculation is: Total Answer Time/Total Automatic Call Distribution (ACD) Calls . This is measurement data and includes only completed calls.
AVAIL AGENT	The number of agents in this split currently available to receive an Automatic Call Distribution (ACD) call from this split. Real-time status data.
ABAND CALLS	The number of calls abandoned during the current period. This is measurement data.
AVG ABAND TIME	The average time abandoned calls waited in queue before abandoning during the current period. The calculation is: Total Abandon Time/Total Calls Abandoned . This is measurement data and includes only completed calls.
ACD CALLS	The number of ACD calls handled by this split during the current period. This includes calls that intraflow into the split. This is measurement data.
AVG TALK TIME	The average talk time for ACD calls handled by this split during the current period. This does not include ring time at the agents' voice terminal. The calculation is: Total ACD Talk Time/Number of ACD Calls . This is measurement data and includes only completed calls.
AVG AFTER CALL	The average After Call Work (ACW) time for ACD calls handled by this split during the current period. ACD calls with no ACW time are included in the average. Time spent on direct incoming or outgoing calls while in ACW are not included in the average. The calculation is: (Total ACW Time – Total ACW Incoming Time – Total ACW Outgoing Time)/Total ACD Calls . This is measurement data and includes only completed calls.
% IN SERV LEVL	Percent in Service Level for a particular skill. It is the percentage of calls that were offered to the skill that were answered within the administered Service Level time according to the service agreement (for example, 80% of the calls within 20 seconds. If all calls were answered in that time, the value for the IN SERV LEVL would be 100%). The administered service level is defined on the hunt group form.

monitor bcms split field descriptions

Field	Description
Split	The number of the split requested. This is translation data.
Split Name	The name of the split requested. If no name exists, EXT xxxxxx appears.
Date	The current date and time, updated every 30 seconds or when the UPDATE key is pressed.
Calls Waiting	The number of calls currently waiting in this split's queue. Direct Agent Calls are preceded by an asterisk. This is real-time status data.
Oldest Call	The time in minutes: seconds that the current oldest call has waited in this split's queue. This is real-time status data.
Staffed	The number of agents currently logged into this split. This is real-time status data.
Avail	The number of agents currently available to receive an ACD call in this split. Agents are in the Auto-in or Manual-in work modes and are not currently on a call. If the agent is on another split's call or in ACW for another split, this agent is not listed as available and will not be recorded here. This is real-time status data.
ACD	The number of agents in this split currently on an Automatic Call Distribution (ACD) call for this split. This includes ACD calls handled by this split that arrive as coverage from another split. This also includes outbound calls (Outgoing Call Manager) distributed through the ACD. If an agent puts an ACD call on hold, but does not enter another state (for example, the agent does not enter the AVAIL state), the agent is still seen as in the ACD state. This is real-time status data.
ACW	The number of agents in this split currently in After Call Work (ACW) split. This is real-time status data.
AUX	The number of agents in this split currently in AUX work for this split. If an agent is on another split's call or in ACW for another split, this agent is not considered in AUX work and is not recorded here. This is real-time status data.
Extn	The number of agents in this split currently on non-ACD calls, incoming or outgoing directly to/from their extensions. If the agents are also in ACW or AUX they are recorded as Extn rather than ACW or AUX. This is real-time status data.
Other Split	The number of agents in this split on another split's call or in ACW for another split. Used if agents belong to multiple splits. This is real-time status data.
Agent	The name of the agent associated with the extension. If no name exists this field is blank.
EXT	The agent's extension. This field is translation data.
STATE	The current state of the agent for this split. Possible states are Avail, ACD, ACW, AUX, Extn In, Extn Out, OtherSplit, and Unstaff. This is real-time status data.

Table continues...

Field	Description
TIME	The clock time at which the agent entered the current state. This is real-time status data.
ACD CALLS	The number of ACD calls (inbound and outbound), that the agent has completed for this split during the current period (half-hour or one-hour). If the maximum number of 255 calls exceeded, 255 appears. This is measurement data.
EXTN IN CALLS	The number of non-ACD incoming calls that the agent has received and completed during the current period, maximum 255. This is measurement data.
EXTN OUT CALLS	The number of outgoing non-ACD calls that the agent has completed during the current period, maximum 255. This is measurement data.

monitor bcms vdn field descriptions

Field	Description
Date	The current date and time (updated every 30 seconds or when Update is pressed).
VDN NAME	The name of the VDN being reported. If the VDN does not have a name administered, this field displays EXT ## where ## is the VDN extension.
CALLS WAIT	The number of calls that encountered this VDN and have not been answered, abandoned, outflowed, or forced busy/disc. Includes calls in queues, in vector processing, and ringing at an agent telephone.
OLDEST CALL	The time the oldest call currently waiting has waited in the VDN. Timing starts when the call enters the VDN.
ACD CALLS	The number of completed ACD calls answered in a BCMS-measured split. The split may have been reached via the queue-to-main, check backup, route-to, messaging split, or adjunct routing commands. Includes Direct Agent calls (EAS only).
AVG SPEED ANS	The average speed of answer for ACD and connect calls (see CONN CALLS below) that have completed for this VDN during the current period. This includes the time in vector processing, in a split queue, and time ringing. The calculation is: Total Answer Time / (Total ACD Calls + Total CONNect CALLS) Answer time for a call is recorded when the call ends. For example, if a call originates in interval x, is answered in interval y, and ends in interval z, the associated answer and talk times are recorded in interval z.
ABAND CALLS	The number of calls to this VDN that have abandoned before being answered during the current period. This includes VDN calls that were routed to an attendant, telephone, or announcement, and abandoned before being answered.
AVG ABAND TIME	The average time abandoned calls waited before abandoning during the current period. The calculation is: Total Abandon Time / Total Calls Abandoned

Table continues...

Field	Description
AVG TALK / HOLD	The average talk time for ACD calls completed by this VDN during the current period. This does not include ring time, but it does include any time the caller spent on Hold. The calculation is: Total Talk Time / ACD Calls
CONN CALLS	The number of completed calls that were routed to a telephone, attendant, announcement, messaging split, or call pickup and were answered there.
FLOW OUT	The number of calls that were routed to another VDN or to a trunk, including successful look-ahead attempts.
CALLS BUSY / DISC	The number of calls that were forced busy or forced disconnect during the current interval. This value includes: • Calls that encountered a busy or disconnect vector step • Calls disconnected by a stop vector step • Calls forwarded to a split with a full queue • Calls forwarded to a split with no available agents and no queue This value does not include abandoned calls.
% IN SERV LEVL	The percent of calls offered that completed and were answered within the acceptable service level defined on the VDN screen. The calculation is: (accepted * 100) / calls offered <i>calls offered</i> is defined as: acdcalls + flowout calls + abandoned + connect + busy / disc <i>accepted</i> is the number of ACD and CONNect calls that were answered within the administered service level. This field is blank if no calls were recorded for this time interval. This field is also blank if no Acceptable Service Level has been administered on the VDN screen.

board

busyout board

Use **busyout board** to busyout all the ports associated with the specified media module.

 Note:

In a media gateway media module can be busied out.

Syntax

```
busyout board location
```

location Physical location of the media module.

Example

```
busyout board 1v3
```

release board

Use **release board** to activate administered maintenance objects on the media module at specified locations.

Syntax

```
release board location
```

location Physical location of the media module.

Example

```
release board 1v9
```

reset board

Reset every administered port on the specified media module.

Caution:

Note that **reset board** can disrupt service and can cause extraneous alarms. Effects of a reset vary depending upon the type of object being reset and upon whether the component is duplicated. See the *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers* for the relevant maintenance object for details.

Syntax

```
reset board location [repeat x]
```

location Physical location of the media module.

repeat # The number of times to repeat the command. The default is 1.

Description

Use **reset board** to perform a software reset of every administered port on the specified media module. Every port must be busied out before the port board is reset.

Example

```
reset board 1v4
reset board 1v4 repeat 4
```

test board

Run tests on specified media module.

*** Note:**

Some tests can be disabled by administration.

! Important:

You cannot perform the destructive long tests on a Switch Node Interface (SNI) board unless the board has been busied out.

Syntax

```
test board location [ repeat #]
```

location Physical location of the media module.

repeat # (Optional) The number of times to repeat the command. The default is 1.

short Run short test sequence.

long Run long test sequence.

clear Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Description

Use **test board** to perform a set of hardware diagnostic tests on a specified media module. The system first validates that the board exists at the specified location. Then, based on the logical type of board (for example, Analog, Digital, Hybrid), a series of tests performs diagnostics on the board and then returns results of the tests along with any possible error codes.

The default is to run the short test sequence after.

Example

```
test board 1v4
```

bri-port

status bri-port

Use **status bri-port** to see the service state, maintenance state, and layer 1 state of an ISDN-BRI port. There is also information about the point-to-point signaling links carried over the port. For more information, see the 'BRI-PORT (ISDN-BRI Port)' section in the *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*.

Syntax

```
status bri-port location
```

location Location of the BRI port

status bri-port field descriptions

Field	Description
Port	The location of the ISDN-BRI port.
Service State	Whether the ISDN-BRI port is in-service or out-of-service .
Maintenance Busy	Whether maintenance testing is currently being performed on the port.
Layer 1 State	The operational state of the physical connection (Layer 1) of the ISDN link carried over the port: • activated — Layer 1 frames are being passed between the port and BRI endpoints • pend-activation — The port is in service, the layer 1 interface device is turned on and layer 1 frames are being sent from the port, but the BRI endpoints are not responding • deactivated — The layer 1 interface device on the BRI has been turned off due to the port being out of service.
TEI Value	The Terminal Endpoint Identifier (TEI) is a layer 2 addressing parameter used by the switch to exchange information with BRI endpoints over the point-to-point signaling link. The TEI is a number from 1 to 127.
	The operational state of the point-to-point signaling link (Layer 2): • assigned — The link is currently in the AWAIT_EST (Await Establish) state at layer 2. If the BRI endpoint supports TEI allocation procedures, those procedures have been successfully executed and a TEI has been assigned to the endpoint by the switch. • established — The link is in the MF_EST_NORM (Multi-Frame Established Normal) state at layer 2. The switch has successfully started the link and is now capable of exchanging layer 3 frames with the endpoint. If the endpoint does not support SPID initialization procedures, the voice extension of the endpoint associated with the link is also displayed. This is the normal state for a link in a point-to-point wiring configuration. • L3-established — The link is in the MF_EST_NORM state at layer 2 and SPID initialization procedures have been successfully completed. The voice extension of the endpoint associated with the link is also displayed. This is the normal state for a link in a multipoint wiring configuration. • hyperactive — Traffic on this link has exceeded the threshold and the link has been suspended.
Endpt Extension	The extension of the voice/data endpoint associated with the link. This field is blank if the link is not in the established or L3-established state.
Endpt SPID	The SPID (Service Profile Identifier) administered for the voice/data endpoint. This field is blank if the link is not in the established or L3-established state.

Table continues...

Field	Description
Service SPID	If the link is associated with the Service SPID this field displays yes and the Endpoint Extension field is blank. Otherwise this field is blank. Service SPID is a feature used by service technicians to check building wiring between the switch and the BRI endpoint.

Interpreting results of status bri-port

The following table helps interpret the results of **status bri-port**. Find the combination of the output field values in your report and follow the actions for the type of endpoint connected to the port.

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
BRI, ASAI	0-126	Assigned	blank	blank	This is a transitory state for BRI endpoints and ASAI adjuncts. The switch is attempting to establish the link. 1. Check the endpoint and wiring by following the SPID Facility test's procedure described in BRI-SET, Various Adjuncts in the <i>Maintenance Alarms for Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i>. 2. Repeat status bri-port to determine that the Layer 2 state of the signaling link is either L3-established (for ASAI adjuncts and BRI endpoints supporting MIM initialization) or established (for fixed TEI BRI endpoints and automatic TEI BRI endpoints not supporting MIM initialization). If it is not, follow normal escalation procedures. (A MIM or management information message is a level-3 message that conveys management and maintenance information between a communications system and a BRI terminal.)

Table continues...

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
ASAI	0-63	Established	blank	blank	This is a transitory state for ASAI adjuncts. ASAI signaling is connected at Layer 2 but the Layer 3 Restart procedure has not been completed between switch and adjunct. 1. Check the adjunct by following the recommended repair procedures of the manufacturer. 2. Repeat status bri-port and determine whether the L2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
BRI	0-126	Established	ext#	blank	This is the normal state for non-MIM initializing, fixed, and automatic TEI BRI endpoints.
BRI, ASAI	64-126	Established	blank	blank	This is a transitory state for automatic TEI BRI endpoints that support MIM initialization. 1. Verify that SPID administration on the switch and the endpoint are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. 2. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
BRI-	64-126	L3-Established	ext#	blank	This is the normal state for automatic TEI BRI endpoints that support MIM initialization.
BRI	0-126	L3-Established	blank	blank	An invalid SPID is assigned to link. Change the SPID value in the BRI endpoint to match the SPID administered to the BRI endpoint on the port. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.

Table continues...

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
BRI	0–126	L3–Assigned	ext#	blank	This is a transitory state for BRI endpoints that support MIM initialization. 1. Wait 5 seconds and repeat the command. If the state has not changed, continue with Step 2. 2. Make sure SPID administration on the switch and endpoint are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	yes	This is a transitory state for BRI endpoints that support MIM initialization when a SPID Facility test has been used to initialize the station. 1. Wait 5 seconds and repeat the command. If the state has not changed continue with Step 2. 2. Make sure SPID administration on the switch and endpoints are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.

Table continues...

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
ASAI BRI	0-126	Hyperactive	ignore	ignore	Link has sent too many messages per unit time. Signaling has been suspended. After 60 seconds, the system attempts to put the link into service. If a link remains in this state while there is no activity at the BRI endpoint, take the following steps: 1. Make sure SPID administration on the switch and endpoints are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 2. 2. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
ASAI	0-126	L3-Restarting	ext#		The switch has sent a Restart message to the adjunct but has not yet received a Restart Acknowledgment message from the adjunct.
ASAI	0-126	L3-Restarted	ext#		After receiving a Restart Acknowledgment message, the switch has sent a Heartbeat message to the adjunct and is waiting for a response.
ASAI	0-126	L3-Established	ext#		This is the normal state for ASAI adjunct.
BRI-	64-126	L3-Established	ext#	blank	This is the normal state for automatic TEI BRI endpoints that support MIM initialization.
BRI	0-126	L3-Established	blank	blank	An invalid SPID is assigned to link. Change the SPID value in the BRI endpoint to match the SPID administered to the BRI endpoint on the port. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.

Table continues...

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
BRI	0–126	L3–Assigned	ext#	blank	This is a transitory state for BRI endpoints that support MIM initialization. 1. Wait 5 seconds and repeat the command. If the state has not changed, continue with Step 2. 2. Make sure SPID administration on the switch and endpoint are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
BRI	0–126	L3–Assigned	ext#	yes	This is a transitory state for BRI endpoints that support MIM initialization when a SPID Facility test has been used to initialize the station. 1. Wait 5 seconds and repeat the command. If the state has not changed continue with Step 2. 2. Make sure SPID administration on the switch and endpoints are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 3. 3. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.

Table continues...

Error Type	Aux Data	Associated Test	Alarm Level	On/Off Board	Test to Clear Value
ASAI BRI	0-126	Hyperactive	ignore	ignore	Link has sent too many messages per unit time. Signaling has been suspended. After 60 seconds, the system attempts to put the link into service. If a link remains in this state while there is no activity at the BRI endpoint, take the following steps: 1. Make sure SPID administration on the switch and endpoints are consistent. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, go to Step 2. 2. Try replacing the endpoint. Repeat status bri-port to determine whether the Layer 2 state of the signaling link is L3-established. If it is not, follow normal escalation procedures.
ASAI	0-126	L3-Restarting	ext#		The switch has sent a Restart message to the adjunct but has not yet received a Restart Acknowledgment message from the adjunct.
ASAI	0-126	L3-Restarted	ext#		After receiving a Restart Acknowledgment message, the switch has sent a Heartbeat message to the adjunct and is waiting for a response.
ASAI	0-126	L3-Established	ext#		This is the normal state for ASAI adjunct.

bulletin-board

display bulletin-board

Use `display bulletin board` to see messages.

Syntax

```
display bulletin-board
```

For detailed information about the Communication Manager bulletin board, see *Administering Avaya Aura® Communication Manager*.

calltype route-chosen

list calltype route-chosen

Use `list calltype route-chosen` to see how digits are handled for a particular call.

Syntax

```
list calltype route-chosen x [ location n | all ] [ partition n ] [ schedule ]
```

x Dialed number

location n (Optional) Location number 1–250 or all. The default is all.

partition n (Optional) Partition Group Number (1–8)

schedule (Optional) Specify a start time for the command.

list calltype route-chosen field descriptions

Field	Description
Location	Location from the command line. You can see what would happen if the telephone number you enter into your administration terminal were dialed from a telephone's call log in this location. • If there are matching entries in the entered location, those get used. • If there are no matching entries in the entered location, Communication Manager tries the entries in location all.
Match	• numeric — the entry in the Calltype Digit Analysis table that was selected for the dialed string • blank — no matching entries for this dialed string in the Calltype Digit Analysis table
length Min Max	• numeric — the entry in the Calltype Digit Analysis table that was selected for the dialed string • blank — no matching entries for this dialed string in the Calltype Digit Analysis table
Selected Location	Phones dialing from this location use the entries on this form. If there are matching entries in the telephone's location, those entries get used. If there are no matching entries in the telephone's location, Communication Manager tries the entries in location all.
After Delete and Insert	The digit string as it is after call type digit manipulation for that pattern, up to four manipulations.

Table continues...

Field	Description
Type	• ext • aar • ars • udp The call type used by the call type algorithm to test the modified string. Call types correspond to the equivalent entries on the Calltype Digit Analysis yable (display calltype analysis).
Result	Results of the analysis on the dialed string. If there was a successful match and completion of the call, the modifications to the dialed string. Results stop at the first successful match and valid route. Use this information to view the call type's specific routing analysis form (AAR Routing table, ARS Routing table, dialplan analysis tables and the uniform-dialplan tables) for more information about the routing of the call.

campon-busyout

campon-busyout

Use **campon-busyout** to busy-out system resources that require maintenance or repair, and to remove idle VoIP resources from the system's pool of available VoIP resources. You can use **campon-busyout** to continue present activity and prevent future activity, so that the facilities eventually become idle and board replacement occurs.

Use **campon-busyout media-gateway/media-server** to select the media processor to be busied out while the media gateway or media-server is still in service. After the media gateway or media server resources are in a busy-out state, the associated media gateway or media-server can be removed from the system without disrupting active calls. Use **status media-processor board** to check the busy-out status of a media processor.

Syntax

```
campon-busyout trunk [ trunk-group | member ] processor [ location ]
```

trunk *trunk-group* Location of the resource.

trunk *member* Location of the resource.

processor *location* Location of the resource.

A redundant **campon-busyout**, issued for a media processor already in the pending busyout or busyout service state, results in ABORT with an error code for any media processor resource that is already busied.

- Busied resources are returned to service. The command result is PASS.
- Resources marked for busyout, pending busyout, are cleared. The command result is ABORT with an error code that signifies the release of a media processor that was in the pending busy service state.

busyout board and **busyout port** override any pending busyout states created with **campon-busyout** for media processors.

capacity

display capacity

Use **display capacity** to see how your system is administered and to see a snapshot status of system resources.

Syntax

```
display capacity [ schedule ]
```

schedule Use schedule to specify a start time for the command.

Description

Use **display capacity** to see the maximum capacities of system resources assigned by the system and the current level of usage. Most of the maximum capacities depend on your contract with Avaya. Capacities are defined in the license files and displayed on the system-parameters customer-options screen.

display capacity field descriptions — Page 1

Field	Description
Current System Memory Configuration	The platform on which the translations were saved. Can also be unknown if no flash card is present or translations made on old load. This is important because platforms are not always compatible. Standard or Extra Large = translations are saved on CM 4.0 or later. Anything other than Standard or Extra Large = translations were saved on a pre-CM4.0 system.
AAR/ARS	

Table continues...

Field	Description
AAR/ARS Patterns	The number of route patterns. For more information about AAR/ARS Pattern, see <i>Administering Avaya Aura® Communication Manager</i> .
Inserted Digit Strings	The number of 12-digit strings inserted and available for AAR/ARS preferences. For more information, see <i>Administering Avaya Aura® Communication Manager</i> .
AAR/ARS Analysis Entries	The number of entries in ARS, AAR and Dial Plan Analysis forms (combined)
AAR/ARS Conversion Entries	The number of entries in ARS and AAR Digit Conversion forms (combined)
Toll Analysis Entries	The number of entries in Toll Analysis form
Digit Nodes (contributes to Percent Full)	Building blocks used for storing entries in ARS, AAR, Dial Plan, Toll and Calltype Analysis and Digit Conversion forms
Short Digit Nodes (contributes to Percent Full)	Building blocks used for storing entries in ARS, AAR, Dial Plan, Toll and Calltype Analysis and Digit Conversion forms
ABBREVIATED DIALING (AD)	
AD Entries Per System	The number of abbreviated dialing entries for both group and personal lists.
AD Personal Lists Per System	The number of abbreviated dialing personal lists. For more information about AD Personal Lists Per System, see <i>Administering Avaya Aura® Communication Manager</i> .
Adjunct Switch Application Interface (ASAI)	
Active Controlling Associations	The number of station domain controls that ASAI adjuncts can request.
Notification Requests	The number of requests ASAI can make to monitor call activity at a split or VDN.
Simultaneous Active Adjunct Controlled Calls	n goThe number of calls that can be controlled by ASAI adjuncts.

display capacity field descriptions — Page 2

Field	Description
ATTENDANT SERVICE	
Attendant Positions	The number of administered attendants.
Queue Length	A real-time snapshot of the number of calls waiting for attendant service.
Queue/Call Status Buttons	The number of attendant queue status buttons administered on stations. The two types of queue status buttons are: • atd-qcalls (ATD - Queue Calls) • atd-qtime (ATD - Queue Time)

Table continues...

Field	Description
Authorization Codes	The number of authorization codes used for security purposes. For more information about Authorization codes, see <i>Administering Avaya Aura® Communication Manager</i> .
BASIC CALL MANAGEMENT SYSTEM (BCMS)	
BCMS Measured Agents	The number of agents the Basic Call Management System (BCMS) is measuring.
BCMS Measured ACD Members	The number of ACD members BCMS is measuring.
BCMS Measured Splits/Skills	The number of hunt groups BCMS is measuring.
BCMS Measured VDNs	The number of vector directory numbers BCMS is measuring.

display capacity field descriptions — Page 3

Field	Description
CALL COVERAGE	
Coverage Answer Groups	The number of coverage answer groups. For more information about Coverage Answer Groups, see <i>Administering Avaya Aura® Communication Manager</i> .
Coverage Answer Group Members	The number of members in all coverage answer groups.
Coverage Paths	The number of administered coverage paths. For more information about Coverage Answer Group Members, see <i>Administering Avaya Aura® Communication Manager</i> .
Call Pickup Groups	The number of administered call pickup groups. For more information about Call Pickup Groups see <i>Administering Avaya Aura® Communication Manager</i> .
Call Records	The maximum number of active calls at a given time.
CALL VECTORING/CALL PROMPTING	
Total Vector Directory Numbers	The number of system VDNs. See <i>Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide</i> .
Meet-me Conference VDNs per system	The number of vector directory numbers for the meet-me conference feature.
Maximum Number of Expanded Meet-me Conf. Ports	License-file based value for the number of Expanded Meet-me Conference ports. The maximum value for this field is 300.
Total Vectors Per System	The number of vectors per system. See <i>Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide</i> .
Meet-me Conference vectors per System	The number of vectors for the meet-me conference feature.

Table continues...

Field	Description
BSR Application - Location Pairs Per System	The number of mappings administered in a multisite network. The maximum number of application-location pairs per system is 2560. For example, for a network of 10 locations, you can assign up to 256 applications. With 20 locations, you can assign up to 128 applications. See <i>Avaya Aura® Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide</i> .
Background BSR Poll VDNs	The number of BBP VDNs associated with the BSR polling
Vector Comment Steps (non-blank)	The total number of available, used and system vector steps that can have non-blank comments
Policy Routing Tables	The number of PRTs that can be defined
Policy Routing Points	The number of PRTs x Number of VDNs defined as destination

display capacity field descriptions — Page 4

Field	Description
DATA PARAMETERS	
Administered Connections	The number of connections between two access or data endpoints. For more information about Administered Connections, see <i>Administering Avaya Aura® Communication Manager</i> .
Alphanumeric Dialing Entries	For more information, see <i>Administering Avaya Aura® Communication Manager</i> .
DIAL PLAN	
Extensions	This includes stations, data endpoints, hunt groups, announcements, TEGs, VDNs, common shared extensions, and code calling IDs.
Miscellaneous Extensions	Anything that is not a station, trunk, data module, or attendant. This includes, but is not limited to, PCOL groups, common shared extensions, access endpoints, administered TSCs, code calling IDs, VDNs, LDNs, hunt groups, announcements, and TEGs.
Calltype Analysis Entries	The number of entries in Calltype Analysis form
UDP Extension Records	The number of 4-digit or 5-digit extension numbers that a user can use to call from one PBX to another.
UDP Digit Nodes	Building blocks used for storing entries in Uniform Dial Plan form
UDP Short Digit Nodes	Building blocks used for storing entries in Uniform Dial Plan form
Digital Data Endpoints	The number of digital serial communication devices that enable the asynchronous transfer of data. This also includes the number of analog adjuncts.
Facility Busy Indicators	The number of visual indicators of the busy/idle status of any trunk group, hunt group member, or station user. For more information see <i>Administering Avaya Aura® Communication Manager</i> .

display capacity field descriptions — Page 5

Field	Description
HUNT GROUPS, SPLITS, OR SKILLS	
Groups/Splits/Skills	The number of ACD hunt groups.
Administered Logical Agents	The number of logical agents administered. Applicable to systems with Expert Agent Selection.
Administered Logical Agent-Skill Pairs	The number of logical agent-skill pairs that are administered.
Logged-In ACD Agents	A real-time field displaying the number of agents actually logged in. For example, if an agent is logged into 4 skills (and there are no other agents), then the Logged-In ACD Agents field is 1 and the Group Members Per System field is 4.
Logged-In Advocate Agents	The number of Advocate agents that are currently logged in.
Logged-In IP Softphone Agents	The number of IP Softphone agents that are currently logged in.
Logged-In SIP EAS Agents	The number of available and used number of ACD agents logged in using the SIP endpoint.
Group Members Per System	The number of agent/group pairs.
CMS Measured ACD Members	The number of agent pairs being measured by CMS.
Dynamic Queue Slots Per System	The number of hunt group queue positions being used. The system pool of queue slots is dynamically assigned as needed. All calls can be queued.
Queue/Call Status Buttons	The number of hunt group queue status buttons administered on stations. There are four types of queue status buttons; attendants use the last two queue status buttons: • q-calls (Queue Calls) • q-time (Queue Time) • atd-qcalls (ATD - Queue Calls) • atd-qtime (ATD - Queue Time)
Intercom Groups Per System	The number of intercom groups set up within your organization.
Modem Pool Groups Per System	The number of modem pool groups. For more information about Modem Pool Groups Per System, see <i>Administering Avaya Aura® Communication Manager</i> .
Personal CO Line (PCOL) Trunk Groups	The number of PCOL trunk groups. For more information about Personal CO Line (PCOL) Trunk Groups, see <i>Administering Avaya Aura® Communication Manager</i> .

display capacity field descriptions — Page 6

Field	Description
RECORDED ANNOUNCEMENTS/MUSIC/AUDIO SOURCES	

Table continues...

Field	Description
Analog Queue Slots	The number of available and used queue slots that can be or have been assigned to analog line port or aux trunk connected announcement hardware for queuing up calls when the port is busy.
Administered Announcement Files	The total number of available and used extensions for announcement / audio sources that can or have been assigned.
Media Gateway VAL Sources	The current usage, license limit, and available capacity associated with the "Maximum Media Gateway VAL Sources" license feature.
TEMPORARY SIGNALLING CONNECTIONS (TSC)	
Administered TSCs	The total number of available and used ISDN administered or fixed Temporary Signaling Connections that can or have been assigned.
NCA-TSC Calls	The number of available and used Non Call Associated Temporary Signaling Connections that can or have been assigned.
REMOTE MESSAGE WAITING LAMPS (aut-msg-wt and Message Lamp Ext for other stations)	
Automatic Message Waiting Count	The total number of Automatic Message Waiting buttons and Message Lamp extensions that are administered for stations. In this total, the system does not include the extensions that are identical to the station extensions.
Used	Indicates the number of current active VoIP channels, which is the number of licenses currently used on active media connections.
Available	Indicates the difference between the license limit and the number of licenses in use. The field specifies the number of additional Avaya Aura® Media Server (MS) VoIP, which can be used as active media channels.
License Limit	Indicates the number of licenses purchased according to the Communication Manager license file.

display capacity field descriptions — Page 7

Field	Description
TRUNKS	
DS1 Media Modules	The number of assigned DS1 media modules.
DS1 With Echo Cancellation	The number of DS1 media modules that can have echo cancellation.
ICHT For ISDN/SIP Trunks	The number of Incoming Call Handling Table (ICHT) entries administered for trunk groups.
ISDN CBC Service Selection Trunks	The number of call-by-call trunk groups.
Trunk Groups	The number of trunk groups administered.
Trunk Ports	The number of trunk ports administered.
H.323 Trunks (included in Trunk ports')	The number of administered H.323 Office trunks.
Remote Office Trunks (included in 'Trunk ports')	The number of administered Remote Office trunks.

Table continues...

SBS Trunks (included in 'Trunk ports')	The number of administered SBS (Separation of Bearer and Signaling) trunks.
SIP Trunks (included in Trunk ports')	The number of administered SIP trunks.
Ad-hoc Video Conferencing Ports	The number of ad-hoc ports configured for the system.

display capacity field descriptions — Page 8

Field	Description
VOICE TERMINALS	
Station Button Memory (units)	The percentage of memory being consumed by every administered button.
Team Button / Monitored stations	The number of team button assignments. Team buttons are used to monitor members of a team of stations, functional between one Communication Manager server and the Tenovis 155 hardware platform.
Customized Button Labels	The percentage of the Customized Labels available on the currently used system.
Station Records	The number of resources being used by regular stations, announcements, and music on hold.
Stations (includes BRI stations)	The number of voice terminals.
Station Records Used by TTI (Not Shared)	TTI ports that are administered by the system when TTI is activated on the Feature-Related System-Parameters screen (change system-parameters features). The ports provide dial-tone to the unadministered physical station attached to the physical port location.
Station Records Used by TTI (Shared)	Ports that are shared with AWOH stations. The ports are administered by the system when is TTI activated on the Feature-Related System-Parameters screen (change system-parameters features). The ports provide dial-tone to the unadministered physical station attached to the physical port location.
Stations (includes BRI stations)	The number of voice terminals.
Stations With Port	The number of connected voice terminals (stations with specific administered ports).
Stations Without Port	The number of voice terminals not having an administered port, such as AWOH.
Other Stations	The number of ports used as conversion resources, agent login ID, MASI, and analog announcements.
TTI Ports	The number of ports assigned by TTI features.
Auto Moves Stations	The number of stations available to move using ACTR.
Administered IP SoftPhones	The number of the currently administered IP soft phones.
Video Capable Stations	The current number of simultaneously administered video capable H.323 stations.

Table continues...

Field	Description
Video Capable IP Softphones	The number of the currently administered video-capable IP soft phones.
ISDN-BRI Endpoint and Trunk Ports	The number of ISDN-BRI ports.

display capacity field descriptions — Page 9

Field	Description
TOTAL LICENSED CAPACITY	
Station and Trunk Ports	The number of subscribed ports in the system.
Station Capacity	
SBS Stations	The number of extensions administered as SBS (Separation of Bearer and Signaling).
Radio Controllers	The number of subscribed Radio Controller media modules.
Wireless Terminals	The number of subscribed wireless terminals.
XMOBILE Stations	The number of X-station mobility (XMOBILE) stations.
EC500	The number of Avaya Extension to Cellular (EC500) ports.
ISDN DECT	The number of ISDN-based DECT X-Mobile stations.
IP DECT	The number of IP-based DECT X-Mobile stations.
PHS	The number of PHS ports.
Off-PBX Telephone - EC500	Usage of the EC500 application (AvayaExtension to Cellular)
Off-PBX Telephone - OPS	Usage of the OPS application (Off-PBX Station, supporting non-native endpoints)
Off-PBX Telephone - PBFMC	Usage of the Public Fixed Mobile Convergence (PBFMC) application.
Off-PBX Telephone - PVFMC	Usage of the Private Fixed Mobile Convergence (PVFMC) application.
Off-PBX Telephone - SCCAN	Usage of the Seamless Converged Communications Across Network (SCCAN) application.
Survivable Processor Capacity	Usage of the total number of Survivable Core Servers and Survivable Remote Servers administered on the system.

display capacity field descriptions — Page 10

Field	Description
System Limit (units)	
Administered Applications (%)	Usage of application memory and mapping memory by Administered Applications
Enterprise Mobility User (%)	Usage of application memory and mapping memory by EMU
Acquired Shared Mappings (%)	Usage of application memory and mapping memory by Acquired Shared Mappings
one-X server Mappings (%)	

display capacity field descriptions — Page 11

Field	Description
CONCURRENT USAGE COUNTS	
IP Stations	The number of IP stations.
IP Stations in TTI State	The number of registered IP stations in the TTI state.
IP Attendant Consoles	The number of IP attendant consoles.
Remote Office Stations	The number of remote office stations.
Unauthorized H.323 Stations	The number of H.323 station types that do not authenticate with Communication Manager.
AES Server Licensed IP Stations	The number of IP stations registered to the switch through the Application Enablement Services (AES) servers and using AES licenses.
IP PORT USAGE COUNTS	
Total IP station ports	The number of ports for IP stations. The total number of IP station ports are calculated using the following fields: • Administered IP Stations and Attendants • Softphone Enabled on Station Form • Unnamed Registrations (TTI IP phones)
Administered IP Stations and Attendants	The number of ports administered with IP stations and attendants.
Softphone Enabled on Station Form	Double the number of stations that have the IP Softphone field enabled on the station forms.
Unnamed Registrations (TTI IP phones)	The number of IP ports used by H.323 phones that are registered without an extension.

display capacity field descriptions — Page 12

Field	Description
ID	Product identifier from the license file • AgentSC = • IP_API_A = • IP_Agent = IP agents • IP_NonAgt = • IP_Phone = IP phones • IP_ROMax = R300 remote office phones • IP_Soft = IP Softphones • IP_Supv = • IP_eCons = IP Softconsole • oneX_Comm =
Rel	Release number of IP endpoint. A blank implies any release.
Used	The number of products registered
Avail.	The number of products available for registration
System Limit	Registration limit

display capacity field descriptions — Page 13

Field	Description
CURRENT SYSTEM INFORMATION	
Software Load	The current software load on which the system is running.
Memory Configuration	The system platform.
Offer Category	The system's offer category.
LAST TRANSLATION LOADED INFORMATION	
Software Load	The software load translations saved before upgrade or reboot. Can also be <code>unknown/no trans</code> if no flash card is present. Also, if load translations were upgraded from one before to G3V4 load 71 or early G3V5 loads, <code>unknown/no trans</code> displays.
Memory Configuration	The platform on which the translations were saved. Can also be <code>unknown</code> if no flash card is present or translations made on old load. This is important because platforms are not always compatible. Standard or Extra Large = translations are saved on CM 4.0 or later. Anything other than Standard or Extra Large = translations were saved on a pre-CM4.0 system.
Offer Category	The offer category that was set when the last save translation was done before upgrade or reboot. Can also be <code>unknown</code> if no flash card is present or translations made on old load.
Platform	A number (identifier) indicating the platform the customer is using.

Table continues...

Field	Description
H.323 Stations via TLS	 Note: The H.323 Stations via TLS field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). This field is available for the USA Department of Defense (DoD) and approved Federal government customers. Communication Manager capacity for H.323 station support for desk phones is: • Large CM Platform- 2000 encrypted channels • Medium CM Platform- 1000 encrypted channels • Small CM Platform (Avaya Solutions Platform S8300)- 160 encrypted channels

cdr-link

busyout cdr-link

Use **busyout cdr-link** to put the call detail recording link in a maintenance busy state.

Syntax

```
busyout cdr-link primary | secondary
```

primary Primary CDR link. This is the default.

secondary Secondary CDR link.

Description

When busied out, the link is dropped and must be re-established later when returned to service.

Example

```
busyout cdr-link secondary
busyout cdr-link
```

release cdr-link

Use **release cdr-link** to remove maintenance objects associated with specified call detail recording (cdr) links from a maintenance busy state.

Syntax

```
release cdr-link primary | secondary
```

primary Primary CDR link. This is the default.

primary Secondary CDR link.

Description

These links provide asynchronous data connections from switches to peripherals. They are composed of:

- A manager that initiates and maintains the link
- A controller/protocol that services the link

The Maintenance Name field displays:

- PRI-CDR for the primary CDR link
- SEC-CDR for the secondary CDR link

Example

```
release cdr-link
release cdr-link primary
```

status cdr-link

Use `status cdr-link` to see the status of the call detail recording (CDR) links.

Syntax

```
status cdr-link
```

Description

If a link is down, the report includes the number of times the switch has tried to re-establish the link. The CDR link is established by socket connection between Communication Manager and a CDR output device such as a CDR adjunct. The link is used by the server to send call detail records to the output device. A system may have up to two CDR links: a primary and a secondary.

status cdr-link field descriptions

Field	Description
Link State	The operational status of the link: • <i>up</i> The link is established and is capable of supporting the application. This is the normal operational state. • <i>down</i> The link is physically down. • <i>endpoint not administered</i> An output device has not been assigned on the CDR system parameters screen.
Number of Retries	The number of times the switch has tried to set up the link.
Date & Time	The last time the CDR link went up or down.
Forward Seq. No	A counter which increments with every Session Protocol Data Unit (SPDU) sent from the switch to the CDR adjunct. Both the primary and secondary CDR outputs have independent Forward Sequence numbers.

Table continues...

Field	Description
Backward Seq. No	A counter that indicates the number of the next Session Protocol Data Unit (SPDU) that is expected from the CDR adjunct. Both the primary and the secondary CDR outputs have independent Backward Sequence numbers.
CDR Buffer % Full	When the switch produces a CDR record that cannot be immediately transmitted to the CDR adjunct, that record is placed in the CDR buffer. This percentage indicates how full the CDR buffer is at any point in time. If the switch, the CDR adjunct, and the IP link that interconnects them are all working properly, this number should be zero or very close.
Reason Code	Why the CDR link (primary or secondary) last changed from up to down or vice versa. Values when CDR is administered are: • CDR connection is closed • CDR connection is closed • CDR Output mode is blank • Data write failure • EIA port Bit rate changes • Survivable Remote Server is inactive • Maintenance Busy • Path is destroyed by COM • Primary extension is changed • Queue for primary CDR is full • Secondary extension is changed

test cdr-link

Use **test cdr-link** to validate that a call detail recording link has been administered and established.

Syntax

```
test cdr-link primary | secondary [ short | long ] [ repeat# | clear ] [ schedule ]
```

primary Primary CDR link. This is the default.

secondary Secondary CDR link.

short Run the short test sequence. This is the default.

long Run the long test sequence.

repeat # (Optional) The number of times to repeat the command. The default is 1.

schedule (Optional) Specify a start time for the command.

clear (Optional) Repeat the test sequence until any active alarms are cleared or until any test in the sequence fails.

Description

test cdr-link first validates that the Call Detail Recording (CDR) link has been administered and exists in the switch. Then individual diagnostic tests run on the link and return results of the test along with any possible error codes.

Example

```
test cdr-link
test cdr-link repeat 4
```

cleared-alarm-notif

status cleared-alarm-notif

Expert Systems use **status cleared-alarm-notif** to detect chronic alarming conditions.

Syntax

```
status cleared-alarm-notif 1 | 2
```

- 1 Display the status for the first OSS telephone number. This is default.
- 2 Display the status for the second OSS telephone number.

Description

Expert Systems use **status cleared-alarm-notif** to detect chronic alarming conditions. If **cleared-alarm-notif** displays Feature is suspended, Expert Systems can identify open trouble tickets as chronic problems for special consideration.

communication-interface links

change communication-interface links

Use **change communication-interface links** to administer the links to the servers from peripheral adjuncts.

See **status links** for more details on links.

Syntax

```
change communication-interface links
```

display communication-interface links

Use `display communication-interface links` to list translations for the links to the servers from peripheral adjuncts.

See `status link` for more details on links.

Syntax

```
display communication-interface links [ schedule ]
```

schedule Specify a start time for the command.

communication-interface processor-channels

change communication-interface processor-channels

Use `change communication-interface processor-channels` to assign each local processor channel to an interface link channel, and to define the information associated with each processor channel on an Ethernet link.

Syntax

```
change communication-interface processor-channels [ schedule ]
```

schedule Specify a start time for the command.

change communication-interface processor-channels field descriptions

Field	Description
Enable	y/n — processor channel is enabled/disabled.

Table continues...

Field	Description
Appl	Identifies the switch application type/adjunct connection used on this channel over a dedicated network. The application gateway is used for conversion between ISDN and TCP/IP. Other forms must be properly administered as well. Valid entries are: • audix — Voice Messaging • dcs — Distributed Communication System • fp-mwi — ISDN Feature Plus Message Waiting Indication. This channel passes message waiting light information for subscribers on the messaging system, from a messaging adjunct on a main switch for a phone on a satellite switch. The terminating location (far end) of this channel must be a Communication Manager system compatible with ISDN Feature Plus proprietary protocol. • gateway — Supports an X.25-connected AUDIX connected to an ISDN DCS network. • gtwy-tcp — Supports a TCP connected AUDIX connected to an ISDN DCS network. • mis — Management Information System, otherwise known as CMS (Communication Management System) • qsig-mwi — QSIG Message Waiting Indication. Used with a QSIG-based interface to a messaging system, this channel passes message waiting light information for subscribers on the messaging system. All msa entries refer to an obsolete product. An error message appears if an msa value is entered: msaamwl, msackl, msahlwc, msallwc, msamcs.
Gtwy To	Identifies which processor channel the given processor channel is serving as a gateway to. Valid entries are a number between 1- (maximum number of processor channels), or blank.
Mode	Identifies whether the IP session is passive (client) or active (server). This field must be blank if the interface link is processor. This field cannot be blank if the type of interface link is ethernet or ppp. Valid entries are c (client), s (server), or blank.
Interface Link	Identifies the physical link carrying this processor (virtual) channel. Links are numbered 1 through 254 or p for processor.
Interface Chan	For TCP/IP, interface channel numbers are in the range 5000-64500. The value 5001 is set for CMS and 5003 is set for DCS.
Destination Node	Identifies the switch or adjunct at the far end of this link. Enter an adjunct name, switch name, far-end IP address, node ID, or leave blank for services local to this switch. For ppp connections, match the Destination Node Name on the ppp Data Module screen.
Destination Port	Identifies the port number of the destination. The number 0 means any port can be used. Valid entries are 0, 5000-64500.

Table continues...

Field	Description
Session Local	The Local and Remote Session numbers can be any value between 1 and 256 (si model) or 384 (r model), but they must be consistent between endpoints. For each connection, the Local Session number on this switch must equal the Remote Session number on the remote switch and vice versa. It is allowed, and sometimes convenient, to use the same number for the Local and Remote Session numbers for two or more connections.
Session Remote	
Mach ID	Destination switch ID identified on the dial plan of the destination switch.

display communication-interface processor-channels

Use **display communication-interface processor-channels** to list the TCP/IP listen port to carry each processor (virtual) channel (on an Ethernet link).

Syntax

```
display communication-interface processor-channels
```

conference

status conference

Use **status conference** to help identify problems with a multimedia conference, and to help solve more complex problems.

Syntax

```
status conference [ all | conference-ID ] [ schedule ] [ endpoint-all | endpoint-ID ]
```

- all** Display all stored conference data.
- conference-ID** Display data for the specified conference (current or last).
- schedule** Schedule a time to run the command.
- endpoint-all** Display conference data for all endpoints in the specified conference. This is the default.
- endpoint-ID** Display conference data for the specified endpoint.

Description

The first screen is displayed when status conference is entered and at least 1 valid conference is found. Use status conference to solve the following multimedia problems:

- A user unable to join or remain joined to a conference.

- A conference having poor video quality due to it being downgraded because of the automatic algorithms — audio AUTO mode and the Px64 video picture specifications.
- A user unable to receive full service, such as being an audio-only endpoint (no video).
- An audio add-on user unable to join or remain joined to a conference.
- A conferee invisible to other users due to interworking problems.
- A user unable to participate in the Multipoint Communications Service conference.
- A continuous conference, without switching endpoints in or out of quadrants.

Depending on the **status conference** command entered, it is possible to have many records display. Active conferences display first (in order of conference-ID), followed by completed conferences (most recently completed first). There is no data or information about conferences yet to begin.

The data for each conference displays in 2 parts: the first screen describes the status of the conference and indicates the modes and levels of the conference. It also shows certain endpoint information such as which endpoints are in use and which endpoint caused the conference operating mode to change. This screen is similar to the administration screens. The remainder of the screens display endpoint level data (up to 8 endpoints per screen), displaying the ports and drop reasons.

status conference output field descriptions — page 1

Field	Description
Status	The current status of the conference: • active • in-use • complete
Conference Name	Always set as MMCH DYNAMIC
Conference Mode	Always set as voice-activated
Password	not applicable
Password Scope	not applicable
Cascade Mode	Conference cascade mode — blank
Audio Mode	The current operating audio mode — G.711-A, G.711-mu, G.728, G.722
Class	The type of conference — dedicated
Data Mode	Data mode capability for this conference — none, any-mlp, ww-pcs
MLP Rate	MLP Data Rate for this conference — blank
No. of Channels	The number of channels (transfer rate) required for each Px64 endpoint — 2.
Chair	Identifies the current chair token holder. This field is always blank.

Table continues...

Field	Description
Conf Bandwidth	The current operating channel conference bandwidth. This can be different from the administered bandwidth because of Rate Adaptation.
Rate Adaptation	Does this conference support Rate Adaptation? — n/y .
Format (in/out)	- For single-screen conference, the video format of the conference, CIF, QCIF, QCIF/CIF, H.CTS, H.CTX+, and SG4. - For conferences other than H.261, the input and output formats are always symmetric and the mode is the same for input and output. These display as H.CTX, H.CTX+, SG4. - For H.261 mode non-continuous presence conferences, the format is always symmetric and displays as CIF and QCIF. The same is true for the non-presentation, continuous presence conference in single-screen. - For presentation mode H.261 single screen continuous presence capable conferences, the input and output formats may be symmetric QCIF/CIF (displayed as CIF) or asymmetric QCIF/CIF, depending on if the format is administered as upgradeable. - For quad-screen conferences, the format is QCIF/CIF to reflect the input of QCIF from every participant and output of CIF to every participant. - For presentation mode quad-screen conference, the format is also QCIF/CIF to reflect the input/output of every participant except the presenter. In quad-screen mode, the input from the presenter is always CIF.
FPS	The CIF frame rate (frames per second) — '-', 30 , 15 , 10 , 7.5 . FPS indicates the rate that an endpoint is capable of receiving frames. Note that there is no indication of the maximum transmit frame rate nor the current frame rate that the MCU can detect. The frame rate changes as a function of the amount of motion in the input image.
QFPS	The ACIF frame rate (frames per second) — '-', 30, 15, 10, 7.5. QFPS indicates the rate that an endpoint is capable of generating/receiving frames. For quad-screen VAS conferences, QFPS reflects the highest common QCIF frame rate of every endpoint and the rate of the video mixer board, which may be lower than the rest of the participants. Note that QCIF calculation takes into account the highest common CIF frame rate declared by every conference participant, since QCIF rate cannot be greater than that of the highest common CIF rate. For quad-screen presentation conferences, QFPS reflects the highest common QCIF frame rate of every participant and the rate of the video mixer board. Note that the QFPS cannot be greater than the CIF frame rate announced by the presenter. QFPS field is blank for proprietary modes.

Table continues...

Field	Description
Lo/Hi Interworking	Conference supports Low Speed/High Speed Interworking. Always n .
Type	The type of conferee, either Audio/Video (P64), Audio Add-on (AUD), Cascade Link (CAS), BONDing Call (BOND), BONDing Cascade Link (BCAS), UCC Controller (UCC), or Dedicated Access (DA). BONDing calls use up to 12 channels to form a single multimedia pipe.
Ext	Endpoint extension chosen at administration. This field is blank.
Meet-me Number	Meet-Me Number administered for the Meet-Me Extension. This field is blank.
Dial Type	Indicates whether dial-in or dial-out is used to join the endpoint to the conference: • in — dial-in • out — dial-out
In Use	Is the endpoint currently participating in the conference or in process of connecting to the conference? • y — The endpoint is in use and is fully connected on all media in an active conference. • c — The endpoint is in use and is fully connected, however the endpoint has changed the conference audio or video capability or has changed the rate of the conference because of rate adaptation. This condition requires analysis of this endpoint's capabilities and mode fields to identify which capability was reduced. • e — The endpoint is in use but the endpoint had capability problems. The endpoint does not have one of the required capabilities (Vid, Bhl, MLP) to be a full participant. For MLP capabilities, see the T120 field. This condition requires analysis of this endpoint's capabilities and mode field to identify the missing capability. • f — The endpoint is in use but is disconnected from all media. This indicates that the endpoint has declared every required capability (channel/video/audio/data) but is not fully connected to all conference media at this time. This endpoint may be in the process of connecting, has failed to connect, or is not a valid video source. This condition requires analysis of this endpoint's capabilities and mode fields to identify the problem. • n — The endpoint was connected in a conference but has/was disconnected or attempted to connect to a conference but was unsuccessful. • blank — until the first call is made from/to the endpoint.

Table continues...

Field	Description
Chl	Data on the quantify and quality of channels (transfer rate)? • y — The endpoint has the required number of channels. • e — The endpoint has not declared support for the correct number of channels and cannot participate fully in the conference. • n — The endpoint has declared the correct number of channels, but every channel has not yet joined the conference, due to either a network or endpoint problem. • blank — Audio add-on endpoints always set to blank.
Aud	Does the endpoint have the required audio capability? • y — The endpoint has the required audio capability. Audio add-on endpoint always have the Aud field set to y once the endpoint has joined the conference. • c — This endpoint is PCM only and it changed the video quality of the conference by changing the operating audio from G.728 to G.711. If the administered audio mode is auto and the administered bandwidth is 112 kbps (56 k/channel) or 128 kbps (64 k/channel), the system starts out with the highest common audio of G.728. When the administered bandwidth is greater than 128 kbps, the system starts out with the highest common bandwidth of 7 kHz. • e — A PCM-only endpoint that did not have the capability of supporting the administered audio mode of G.728 (such as a data conference), or G. 278/G.711 endpoint that did not have the capability of supporting the administered audio mode of 7 kHz. Such endpoints operate with PCM audio and interwork with the current operating audio mode. • blank — until the first call is made from/to the endpoint.

Table continues...

Field	Description
Vid	Does the endpoint have the required video capability and is receiving video? • y — The endpoint has the required video capability and should be receiving video if the Chl, Aud, and Dat fields are y. • c — It downgraded the conference's video quality - either from CIF to ACIF or by decreasing the frame rate. The conference video mode is set by default to CIF and if a QCIF-only endpoint joins the conference, then the entire conference is made to operate in QCIF, with the video clarity downgraded. Also, the conference frame rate is initially set to the highest frame rate that can then be reduced by any endpoint. If the conference video mode is not administered with upgrade capability, then if the video parameters for a conference have been downgraded, they are not upgraded until every endpoint disconnects from the conference. • e — The endpoint has not declared any video capability in its cap-set. • n — Audio only, not receiving video, possibly due to an audio or data problem. • blank — Audio add-on endpoints always blank.
Mlp	The state of the Control Link to the ESM (T.120 stack terminator), the endpoint MLP data capability, and the state of the data connection in the T.120 stack. This field value is always blank, indicating that the Data Mode for the conference is none, and therefore, the data does not apply, or the endpoint has never joined the conference.
Gx	Does the endpoint have the Still Frame Graphics capability? • y — This endpoint has this capability. • e — This endpoint did not declare this capability. The conference retains the still frame graphics capability when a non-compliant endpoint joins the conference. • blank — This endpoint has never joined the conference.

Table continues...

Field	Description
Rate Adpt	Rate adaptation/interworking indicator. Values of 5 and 6 apply only to low-speed/high-speed interworking. Every other value applies only to rate adaptation. • 5 — A 56-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • 6 — A 64-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • y — This endpoint has joined a conference at the administered rate of 64 kbps, but (because rate adaptation to 56 kbps was triggered by another endpoint) this endpoint has successfully rate-adapted to 56 kbps. • c — The administered bandwidth of a conference is 64 kbps and this endpoint has joined the conference at 56 kbps. The first 56-kbps endpoint that joins a 64-kbps rate-adaptable conference triggers rate adaptation (see Join Time below). • n — A 64-kbps conference was triggered to rate adapt to 56 kbps by some other endpoint. This endpoint joined the conference at the bandwidth of 64 kbps, but encountered problems in rate adapting down to 56 kbps. This endpoint may have the audio and may be receiving video, but is not a valid video source. • blank — Rate adaptation was never triggered by any endpoints. So, if an endpoint is in use and connected, then it joined the conference at the administered bandwidth.
Bond Mode	Bonding Mode — blank. This field is blank for calls that are not related to bonding.

Table continues...

Field	Description
Ts	Indication of the talking state of the endpoint. • t — At the time the command was invoked, voice energy (talking) was detected from the endpoint. • m — At the time the command was invoked, the endpoint indicated to the MCU that it was muted. It is possible that an endpoint may mute, but not send any indication to the MCU. In this situation the MCU does not display a mute indication. • M — At the time the command was invoked, the endpoint's audio was muted via UDD/CRCS Agent interface. M displays when both the endpoint and the UCC/CRCS Agent have muted the endpoint audio. • S — At the time the command was invoked, the endpoint's audio was muted because of solo-audio state set by UCC/CRCS Agent. While in solo-audio state, new endpoints joining the conference are automatically muted. • blank — At the time the command was invoked, voice energy (talking) was not being detected from the endpoint.

Table continues...

Field	Description
Vs	• a — This value applies only to quad-screen conferences. *a indicates that an endpoint is part of the current mixed image and is fixed in one of the quadrants via administration. *a indicates that the endpoint is fixed in a quadrant but is not currently connected (Fill image displays). • b — For full-screen conference it indicates that at the time the command was invoked, this endpoint's video was being broadcast to other sites. This conference was in VAS, broadcast, or presentation mode. For quad-screen VAS conference it is prefixed with an asterisk (*) and indicates that this endpoint's video is part of the mixed image because of VAS. For quad-screen presentation conferences, b(without an asterisk) identifies the presenter as the broadcaster. • B — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • c — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in chair mode and the broadcaster was designated by the chair. Chair features can only be performed in full-screen mode. • i — At the time the command was invoked the endpoint was not a valid video source. For continuous presence conference, if this endpoint is fixed in a particular quadrant, a pound (#) is affixed before i. • r — For full-screen conferences, at the time the command was invoked the endpoint's video was the return video to the broadcaster. For continuous presence conference in presentation mode, *r represents a VAS quadrant that is part of the mixed image. • R — At the time the command was invoked, the endpoint's video was the return video to the broadcaster because of the UCC browse feature. UCC Browse feature can only be performed in full-screen mode. • s — At the time the command was invoked this endpoint's video was suppressed at the request of the endpoint. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant a pound (#) is affixed before s. • S — At the time the command was invoked this endpoint's video was suppressed via UCC/CRCS Agent interface. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant, a pound (#) is affixed before S. S is displayed when the endpoint and the UCC/CRCS Agent have suppressed the endpoint video.

Table continues...

Field	Description
	• u — For full-screen conferences, at the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode and the broadcaster was designated by the UCC/CRSCS Agent interface. For quad-screen conferences, it indicates that UCC/CRCS Agent designated this endpoint as fixed in a quadrant. An asterisk (*) is affixed before u if the endpoint is currently part of the quad image, and a pound (#) is affixed if the endpoint is not currently joined. • U — Applies only to quad-screen conference and indicates that UCC/ CRCS Agent designated a quadrant as VAS. An asterisk (*) is affixed before U to indicate that this endpoint is part of the current quad image. • v — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode but the endpoint has asked to be a broadcaster via See-Me request and was granted a MCV (Multipoint Command Visualize) token. The See-Me feature is only performed in full-screen mode. • blank — At the time of the request the endpoint's video was not broadcast, return, video, or part of the mixed-image, but it is a valid video source.

status conference output field descriptions — page 2

Field	Description
Sum Grp	The VD audio Level 1 (L1) and Level 2 (L2) summer group parts for each assigned group (1–4). Summer parts are assigned only for conferences with over 6 participants. When a conference operates at an audio mode of 7 kHz (administered audio mode is 7 kHz, or auto with the bandwidth greater than 128 kbps), the system allocates “primary” and “secondary” L1 and L2 summer parts. These primary and secondary parts are allocated as adjacent port slots on the same board. Status conference only displays the primary summer ports. The secondary summer ports are always one slot higher than the displayed primary summer port.
Join Time	Time (in 24-hour notation) when the channel joined the conference.
Drop Time	The endpoint is idle if the first channel has a drop time.

Table continues...

Field	Description
Drop Reason	The reason for the channel's disconnect: • 2-pri — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as primaries (see Cascading for a description of primary-secondary compatibility). • 2-sec — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as secondaries (see Cascading for a description of primary-secondary compatibility). • Agent — The reservation agent has caused the call to disconnect (for example, the agent has changed a connected dial-out destination number). • Bandwidth — mismatch between a call and the conference it attempted to join. For example, a 56-kbps call attempted to join a 64-kbps conference that does not permit rate adaptation. • BondHshake — Bonding handshake drop reason can be caused due to the following reasons: information channel parameter not supported or invalid, parameter negotiation terminated out of sequence, timer expired because of the secondary channels did not establish, or BONDing framing was not detected for one of the other channels. • Busy — This dial-out drop reason occurs when the MCU detects that the conferee's terminal equipment is busy. This drop reason is detected by an ISDN cause value (for example, h0). See Dial-out for a description of CPTR usage. • Chair — disconnected the endpoint, using either Chair Command Disconnect (CCD) or Chair Command Kill (CCK) signals. • Conf End — The conference was ended due to reaching stop time for a reserved conference or due to an active conference being converted to file. • Endpoint — Clearing received from DS1. The disconnect came from the endpoint. The endpoint notified the MCU that it intended to disconnect. • Far-end — Clearing received from DS1. The disconnect came from either the network or the endpoint. • Handshake — Either framing was never found (the endpoint could not complete initialization: problems finding Frame Alignment Signal (FAS), Multi Frame Alignment (MFA) and getting a corrected coded cap-set) or framing was lost for some time (over 40 seconds) and the endpoint was disconnected.

Table continues...

Field	Description
	• IDtimeout — The MCU has not received response to the UIN/ password Query from the H.320 user after three attempts. Each attempt has a system administered timeout period. • Internal — MCU has a problem allocating trunk resources necessary to route the dial-out call for the specified dial-numbers. This problem can be associated with routing pattern or trunk associated translation (for example, TAC specified in the dial-out number or routing pattern points to a trunk group without members), or it can indicate a lack of trunk resources (for example, every trunk member is maintenance busy or every in-service member is busy on a call). • Network — Clearing received from DS1. The disconnect came from the network. The endpoint that had the disconnect notification capability disconnected without notifying the MCU. • No-ring — This dial-out drop reason occurs when the call has been up for 30 seconds and no ringing is detected. • Not-MCU — The dial-out destination number(s) of the CAS extension has terminated to a number that is not a dial-in cascade MCU extension. • Password — Either the user entered the wrong password or the audio add-on user did not enter it within the specified time period. Note that the audio add-on user gets one attempt to enter a correct password and inter-digit timing for each digit (that is, about 10 seconds between digits). • Pre-AnsDrop — The call disconnected before answer by an endpoint. The cause of the disconnect may be the network, an endpoint, or a terminal adapter. This drop reason is different from No-answer, which indicates that a 60-second timeout occurred while alerting. In this case, the call drops before the 60-second timer has expired. Some busy endpoints connected through terminal adapters display this behavior. • Resource — MCU could not provide resources (VC or MMI) when the call arrived or lost the resources during the call. This could be due to them being Out of Service, busied out by craft, or being used by system maintenance. This drop reason could also occur if the DS1/ MMI cable is disconnected. If there was a resource problem when the call arrived, it would get reorder (fast busy) and not get disconnected by the MCU. • Reorder — This dial-out drop reason occurs when the MCU detects that there are no available trunks in the network to place the call. This drop reason is detected by MCU CPTR resources. See Dial-out for a description of CPTR usage. • System — An MCU restart (level 2) disconnected every call.

Table continues...

Field	Description
	• UIN-Inv — The user entered an invalid User Identification Number. • Unknown — The system could not determine the cause of the disconnect. • Wrong-num — This dial-out drop reason occurs when the MCU detects the wrong destination number was dialed. This drop reason is detected by MCU CPTR resources SDN cause value. See Dial-out for details. • UCC — controller intentionally disconnected the endpoint.
AC Num	Administered Connection Number - from 1 to 128. AC number can be used to further diagnose a problem by combining status conference information with status administered connection and data stored in the error and alarm logs.
Ports Trunk	The data endpoint that the channel is using.
Ports Video	The MMI port for the channel.
Ports Aud	If the endpoint type is not UCC, the VC audio encoder port (which is always paired to a decoder port) for the channel (only the first channel). Because only one audio encoder port is allocated per endpoint, it is together with the ESM data port in the endpoint's channel 1 port slot position of the Port Aud/ESM column. For UCC endpoint type, the channel 1 port slot position displays the allocated Call Classifier resource.
Ports ESM	The Expansion Service Module MMI data port. This field is always blank.
Sum Grp	Endpoint's assigned summer group number. The summer group port assignments are on screen 1.
Software	For Avaya use only.

status conference x endpoint y field descriptions — page 1

Field	Description
Endpoint	Endpoint-ID is a slot number associated with the endpoint entered on the conference forms.
Product	Product identification number obtained from the endpoint.
Manufacturer/Country	Manufacturer identification number and manufacturer's country code obtained from the endpoint.
Terminal Name	blank
Sum Grp	Summer group number to which this endpoint belongs and the VC Audio Level (L1) and Level 2 (L2) summer ports for this group. These fields have an entry only for conferences with over 6 participants.
Dial Out #1	Blank
Dial Out #2	Blank

Table continues...

Field	Description
In Use	Is the endpoint currently participating in the conference or in process of connecting to the conference? • y — The endpoint is in use and is fully connected on all media in an active conference. • c — The endpoint is in use and is fully connected, however the endpoint has changed the conference audio or video capability or has changed the rate of the conference because of rate adaptation. This condition requires analysis of this endpoint's capabilities and mode fields to identify which capability was reduced. • e — The endpoint is in use but the endpoint had capability problems. The endpoint does not have one of the required capabilities (Vid, Bhl, MLP) to be a full participant. For MLP capabilities, see the T120 field. This condition requires analysis of this endpoint's capabilities and mode field to identify the missing capability. • f — The endpoint is in use but is disconnected from all media. This indicates that the endpoint has declared every required capability (channel/video/audio/data) but is not fully connected to all conference media at this time. This endpoint may be in the process of connecting, has failed to connect, or is not a valid video source. This condition requires analysis of this endpoint's capabilities and mode fields to identify the problem. • n — The endpoint was connected in a conference but has/was disconnected or attempted to connect to a conference but was unsuccessful. • blank — until the first call is made from/to the endpoint.
Enh BAS	Enhanced Basic Service Flag • y — The endpoint supports the enhanced BAS commands/caps • n — The endpoint only supports the basic BAS commands/caps
Chl	Data on the quantify and quality of channels (transfer rate)? • y — The endpoint has the required number of channels. • e — The endpoint has not declared support for the correct number of channels and cannot participate fully in the conference. • n — The endpoint has declared the correct number of channels, but every channel has not yet joined the conference, due to either a network or endpoint problem. • blank — Audio add-on endpoints always have a blank Chl field.

Table continues...

Field	Description
Aud	Does the endpoint have the required audio capability? • y — The endpoint has the required audio capability. Audio add-on endpoint always have the Aud field set to y once the endpoint has joined the conference. • c — This endpoint is PCM only, and it changed the video quality of the conference by changing the operating audio from G.728 to G.711. If the administered audio mode is auto and the administered bandwidth is 112 kbps (56 k/channel) or 128 kbps (64 k/channel), the system starts out with the highest common audio of G.728. When the administered bandwidth is greater than 128 kbps, the system starts out with the highest common bandwidth of 7 kHz. • e — A PCM-only endpoint that did not have the capability of supporting the administered audio mode of G.728 (such as a data conference). G.278/G.711 endpoint that did not have the capability of supporting the administered audio mode of 7 kHz. Such endpoints operate with PCM audio and interwork with the current operating audio mode. • blank — The field is blank until the first call is made from/to the endpoint.
Vid	Does the endpoint have the required video capability and is receiving video? • y — The endpoint has the required video capability and should be receiving video if the Chl, Aud, and Dat fields are y. • c — It downgraded the conference's video quality - either from CIF to ACIF or by decreasing the frame rate. The conference video mode is set by default to CIF and if a QCIF-only endpoint joins the conference, then the entire conference is made to operate in QCIF, with the video clarity downgraded. Also, the conference frame rate is initially set to the highest frame rate that can then be reduced by any endpoint. If the conference video mode is not administered with upgrade capability, then if the video parameters for a conference have been downgraded, they are not upgraded until every endpoint disconnects from the conference. • e — The endpoint has not declared any video capability in its cap-set. • n — Audio only, not receiving video, possibly due to an audio or data problem. • blank — Audio add-on endpoint always have the Vid field set to blank.

Table continues...

Field	Description
Mlp	The state of the Control Link to the ESM (T.120 stack terminator), the endpoint MLP data capability, and the state of the data connection in the T.120 stack. This field value is always blank, indicating that the Data Mode for the conference is none , and therefore, the data does not apply, or the endpoint has never joined the conference.
Gx	Does the endpoint have the Still Frame Graphics capability? • y — This endpoint has this capability. • e — This endpoint did not declare this capability. The conference retains the still frame graphics capability when a non-compliant endpoint joins the conference. • blank — This endpoint has never joined the conference.
Rate Adpt	Rate adaptation/Interworking indicator. Values of 5 and 6 apply only to low-speed/high-speed interworking. Every other value applies only to rate adaptation. • 5 — A 56-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • 6 — A 64-kbps (low-speed) endpoint has joined a high-speed (128-kbps or above) conference. This endpoint is connected with audio-only capability, but is neither a valid video source nor destination. • y — This endpoint has joined the conference at the administered rate of 64 kbps, but (because rate adaptation to 56 kbps was triggered by another endpoint) this endpoint has successfully rate adapted to 56 kbps. • c — The administered bandwidth of the conference is 64 kbps and this endpoint has joined the conference at 56 kbps. The first 56-kbps endpoint that joins 64-kbps rate-adaptable conference triggers rate adaptation (see Join Time below). • n — A 64-kbps conference was triggered to rate adapt to 56 kbps by some other endpoint. This endpoint joined the conference at the bandwidth of 64 kbps, but encountered problems in rate adapting down to 56 kbps. This endpoint may have the audio and may be receiving video, but is not a valid video source. • blank — Rate adaptation was never triggered by any endpoints. So, if this endpoint is in use and connected, then it joined the conference at the administered bandwidth.
Bond Mode	Bonding Mode — blank. This field is blank for calls that are not related to bonding.

Table continues...

Field	Description
Ts	Indication of the talking state of the endpoint. • t — At the time the command was invoked, voice energy (talking) was detected from the endpoint. • m — At the time the command was invoked, the endpoint indicated to the MCU that it was muted. It is possible that an endpoint may mute, but not send any indication to the MCU. In this situation the MCU does not display a mute indication. • M — At the time the command was invoked, the endpoint's audio was muted via UDD/CRCS Agent interface. M displays when both the endpoint and the UCC/CRCS Agent have muted the endpoint audio. • S — At the time the command was invoked, the endpoint's audio was muted because of solo-audio state set by UCC/CRCS Agent. While in solo-audio state, new endpoints joining the conference are automatically muted. • blank — At the time the command was invoked, voice energy (talking) was not being detected from the endpoint.

Table continues...

Field	Description
Vs	Indication of the MCU video state for this endpoint. For quad-screen conferences, an asterisk (*) is affixed before the value of Vs to indicate that an endpoint is currently part of the mixed image. A pound (#) may be affixed before the value of Vs to indicate that an endpoint was fixed to be in the mixed image (via administration or UCC/CRCS Agent), but instead, a Fill video is shown in its place. This occurs when the video of an endpoint that is fixed in a quadrant cannot be used as a video source because the endpoint is currently not joined to the conference, has suppressed its video, or has invalid video to be the video source. Notice that at most four endpoints have an * or # affixed before the Vs field value. For quad-screen conference in VAS mode, the mixed image is broadcast to every endpoint. For quad-screen conference in presentation mode, the mixed image is return video to the presenter. • a — This value applies only to quad-screen conferences. *a indicates that an endpoint is part of the current mixed image and is fixed in one of the quadrants via administration. *a indicates that the endpoint is fixed in a quadrant but is not currently connected (Fill image displays). • b — For full-screen conference it indicates that at the time the command was invoked, this endpoint's video was being broadcast to other sites. This conference was in VAS, broadcast, or presentation mode. For quad-screen VAS conference it is prefixed with an asterisk (*) and indicates that this endpoint's video is part of the mixed image because of VAS. For quad-screen presentation conferences, b(without an asterisk) identifies the presenter as the broadcaster. • B — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • c — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in chair mode and the broadcaster was designated by the chair. Chair features can only be performed in full-screen mode. • B — At the time the command was invoked the endpoint's video was being broadcast to other sites because of the UCC roll call feature. UCC roll call feature can only be performed in full-screen mode. • i — At the time the command was invoked the endpoint was not a valid video source. For continuous presence conference, if this endpoint is fixed in a particular quadrant, a pound (#) is affixed before i. • r — For full-screen conferences, at the time the command was invoked the endpoint's video was the return video to the

Table continues...

Field	Description
	broadcaster. For continuous presence conference in presentation mode, *r represents a VAS quadrant that is part of the mixed image. • R — At the time the command was invoked, the endpoint's video was the return video to the broadcaster because of the UCC browse feature. UCC Browse feature can only be performed in full-screen mode. • s — At the time the command was invoked this endpoint's video was suppressed at the request of the endpoint. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant a pound (#) is affixed before s. • S — At the time the command was invoked this endpoint's video was suppressed via UCC/CRCS Agent interface. For continuous presence conference with fixed quadrant participants, if this endpoint is fixed in a particular quadrant, a pound (#) is affixed before S. S is displayed when the endpoint and the UCC/CRCS Agent have suppressed the endpoint video. • u — For full-screen conferences, at the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode and the broadcaster was designated by the UCC/CRCS Agent interface. For quad-screen conferences, it indicates that UCC/CRCS Agent designated this endpoint as fixed in a quadrant. An asterisk (*) is affixed before u if the endpoint is currently part of the quad image, and a pound (#) is affixed if the endpoint is not currently joined. • U — Applies only to quad-screen conference and indicates that UCC/ CRCS Agent designated a quadrant as VAS. An asterisk (*) is affixed before U to indicate that this endpoint is part of the current quad image. • v — At the time the command was invoked this endpoint's video was being broadcast to other sites. The conference was in VAS mode but the endpoint has asked to be a broadcaster via See-Me request and was granted a MCV (Multipoint Command Visualize) token. The See-Me feature is only performed in full-screen mode. • blank — At the time of the request the endpoint's video was not broadcast, return, video, or part of the mixed-image, but it is a valid video source.

status conference x endpoint y field descriptions — page 2

Field	Description
Join Time	Time (in 24-hour notation) when the channel joined the conference.
Drop Time	The endpoint is idle if the first channel has a drop time.

Table continues...

Field	Description
Drop Reason	The reason for the channel's disconnect: • 2-pri — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as primaries (see Cascading for a description of primary-secondary compatibility). • 2-sec — This drop reason occurs when an administration error causes a mismatch in primary-secondary designation for a cascade link. This mismatch shows that both MCUs are administered as secondaries (see Cascading for a description of primary-secondary compatibility). • Agent — The reservation agent has caused the call to disconnect (for example, the agent has changed a connected dial-out destination number). • Bandwidth — mismatch between a call and the conference it attempted to join. For example, a 56-kbps call attempted to join a 64-kbps conference that does not permit rate adaptation. • BondHshake — Bonding handshake drop reason can be caused due to the following reasons: information channel parameter not supported or invalid, parameter negotiation terminated out of sequence, timer expired because of the secondary channels did not establish, or BONDing framing was not detected for one of the other channels. • Busy — This dial-out drop reason occurs when the MCU detects that the conferee's terminal equipment is busy. This drop reason is detected by an ISDN cause value (for example, h0). See Dial-out for a description of CPTR usage. • Chair — disconnected the endpoint, using either Chair Command Disconnect (CCD) or Chair Command Kill (CCK) signals. • Conf End — The conference was ended due to reaching stop time for a reserved conference or due to an active conference being converted to file. • Endpoint — Clearing received from DS1. The disconnect came from the endpoint. The endpoint notified the MCU that it intended to disconnect. • Far-end — Clearing received from DS1. The disconnect came from either the network or the endpoint. • Handshake — Either framing was never found (the endpoint could not complete initialization: problems finding Frame Alignment Signal (FAS), Multi Frame Alignment (MFA) and getting a corrected coded cap-set) or framing was lost for some time (over 40 seconds) and the endpoint was disconnected.

Table continues...

Field	Description
	• IDtimeout — The MCU has not received response to the UIN/ password Query from the H.320 user after three attempts. Each attempt has a system administered timeout period. • Internal — MCU has a problem allocating trunk resources necessary to route the dial-out call for the specified dial-numbers. This problem can be associated with routing pattern or trunk associated translation (for example, TAC specified in the dial-out number or routing pattern points to a trunk group without members), or it can indicate a lack of trunk resources (for example, every trunk member is maintenance busy or every in-service member is busy on a call). • Network — Clearing received from DS1. The disconnect came from the network. The endpoint that had the disconnect notification capability disconnected without notifying the MCU. • No-ring — This dial-out drop reason occurs when the call has been up for 30 seconds and no ringing is detected. • Not-MCU — The dial-out destination number(s) of the CAS extension has terminated to a number that is not a dial-in cascade MCU extension. • Password — Either the user entered the wrong password or the audio add-on user did not enter it within the specified time period. Note that the audio add-on user gets one attempt to enter a correct password and inter-digit timing for each digit (that is, about 10 seconds between digits). • Pre-AnsDrop — The call disconnected before answer by an endpoint. The cause of the disconnect may be the network, an endpoint, or a terminal adapter. This drop reason is different from No-answer, which indicates that a 60-second timeout occurred while alerting. In this case, the call drops before the 60-second timer has expired. Some busy endpoints connected through terminal adapters display this behavior. • Resource — MCU could not provide resources (VC or MMI) when the call arrived or lost the resources during the call. This could be due to them being Out of Service, busied out by craft, or being used by system maintenance. This drop reason could also occur if the DS1/ MMI cable is disconnected. If there was a resource problem when the call arrived, it would get reorder (fast busy) and not get disconnected by the MCU. • Reorder — This dial-out drop reason occurs when the MCU detects that there are no available trunks in the network to place the call. This drop reason is detected by MCU CPTR resources. See Dial-out for a description of CPTR usage. • System — An MCU restart (level 2) disconnected every call.

Table continues...

Field	Description
	• UIN-Inv — The user entered an invalid User Identification Number. • Unknown — The system could not determine the cause of the disconnect. • Wrong-num — This dial-out drop reason occurs when the MCU detects the wrong destination number was dialed. This drop reason is detected by MCU CPTR resources SDN cause value. See Dial-out for details. • UCC — controller intentionally disconnected the endpoint.
Drop Code	A detail code complementing the Drop Reason (see above). Additional bonding related information may be obtained from supplementary Bonding Drop Codes described above.
AC Num	Administered Connection Number - from 1 to 128. AC number can be used to further diagnose a problem by combining status conference information with status administered connection and data stored in the error and alarm logs.
Ports Trunk	The data endpoint that the channel is using.
Ports Video	The MMI port for the channel.
Ports Aud	If the endpoint type is not UCC, the VC audio encoder port (which is always paired to a decoder port) for the channel (only the first channel). Because only one audio encoder port is allocated per endpoint, it is together with the ESM data port in the endpoint's channel 1 port slot position of the Port Aud/ESM column. For UCC endpoint type, the channel 1 port slot position displays the allocated Call Classifier resource.
Ports ESM	The Expansion Service Module MMI data port. This field is always blank.
Ports Bonding	The MMI port used for Bonding for the channel.
Fr Err	Frame error counter. A circular hex counter (0-FF) to indicate the occurrence of framing errors.

status conference x endpoint y field descriptions — page 3, Conference Info

Field	Description
Conference Info	
Applies mostly to full-screen conferences.	

Table continues...

Field	Description
Broadcaster	Indicates the endpoint number that is the current broadcaster. Applies to full-screen and quad-screen presentation mode conferences. • Broadcast — a broadcast mode broadcaster. • Chair — the broadcaster was designated by the chair. • See-Me — the broadcaster is a result of MCV request from an endpoint. • Presenter — a presentation mode broadcaster. • Rollcall — the broadcaster was designated by the UCC via the Rollcall feature. • UCC — the broadcaster was designated by the UCC. • VAS — Voice Activated Switching broadcaster.
Next Broadcaster	Indicates the endpoint number that is selected to be the next broadcaster.
Return Vid	Indicates the endpoint number that is the current return video. The return video can be qualified with the following keywords: • blank — the return video is the previous broadcaster forced to be return video because of VAS, action by Chair, action by UCC, or endpoint MCV request. The broadcaster qualifier identifies which action forced this endpoint to become return video. • Autoscan — auto scan return video. This is true only when conference mode is broadcast with auto scan. • Browse — the return video was designated by the UCC via the Browse feature. • VAS — a Voice Activated Switching return video.
Next Return Vid	Indicates the endpoint number that is selected to be the next return video. MCU

status conference x endpoint y field descriptions — page 3, Mode Commands/Communication Modes

This is a collection of both incoming and outgoing bandwidth allocations for the multiplex. The Incoming data is the rate at which the MCU thinks the endpoint is communicating based on the Bit-rate Allocation Signal (BAS) codes received from the endpoint/codecs and the capabilities the MCU has declared. The Outgoing data is the rate from the MCU toward the endpoint.

Field	Description
Conf	The desired conference operating mode. This may be different from the endpoint in (EPT-IN) or endpoint out (EPT-OUT) modes.
Cmd	labels for the various types of mode commands

Table continues...

Field	Description
Stat	Compatibility of conference mode and the incoming mode. • y — indicates mode compatibility • n — indicates that the modes are not compatible
EPT-IN	Communication modes coming in from an endpoint.
EPT-OUT	Communication modes sent out to an endpoint based on the number of channels connected and the capabilities of the endpoint.
XRate	One of the supported transfer rates. XRATE may be 64 when the endpoint is just dialing in, or in the event of problems. It implies that only one B-channel is being used.
Audio	Audio rate (kbps bandwidth) of the conference and the endpoint must be the same but not necessarily their mode. When the audio rate of the conference and the endpoint are different the endpoint's audio will interwork but the endpoint's video will be invalid. MCU may or may not send video to such an endpoint. Other possible AUDIO mode values include neutral (neutralized I-channel) and Au-off , Frm (no audio signal) which never match conference mode and are not supported by MCU.
56/64	The 56/64 field is derestrict when operating at per-channel rates of either 64, 128, 192, 256, 320, 384, 512, 768, 1472, 1536, or 1920 kbps. It is restrict when operating at rates of either 56, 112, 168, 224, 280, 336, 448, or 672 kbps. Note that if the conference is configured for N x 56-kbps operation, the endpoint may signal either via capabilities or modes that is operating at the proper rate. In such a case, even when we receive derestrict command which does not match the conference communication mode of restrict , if the capability indicates restrict (MISC capability has restrict displayed on Page 4) the STAT 56/64 is y to indicate 56/64 compatibility between the conference and the endpoint.
Video	The Video mode: H.261 (recommended), H.CTX (proprietary), H.CTX+ (proprietary), or SG4 (proprietary) indicate that video is on in the direction indicated; video-off when the video is off.
Mlp	Multi Layer Protocol data mode. When Data Mode is administered as any-mlp or ww-pcs , the MLP mode should be var-MLP . Other values will affect video status. The MLP mode should be MLP-off when Data Mode is administered as none . Again, other values in this mode will affect video status.
H_Mlp	The High Speed MLP mode. The HMLP mode should be H-MLP-off . Other values in this mode will affect video status.
LSD	Low Speed Data mode. The LSD mode should be LSD-off . Other values in this mode will affect video status.

Table continues...

Field	Description
HSD	High Speed Data mode. The HSD mode should be HSD-off . Other values in this mode will affect video status.
CRYPT	Encryption mode. The CRYPT mode should be encrypt-off . Other values in this mode will affect video status.
S/M	Single-/multi-channel interoperability mode. 6B-H0-comp indicates that the sender is interoperating multiple channels and a single channel (for example, 6B and H0). Not-comp-6B-H0 indicates that the sender is not interoperating between 6B and H0. Normally this value is Not-comp-6B-H0 . Other values in this mode will affect video status.

status conference endpoint field descriptions — page 3, Endpoint Misc Info

EPT MISC contains miscellaneous states and counters for an endpoint. The flags can be **y** or **n**. The counters start with initial value of 0x00, they increment to 0xff, and then wrap around to 0x01. **AIM** and **VIS** are BAS commands which can be sent as input (I) to MCU from an endpoint or as output (O) from MCU to an endpoint.

Field	Description
AIM	Audio Indicate Muted. y on input (I) indicates that this endpoint has muted its audio. MCU will not VAS to an endpoint displaying mute indicate. n on input indicates that this endpoint has not muted (only if endpoint audio mode is turned on). y on output (O) indicates that every other endpoint in the conference has muted its audio (have sent AIM to MCU). MAC in turn tells this endpoint (by sending it AIM) that there is no audio output from MCU. n on output indicates that there is an audio path open across the bridge.
VIS	Video Indicate Suppressed. y on input (I) indicates that this endpoint has suppressed its video (indicated video is muted). y on output (O) indicates that the MCU is not sending video to this endpoint because there is no video broadcaster (broadcaster has not joined or broadcaster's video is not valid).

Table continues...

Field	Description
MIS	Multipoint Indicate Secondary-status. This command is only sent as output (O) to an endpoint. n indicates that the endpoint is viewed as capable of being a valid source (although not necessarily at this moment). y is correct for video. y indicates that MIS was sent to an endpoint and that this endpoint is viewed as a secondary endpoint. The endpoint is included in the audio portion of the conference but not the video portion. Video will not be sent.
MCV	Multipoint Command Visualize. This command is only sent as input (I) from an endpoint. y indicates that an endpoint has requested to become a broadcaster. This is used during Still Frame Graphics and to force presentation mode.
TALK	Multipoint Command Visualize. This command is only sent as input (I) from an endpoint. y indicates that an endpoint has requested to become a broadcaster. This is used during Still Frame Graphics and to force "presentation" mode.
VRCV	y indicates if the endpoint is receiving video (MMCH is sending video to the endpoint). The VRCV counter indicates the number of times video was sent/not sent to this endpoint.
BCTK	Applies to single screen and quad-screen presentation mode conferences. y indicates that the endpoint is the video broadcast source. The BCTK counter indicates the number of times this endpoint was the video broadcast source.
RTTK	Applies to single screen conferences. y indicates that the endpoint is the return video source. The RTTK counter indicates the number of times this endpoint was the return video source.
BCLS	Applies to single screen and quad-screen presentation mode conferences. y indicates that the endpoint is watching the video of the broadcast source.
RTLS	Applies to single screen conferences. y indicates that the endpoint is watching the video of the return source.
HYPR	y indicates hyperactivity from an endpoint (MCU isolated endpoint from the MCU conference due to thrashing behavior) and affects endpoint's status as a video source (for 5 seconds of hyperactivity timer). The HYPR counter indicates the number of times this endpoint was hyperactive.

Table continues...

Field	Description
DMUTE	y indicates that the decoder was muted by the VC board or the software in the MCU. VC board mutes the decoder when it loses MMI or endpoint framing is lost, when it receives an invalid audio code word, and when endpoint is hyperactive. The only time that the MCU software mutes the decoder of an endpoint is to mute every endpoint, other than the broadcaster, when a mode of a conference is broadcastw/scan (broadcast with auto scan). The DMUTE counter indicates the number of times this endpoint's decoder was muted by the VC board.
VFMT	The video format applicable only to quad-screen conferences. Always n , indicating QCIF format.
H.261	y indicates video framing loss. The H.261 counter indicates the number of times the framing was lost.

status conference endpoint field descriptions — page 3, Frame Alignment Word Info

Frame Alignment Word (FAW) includes channel information for the communication paths labeled CHL 1 and 2. For 2B calls, both CHL 1 and 2 are used. For 1-channel calls (at rates of 112, 128, 168, 196, 224, 256, 280, 320, 336, 384, 768, 1472, 1536, and 1920 kbps), only CHL 1 is used.

A-OUT, **A-IN**, **M-FRM**, **MFA**, and **MFN** are flags with values of **y** or **n**.

Field	Description
A-OUT	MCU has endpoint framing.
A-IN	Endpoint has MCU framing.
M-FRM	Multichannel frame alignment is present (alignment of both channels in 2B).
MFA	Multiframe alignment word is present (required in 2B call).
MFN	Multiframe numbering is present (required in 2B call).
FAS	Frame Alignment Signal (FAS) channel number (1 or 2). This number should match the column header.
MCUFAL	MCU Frame Alignment Loss (MCUFAL). A counter of the number of times the MCU indicates to the endpoint that it has lost endpoint FAW or multichannel synchronization (M-FRM). The MCU a-bit toggles when the MCU gains or loses endpoint multichannel synchronization. This counter starts with an initial value of 0x00, increments to 0xff, then wraps around to 0x01. The MCUFAL count is also shown in the Fr Err field.
FEFAL	Far End Frame Alignment Loss (FEFAL). A counter of the number of changes the MCU detects in the endpoint's a-bit (A-OUT). The endpoint a-bit toggles when an endpoint gains or loses MCU framing. This counter starts with an initial value of 0x00, increments to 0xff, then wraps around to 0x01.

status conference endpoint field descriptions — page 4

Fields on this page only when an endpoint declares the specific capability. For example, if an endpoint does not declare the VID H.CTX capability, the H.CTX field does not display.

Field	Description
VID	Provides information about the type of video and frame rate the endpoint supports. vfmt — does not display if the endpoint has no video capability. Every value is blank if there is an active call or if this is an audio-only endpoint. Otherwise, values for this field include: • FCIF — full CIF. • QCIF — quarter CIF. Support of CIF implies support of QCIF. In general, for larger screens, CIF displays sharper resolution video, which ZCIF is blocked, but may run at higher frame rates and less clear. The differences are less observable on very small displays. • cfps and qfps — maximum frame rate (frames/second) at which the endpoint can receive video for CIF and QCIF operating modes. CIF frame-rate values are 30 fps, 15 fps, 10 fps, and 7.4 fps. If the endpoint does not support CIF (that is, the vfmt field is QCIF), the cfps value should be blank. • da_sfg — indicates support for H.261 Still Frame Graphics transfers. • H.CTX, H.CTX+ and SG4 — proprietary video format capabilities. • SG4_sfg — indicates support for SG4 Still Frame Graphics.
MISC	The restrict field is one way for an endpoint to indicate that it is operating at 56 kbps per channel. Another way is the 56/64 command mode with restrict. An endpoint on a 56-kbps conference must send one or both of the 2 indications that they are operating at 56 kbps before they become a video source in a 56-kbps conference. If they signal either way that they are operating at 56 kbps in a 64- or 384-kbps conference, they are an audio-only source, but the MCU continues to send Selected Communication Mode (SCM) toward them when possible. A MISC capability of derestrict and a 56/64 command of derestrict together indicate that an endpoint is operating at 64 kbps. If either is restrict, the conference operates at 56 kbps. Other field values include: • dcomp — indicates support for WorldWorx PCS data compliance. • mbe — indicates support for Multi Byte Extension. MBE capability is used for the exchange of passwords, terminal names, and other special capabilities, such as, support of WorldWorx PCS specific features. • cic — Chair Indicate Capability. Indicates chair control capability.

Table continues...

Field	Description
XR	Transfer rate capabilities are statement about the speeds at which the endpoint can operate over the current connection and operate a Px64 Multiplex. For a 384-kbps (H0) call, the endpoint sends its capabilities to indicate 384-kbps support, which displays as 384. On a 336-kbps call, the endpoint must signal 384-kbps support. If an endpoint does not indicate support for 384 kbps on a 384-/ 336-kbps conference, the MCU provides Audio Only Communications Mode (ACOM). For a 2B conference, the MCU sets the rate to 2x64, expecting the endpoints to do likewise (64x2 is displayed; if this is not displayed, there is no 64x2 capability). Endpoints may occasionally take 2x64 (or the current channel rate: 384, 768, 1472, 1536) out of their capability. This is Mode 0 forcing and is part of normal procedures. The MCU will provide AOCM if the endpoint does not signal support matching the configuration of the conference.
AUD	The audio fields are statements of the audio protocols that the endpoint supports. 711m and 711a are PCM (G.711) and support Mu and A-law, respectively, and at least one is required of endpoints. The g728 field indicates whether G.728 is supported (LB_CELP). This value depends upon the type of the endpoint and how that endpoint is currently configured. The g722_48 field indicates endpoint support for G.722 (7 kHz) at both 48 and 56 kbps. Therefore, g722_48 indicates that the endpoint supports G.722 audio at both rates. The g722_64 field indicates endpoint support for G.722 at 64 kbps in an unframed (not supported by the MCU) mode.
LSD	The LSD fields indicate the capabilities for Low Speed Data conferencing.
HSD	The HSD fields indicate the capabilities for High speed Data conferencing.
MLP	The MLP fields indicate the capabilities for Multi Layer Protocol Data capabilities.
HMLP	The HMLP fields indicate the conference's capability for High Speed MLP data conferencing.

status conference endpoint field descriptions — page 5, Endpoint Call Status Information

This screen summarizes such call-related status as per-channel join counts, join/drop time, drop reason, drop code, and auxiliary bonding drop code. It also contains a drop code and software fields from the previous call. The data on the page is always retained. The Endpoint Call Status Information section groups together call-related fields. The Join Count field is described below, and other fields are described in the following field description tables.

Field	Description
Join Count	Shows the number of times this endpoint joined this conference during this conference session. This counter starts with 0, can increment to 64, and wraps around back to 1.

status conference endpoint field descriptions — page 6, Administered Connections

This screen summarizes information about the administered connections associated with this endpoint. This data can be viewed while the conference is active.

Field	Description
Dial-Out Number	The actual numbers that are dialed out by the administered connections for each channel in the call. Note that the dial Out #1 and #2 on page 1 of the forms display the DCP endpoint number. This is particularly useful with bonding dial-out calls.
Connection State	Indicates the current call state of the AC. The following are connection states associated with dial-out ACs: • enabled — transient in nature and indicates that an AC is about to enter the attempting to connect state. • disabled — this may mean one of three things: - The AC has reached an administered retry threshold, and all retries are stopped. Verify this by checking the error log and checking whether an error type of 9 is logged against the AC. - The AC was in a connected state and the far end disconnected. - The initial channel call has not yet connected. No dial out call attempt is made for the additional channel(s) until the initial channel has reached a connected state. • not scheduled — transient in nature and indicates that an AC is about to enter the attempting to connect state. • waiting to retry — the AC is inactive (sleeping) and waiting for the retry timer to expire. Once the timer expires, the AC sends a dial out call and enters the attempting to connect state. ACs in this state indicate that the dial out call has failed at least once. • attempting to connect — the AC is active on a call, but the call has not yet connected. • connected — the call associated with the AC has been answered and join cut-through to the conference.
Retry Count	Number of retries have been attempted for this AC during this join attempt. This field does not clear when the AC connects. This field clears when a new join attempt is made via a Redial feature. Note that this is different from the Join Count which counts the number of times the channel joined the conference during this conference session.
Failure Cause	ISDN or CPTR cause value (values lower than 0x7f) recorded when the last dial out call was dropped. Values above 0x7f are generated internally. The following table lists all possible failure cause values displayed by this field and its associated description. This value is logged in the error log and is displayed with display errors . Err Type is displayed as a decimal.

Status AC — Failure Cause Values

Failure Causes	Description
0x00 (0t0)	Not applicable
0x01 (0t1)	Incorrect destination address
0x02 (0t2)	Reason unknown
0x06 (0t6)	Reason unknown
0x10 (0t16)	Normal call clearing
0x11 (0t17)	Endpoint not available
0x12 (0t18)	ISDN timer expired
0x15 (0t21)	Reason unknown
0x12 (0t22)	Destination address changed
0x1C (0t28)	Bad destination or access denied
0x1D (0t29)	Access denied
0x1F (0t31)	Reason unknown
0x22 (0t34)	Trunks unavailable
0x26 (0t38)	Temporary or facility failure
0x29 (0t41)	Temporary or facility failure
0x2A (0t42)	Resources unavailable
0x2C (0t44)	Resources unavailable
0x32 (0t50)	Access denied
0x34 (0t52)	Access denied
0x36 (0t54)	Access denied
0x3A (0t58)	Resources unavailable
0x41 (0t65)	Required capability not implemented
0x42 (0t66)	Required capability not implemented
0x45 (0t69)	Required capability not implemented
0x51 (0t81)	ISDN protocol error
0x52 (0t82)	Required capability not implemented
0x58 (0t88)	Incorrect destination number
0x60 (0t96)	ISDN protocol error
0x61 (0t97)	ISDN protocol error
0x62 (0t98)	ISDN protocol error
0x64 (0t100)	ISDN protocol error
0x66 (0t102)	ISDN timer expired
0x7f (0t127)	Reason unknown
0xC2 (0t194)	Ring no answer

Table continues...

Failure Causes	Description
0xC8 (0t200)	Hi and dry – no feedback detected
0xC9 (0t201)	Cascade link administered wrong
0xCA (0t202)	CPTR not available to detect failure

configuration

list configuration media-gateway

Use `list configuration media-gateway` to see all the assigned ports on the media modules for the specified gateway.

Syntax

```
list configuration media-gateway x
```

x Gateway number.

list configuration media-gateway field descriptions

Field	Description
Board Number	Physical location of the ports. Vn is the module number (V1–V4) or the virtual slots V8 or V9.
Board Type	Type of Avaya Media Module in the slot. If an administered Media Module is in conflict with the inserted Media Module, a pound sign (#) is displayed to the left of the Module Type field on the Media Gateway screen.
Code	Media Module code. Displays the value as Avaya Solutions Platform S8300 for an Avaya Solutions Platform S8300 ICC media module.
Vintage	Hardware and firmware vintage of the module. No code or vintage is listed for the virtual media modules in slots V8 and V9.
Assigned Ports	Status of ports associated with Media Module/slot. Blank means no assigned port.

list configuration software-versions

Use `list configuration software-versions` to display:

- software version numbers and compatibility indexes of the software load modules stored in system memory (RAM)
- the dates and times when translation and announcement data were last saved
- information about any software update files that have been applied to the system

Syntax

```
list configuration software-versions [ memory-resident ][ schedule ]
```

memory-resident Specifies display of RAM-resident files.

schedule Specify a time to run the command.

If the memory card contains a core dump file, fields for tape or memory card data display — **coredump**. When a core dump is present, all other files on the device are marked invalid.

If the memory card cannot be read at the time the command is entered, the relevant fields display — **no tape or memory card**. (This does not indicate that the system does not recognize the presence of the device.)

list configuration software-versions field descriptions

Field	Description
Software Version	Information related to the current software-load module stored in memory
Memory Resident	Version number of the RAM-resident load module
Disk Resident	The last date and time that translation data was saved to disk. This date is read from disk, and is blank if the disk is not installed.
Translation Data	Information related to the translation files as stored in memory and the disk.
Memory Resident	Date and time marked on the disk when translation data was last read into memory. This is stored in memory and is not modified by changes to translation data. Date invalid is displayed when the timestamp does not contain the expected information.
Disk Resident	The last date and time that translation data was saved to disk. This date is read from disk, and is blank if the disk is not installed.
Disk Second Copy	The last date and time that translation data was saved to disk. This date is read from the second copy of the file on the disk.

coverage path

list coverage path

Use **list coverage path** to see all the coverage paths that you have defined in the system along with a summary of the options defined.

Syntax

```
list coverage path [path x][to-path x][count n], [schedule]
```

craft2

enable craft2

Use **enable craft2** to create a second craft login assigned to Profile 3. Only one login in addition to craft can be enabled to use Profile 3 at a time.

To change the name of the second craft login, disable the current login (disable craft2) and enable a new one.

Only logins assigned to profiles 0 (init), 1 (inads), and 2 (dadmin) can run this command.

Syntax

```
enable craft2 [xyz]
```

xyz The name of the second craft login.

disable craft2

Use **disable craft2** to remove the second craft login assigned to Profile 3.

Only logins assigned to profiles 0 (init), 1 (inads), and 2 (dadmin) can run this command.

cti-link

busyout cti-link

Use **busyout cti-link** to busyout a specified endpoint for a link that is administered on the AESVCS Administration page of the IP Services screen. An ASAI adjunct link provides connectivity to an ASAI adjunct (for example, CentreVu CT), which is connected to an Ethernet LAN.

See **status link** for more details on links.

Syntax

```
busyout cti-link link
```

link Link number (1–8)

Feature interactions for busyout cti-link

- All ASAI service is disabled.
- A Warning alarm is generated even if more severe CTI link (for example, adj-ip) alarms are present.
- Periodic and scheduled tests continue to run. No alarms more severe than a Warning are generated until the CTI link is released from busyout.

- The release of CTI link from busyout retires all alarms.
- If a problem still exists, background maintenance generates new alarms within a few minutes.

change cti-link

Use the **change cti-link** command to modify the fields associated with the CTI link screen. You can use this command only when you enable the **ASAI Link Core Capabilities** field or the **Computer Telephony Adjunct Links** field on the System Parameters Customer Options screen.

Syntax

```
change cti-link n
```

n The Computer Telephony Integration (CTI) link number.

change cti-link field descriptions — page 1

Name	Description
COR	To specify the class of restriction number.
CTI Link	To specify the CTI link number.
Extension	To assign an extension to the CTI link.
Name	To assign a name to the CTI link.
Port	To assign a port number to CTI link. The following are the character specifications for ports: • 01 to 64: The first and the second characters represent the cabinet number. • A to E: The third character represents the carrier number. • 01 to 20: The fourth and the fifth characters represent the slot number. • 01 to 32: The sixth and the seventh characters represent the circuit number. If the Port field is set to X, no hardware is associated with the port.
Type	To specify the type of the CTI link. The available types of CTI links are: • ADJ-IP: Computer Telephony Adjunct links. • ASAI-IP: The associated adjunct controls all agent logins.
CRV Length	To specify the length of the Call Reference Value (CRV) for each interface. You cannot modify this field unless you busy out the CTI link.
Fixed TEI	To enable the fixed Terminal Endpoint Identifier (TEI) for an endpoint. Use TEI to use multiple physical phones on a single BRI interface. You cannot modify this field unless you busy out the CTI link.
MIM Support	To enable Management Information Message (MIM) for a CTI link.
XID	To enable Layer 2 XID testing capability for the system.

change cti-link field descriptions — page 2

Name	Description
Block CMS Move Agent Events	To enable the blocking of some event messages that are related to an agent move. The system does not send event messages related to the changes to the agent state, such as logout followed by login and return to a previous state. You cannot modify this field unless you busy out the CTI link.
Event Minimization	To enable event minimization for the CTI link. Event minimization limits the number of event reports that the system sends to an adjunct. Use this field when the system sends event reports on multiple associations, but the adjunct receives only a single report. The selection of the association on which the event is sent is based on association precedence as follows: • Active notification • Call control • Domain control You cannot modify this field unless you busy out the CTI link.
Send disconnect Event for Bridged Appearance	To specify if the system must send an event report when a bridged appearance disconnects. You cannot modify this field unless you busy out the CTI link.
Special Character for Restricted Number	To append the asterisk (*) to the digit string of the restricted number.
Two-Digit Aux Work Reason Codes	To enable sending of two-digit Aux Work Reason Codes over the CTI link. All messages that include Aux Work Reason Codes process codes from 1 to 99. You cannot modify this field unless you busy out the CTI link.

list cti-link

Use `list cti-link` to list the administered CTI links.

For more information about the links, see “status link”.

Syntax

```
list cti-link number [ count ]
```

number The cti-link number.

count The maximum number of links that the system must list.

CTI Links field descriptions

Name	Description
Link	The CTI Link number.
Ext	The extension associated with the CTI link.

Table continues...

Name	Description
Type	The CTI Link type: ASAI-IP or ADJ-IP.
Port	The port number.
Name	The node name for the link.
COR	The class of restriction number.

list usage cti-link

Use **list usage cti-link** to list vectors and IP services that use the specified CTI link, and indicate whether the link is currently used to monitor a hunt group as a controlling link, and/or through an event notification or domain control association.

CTI links are identified by the CTI link number in Communication Manager administration screens, not by extensions. For CTI links, use **list usage cti-link** instead of **list usage extension**.

Syntax

```
list usage cti-link link
```

link Link number (1–64).

release cti-link

Use **release cti-link** to release a busied-out endpoint for a link that is administered on the AESVCS Administration page of the IP Services screen. An ASAI adjunct link provides connectivity to an ASAI adjunct (for example, CentreVu CT), which is connected to an Ethernet LAN.

See **status link** for more details on links. For more information, see Busyout and Release Commands.

Syntax

```
release cti-link link#
```

link# Link number.

test cti-link

Use **test cti-link** to test the specified CTI link.

For more information on the CTI link, see **status firmware download**. See **status link** for more details on links.

Syntax

```
test cti-link n [ short | long ][ repeat # | clear ]
```

n Link number.

- short** Execute a series of nondestructive diagnostic tests.
- long** Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
- repeat #** (Optional) The number of times to repeat the command. The default is 1.
- clear** Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

customer-alarm

test customer-alarm

Use **test customer-alarm** to test the customer provided alarm device by closing the alarm relay contact on the PN and EPN maintenance media module in a specified cabinet, including the TN2312BP, for 1 minute and then restoring the alarm relay contact to its current state. Verify the test by checking the customer alarm attached to the specified media module.

Syntax

```
test customer-alarm UU C [ short | long ][ repeat # | clear ][ schedule ]
```

location UU C Extension of the data module or data channel to be tested, per dial-plan.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a start time for the command.

Example

```
test customer-alarm
test customer-alarm 02 r 2
test customer-alarm 01b r 25
test customer-alarm 2a
test customer-alarm 2a sh
test customer-alarm 3 c
```

data-module

busyout data-module

Use **busyout data-module** to put a data module in a maintenance busy state, even an uninstalled data module.

Use **release data-module** to return the specified data module or data channel into service.

Syntax

```
busyout data-module extension
```

extension Extension number per dial plan.

Use **list data-module** to see a list of every data module administered on the system, including the extension, port, type, and other data for each data module. The maintenance object name for each data module in the Type field is:

Type of data module	Maintenance Object
adm-t	BRI-SET
announcement	DAT-LINE
dtdm	DIG-LINE
pdm	PDMODULE
system-port	DAT-LINE

Example

```
busyout data-module 31300
```

release data-module

Use **release data-module** module to activate the specified data module or data channel. Hardware tests are executed to verify that the equipment is functioning.

For more information, see Busyout and Release Commands.

Syntax

```
release data-module extension
```

extension Extension number associated with data module or data channel.

status data-module

Use **status data-module** to see the internal software states of a specified data-module port. This information helps diagnose and locate facilities to which the data module is connected.

Syntax

```
status data-module extension
```

extension Data module extension.

status data-module field descriptions

Field	Description
Data Ext/Sta Ext for Stn DM	Data module extension number. For DTDMs, the connected station extension is shown.
Port/ChannelNumber	Location of the port connected to the data module. For data channels, the channel number is shown.
Service State	The operational state of the data-module: • in-service/idle — data module is connected but idle. • in-service/active — data module is connected and in use. • out-of-service — data module has been removed from service • disconnected — data module no longer appears to be present

If the specified port is administered as a system port, the following fields will be for more information.

Field	Description
CF Destination Ext	The call-forwarding destination, if any, of the station.
Maintenance Busy	Whether the object is busied out for testing.
Connected Ports	Locations of ports to which the data module is currently connected.
Service State	The operational state of the associated port.

test data-module

Use **test data-module** to perform hardware diagnostic tests on a data module or a data channel. Test results are determined by the interface to the digital switch-data line port, digital line port, or network control data channel.

Syntax

```
test data-module extension [ short | long ][ repeat # | clear ][ schedule ]
```

extension Extension of the data module to be tested (per dial-plan).

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a start time for the command.

Example

```
test data-module 30000 1
test data-module 30000
test data-module 32000 sh r 2
test data-module 33000 1 r 25
test data-module 30000 c
```

digit-string

list usage digit-string

Use **list usage digit-string** to see all the vectors, vector tables, and Best Service Routing (BSR) plans that use a specific dial string.

Syntax

```
list usage digit-string string (0-9 +?*\#~prwWms), [schedule]
```

directory

list directory

Use **list directory** to list every file in the specified board's memory file system.

Forward slash (/) is the default path for listing files in the root directory. To list the files in a directory other than the **/root** directory, specify the complete path.

Syntax

```
list directory board location | path
```

board File location or directory name.

path Path to the directory.

Example

```
list directory board 1c12
```

list directory source

Syntax

```
list directory source [source ] location [gateway] OR [media-server] [directory path name]
```

location	location of the directory
slot	slot number
gateway	gateway number that has value ranging from 1 — 250

Use the `list directory source` announcement files contained on a media gateway, or a media server.

disabled-MOs

list disabled-MOs

Use `list disabled-mos` to list the maintenance objects that have been disabled with `disable mo`, `disable all`, or `disable mo-all`, as well as whether or not the command has been run.

Use `display disabled-tests` for numbers of tests that have been disabled.

Syntax

```
list disabled-mos [ schedule ]
```

schedule Specify a time to run the command.

disabled-tests

display disabled-tests

Use `display disabled-tests` to display the list of maintenance tests that have been disabled.

The disabled tests are not available for background or demand testing.

ds1-facility

busyout ds1-facility

Use **busyout ds1-facility** to put a DS1 facility of a DS1C complex into a maintenance busy state. Each DS1C complex uses from 1 to 4 DS1 facilities.

- The packet facility carries the control channel for every facility in the complex, all packet traffic, and some circuit connections.
- The other facilities carry circuit connections only.

Syntax

```
busyout ds1-facility location [ override ]
```

location Location of the ds1-facility.

override All packet and circuit traffic on the packet facility is switched to another facility, and all traffic that was on the destination facility before the switch is dropped.

Whenever the media module resets, the packet facility is set on the **a** facility. If system software detects a problem with this facility, it switches the packet and control traffic to another facility. The **busyout** command is not allowed on the packet facility without **override**. When **override** is used, all packet and circuit traffic on the packet facility is switched to one of the other three facilities, and all traffic that was on the destination facility before the switch is dropped.

There is no way to tell which facility is carrying the packet and control traffic without attempting to busy it out. If there is only one facility left in service on the media module, it cannot be busied out. In this case, the media module must be busied out.

Caution:

Busying out a non-packet facility disrupts all traffic carried on that facility. Using **override** to busy the packet facility disrupts all traffic on the facility to which the packet and control traffic is moved. This facility cannot be determined in advance.

On critical-reliability systems (duplicated PNC) a facility on the active PNC cannot be busied out. Use **busyout pnc** to busyout a standby PNC, and then busyout a facility on the standby PNC.

Example

```
busyout ds1-facility 6b
```

test ds1-facility

Use **test ds1-facility** to perform a series of tests on the specified facility. Each test runs diagnostics on the facility and returns results of the test along with any possible error codes. The long test is destructive and is not enabled unless the facility has been busied out.

Syntax

```
test ds1-facility location [ short | long | external loopback ] [ repeat # ] [ schedule ]
```

location	Location of the DS1 Converter media module.
short	Run a series of nondestructive diagnostic tests.
long	Run a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
external loopback	This initiates a destructive test that sends a test pattern to an external device and returns it for comparison to the original. Configure the external device to loop back the signal. For more information, see <i>Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers</i>
repeat #	Number of times to repeat the test.
schedule	Specify a start time for the command.

Example

```
test ds1-facility 1v902
```

ds1-loop

test ds1-loop

Based on the command parameter, a long-duration loopback/span test or series of short-duration loopback tests will be executed.

Long-duration loopback tests run for an extended period of time until the system technician terminates it. Short-duration loopback tests return the result of the test to the screen when finished executing. Use **list measurements ds1 summary** to monitor the status of a long-duration loopback/span test.

If the [inject-single-bit-error] parameter is used, but no CPE loopback jack, far-end CSU, or one-way span test is active on the DS1 media module, the following error message displays:

Parameter valid if a loopback/span test is active on the DS1.

Syntax

```
test ds1-loop location [ cpe-loopback-jack-test-begin [ number-of-bitsbit-pattern ]
| far-csu-loopback-test-begin | one-way-span-test-begin | end-loopback/span-test
| inject-single-bit-error | ds1/csu-loopback-tests ]
```

location	Represents the physical position of the board to be tested. It is represented by media gateway, slot position.
cpe-loopback-jack-test-begin	For DS1 boards, this causes a long-duration loopback test to be setup through the CPE (customer-premises equipment) loopback jack. The command enables you to specify a loop-up code for the CPE loopback

<i>number-of-bits bit-pattern</i>	jack if it differs from the default of 0x47F. Specify the number-of-bits in the loop-up code as well as the actual bit-pattern (in hexadecimal). The test aborts if the busyout command has not been set
far-csu-loopback-test-begin	For DS1 boards, this causes a long-duration loopback test to be setup through the far-end CSU (channel service unit).
one-way-span-test-begin	For DS1 boards, this begins execution of a long-duration one-way span test.
end-loopback/span-test	For DS1 boards, this parameter terminates long-duration one-way span and loopback testing.
inject-single-bit-error	For DS1 boards, this parameter causes a single bit error to be sent within an active framed 3-in-24 test pattern used in long-duration loopback and span testing.
ds1/csu-loopback-tests	For DS1 boards, this parameter executes the following loopback tests: DS1 Board LoopBack, CSU Module Equipment LoopBack, and CSU Module Repeater LoopBack. These tests are performed sequentially for a short duration each, and individual PASS/FAIL/ABORT test results are reported following each test.

Feature Interactions for test ds1-loop

Loopback or span tests are enabled on DS1 boards that are busied out.

One of the CPE loopback jack, far-end CSU, one-way span, or DS1/CSU loopback tests may be active at any given time on a DS1 span.

Example

```
test ds1-loop 1v2
```

eda-external-device-alm

list eda-external-device-alm

For detailed information regarding **list eda-external-device-alm**, refer to 'EXT-DEV' in *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers*

test eda-external-device-alm

Use **test eda-external-device-alm** to perform hardware diagnostic tests on the alarm port for either an individual device, or every external device.

If `all` is entered, `test eda-external-device-alm` performs a hardware diagnostic test on every administered external device's alarm port. If an administered external device's alarm port is entered, this command performs a hardware diagnostic test on that port.

The test **passes** if the external device is not reporting an external device alarm and **fails** if the external device is reporting an external device alarm. If the technician specifies a port, it must be administered as an external device's alarm port either on a maintenance board or on an analog line board.

errors

clear errors

Use `clear errors` to move every error and resolved alarm to the cleared errors list, to make room for new incoming error messages that might otherwise be dropped. Clear errors does not clear active alarms from the alarm log. Cleared error entries are the first entries overwritten when additional room is needed to log new entries.

Use `display errors clear` to list the cleared errors.

Caution:

Use `clear errors` with care. Cleared data is lost when the logs fill up.

Syntax

```
clear errors
```

display errors

Use `display errors` to select the errors that appear on the hardware error report.

Errors can result from in-line firmware errors, periodic tests, failures detected while executing a test command, software inconsistency, or a data audit discrepancy. The error log is restricted in size. A new entry overwrites the oldest unalarmed entry. The overwritten entry must be at least six minutes old, or the new entry is dropped.

Syntax

```
display errors [ high-resolution ] [ schedule ]
```

high-resolution

Include high resolution time stamps for the first occurrence and last occurrence of the error. This shows seconds and a sequence count within a second. The sequence count starts over for each second.

See Error Log Report High Resolution.

schedule

Specify a time to run the command.

Help messages

- When the first page of a multiple page list of alarms/errors or after the **Prev Page** key is pressed:

Press CANCEL to abort or NEXT PAGE for next page

- After the **Next Page** key is pressed and there are more pages of alarms/errors to be displayed:

Press CANCEL to abort, NEXT PAGE for next page, PREV PAGE for previous page.

- After the **Next Page** key is pressed and there are no more alarms/errors to be displayed:

Press CANCEL to abort, NEXT PAGE to complete, PREV PAGE for previous page.

System Reboots and Error and Alarm logs

Avaya Aura® Communication Manager software attempts to save the error and alarm logs to the disk when any of the following events take place:

- The save translation command is executed.
- Translations are saved as part of scheduled maintenance (as administered on the Maintenance-Related System Parameters screen).
- A demand or software-escalated system reboot takes place.

Whenever the Communication Manager software reloads, the error log is restored from the disk. Since the logs are saved to the disk, the versions restored at reload time may not be current. This occurs when either:

- The attempt to save at reload did not succeed.
- The server that is active coming out of reload is not the same one to which the logs were last saved.

In such a case, the logs will not show the errors and alarms that have been logged since the last time a save was made to the server that became active with the reboot. When looking at errors that precede the last reload, look for indications preceding the reload to determine whether the logs restored at reboot are complete. System resets less severe than a reload rarely affect the error and alarm logs.

Note:

If there are system errors in the error log, use **display initcauses** for more information. Information that could not be logged during a system reset may be found here.

display errors input field descriptions

The display errors input screen specifies which errors display on the report. When every selection has been made, press **ENTER**. If no selections are made or if the schedule option is specified, the system displays every error from the last day that are associated with active alarms.

Field	Description
Error Type	The report can be restricted to specific error codes. Default is every error.

Table continues...

Field	Description
Error List	The report can be restricted to errors from one of three lists described below: active-alarms, errors, or cleared-errors. Default is active-alarms.
Interval	Specifies error records for the last month, hour, day, week, or all errors (m, h, d, w, a). The default is all.
From	Specifies error records starting from the time specified by (month/day/hour/minute). If no From date is entered, errors from the earliest record in the log are displayed.
To	Specifies every error record up to the time specified by mm/dd/hh/mm . If no To date is entered, every error up to the current date appears.
Equipment Type	To limit the report to a specific group of components, enter the location of a type of equipment in one of the following fields. If no entry is made, errors for the entire system are displayed. • Gateway: Enter the gateway number. • Board: Enter the media gateway slot address of the media module (for example, 41v4). If the cabinet number is omitted, it defaults to 1. • Port: Enter the media gateway slot circuit address of the media module (for example, 1v408). • Category: Enter a category to restrict the report to maintenance objects in a specific category. The HELP key displays a list of categories. • Extension: Enter the extension number of a port. • Trunk (group/member): Enter a trunk-group number, or a trunk-group and member number separated by a slash (for example, 78 or 78/1).

display errors output field descriptions

Field	Description
Port	The physical location of the alarmed object. • For media module based MOs, the location is <code>media-gateway-[slot]-[circuit]</code>. • For MG based objects, such as TDM-BUS, the location displays as 1v4.
Maintenance Name	The name of the MO as it appears in the alarm and error logs.

Table continues...

Field	Description
	The alternate name depends upon the type of the object. For example: • Station MO — alternate name is <i>nnnnn</i> (extension) • Trunk MO — alternate name is <i>nn/n</i> (trunk-group number/member number) • Personal CO line MO — alternate name is <i>P/xx</i> (P/personal CO line group number)
Error Type	Numerical error code that identifies the type of problem. The meanings of these codes are explained under the name of the MO in the <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> .
Aux Data	Additional numerical information about the error type. Only the most recent auxiliary data for each error type appears.
	First line: Month, day, hour, and minute (and second, if the high-resolution command-line option is used) that the error was first recorded. Second line: The month, day, hour, and minute (and second, if the high-resolution command-line option is used) of the most recent error. If the system is unable to retrieve the time of day when the error occurred, a dummy date will be stamped in the log so as to distinguish it from reliable data. It appears as 00/00/01:07.
Seq Cnt	Sequence Count. These numbers give the order in which the errors were logged. Each sequence covers a period of one second. Sequence numbers are assigned to the first and last occurrences of a given error within the one second period given in the time stamp. There may be gaps in the sequence numbers within a given second because the last occurrence of an error may replace an existing entry and because sequence numbers are also assigned to software events not shown in the hardware error log. This information appears when the high-resolution option is specified on the command line.
Err Cnt	The total number of times that the error type has occurred. The maximum entry is 999.
Err Rt	Average hourly rate at which the error has occurred from the first occurrence to the present. The maximum entry is 999.
Rt/Hr	An approximation of the rate at which this error occurred in the last hour. The maximum entry displayed is 999.

Table continues...

Field	Description
Al St	Alarm Status. A character indicating the status of this MO in the error and alarm logs. • a — active alarm entry • r — resolved alarm entry • c — resolved alarm entry due to long clear option of test • s — resolved alarm entry due to a software-requested (non-demand) system restart • t — resolved alarm entry due to a technician-requested system restart • n — not alarmed
Ac	y/n — Whether the maintenance object is still under active consideration by the maintenance subsystem.

ess

disable ess

Use **disable ess** to disable a Survivable Core Server or main server from connecting to Procr. The **disable ess cluster n** command allows a Survivable Core Server cluster to be disabled (taken out of service).

Communication Manager preserves the enabled/disabled status of Survivable Core Servers and Main servers across server shutdown and restart.

A disabled Survivable Core Server remains registered and receives file sync translation updates.

Execute **disable ess** from either a main or Survivable Core Server. A Survivable Core Server may disable only its own cluster ID. When **disable ess** is run from the main server, any and all clusters may be disabled including the main server itself.

Caution:

Use caution when using **disable ess all**. Since the main typically controls Procr and a cluster may not be disabled when it controls Procr, it is generally safe to use **disable ess cluster all** to disable only the Survivable Core Server clusters.

Be aware that if the main is not controlling Procr and **disable ess cluster all** is used, the main will also be disabled.

When a Survivable Core Server is disabled, it reboots. After the reboot, the server is in the Survivable Core Server disabled state and will not connect to any Procr. If the cluster involves duplicated servers, this process may take slightly longer while the active server informs the

standby of its new Survivable Core Server disabled state. When the system duplicates Survivable Core Server, the standby server also gets updated and rebooted.

When a valid **disable ess** command is run from a Survivable Core Server:

- The server reboots.
- No SAT screen is displayed.
- Once the server has rebooted, use **status ess cluster** to confirm that the disable operation succeeded.

When a valid **disable ess** command is run from a main server:

- TEST RESULTS screen appears
- If the **disable ess** command specifies the cluster ID of the main itself, the server reboots and no SAT screen is displayed.
- Use **status ess cluster** to confirm that the disable operation succeeded.

Syntax

```
disable ess[ all | cluster n]
```

all Disables all Survivable Core Servers

cluster n Number (1–999) of the cluster ID for the target Survivable Core Server or main server.

Error codes

The following table describes the error codes that may be returned from the **disable/enable ess** commands:

Error Code	Description
1991	Requested Survivable Core Server cluster is not administered
1992	Requested Survivable Core Server cluster is not registered
1993	Requested Survivable Core Server is controlling an Procr PN
1994	A Survivable Core Server cluster may not enable/disable other clusters.
2500	Internal operation failed

Example

```
disable ess cluster 7
disable ess all
```

enable ess

Use **enable ess** to enable a Survivable Core Server. Once a Survivable Core Server cluster is enabled, it attempts to connect to Procr.

Use **enable ess** from either a main or a Survivable Core Server. A Survivable Core Server may enable only its own cluster ID. When **enable ess** is run from the main server, any and all cluster

IDs may be enabled including the main itself. Care should be taken when using **enable ess all**.

When a Survivable Core Server is enabled, it removes its translations and reboots. The TEST RESULTS screen is not displayed.

When a main server is enabled, it reboots but does not remove its translations. A TEST RESULTS screen is displayed. The exception is when the **enable ess** cluster command specifies the cluster ID of the main itself. In that case, the server reboots and no screen is displayed.

After the reboot, the server is in the Survivable Core Server enabled state and will attempt to connect to Procr. If the cluster involves duplicated servers, this process may take slightly longer while the active server informs the standby of its new Survivable Core Server enabled state.

Syntax

```
enable ess[ all | cluster n ]
```

all Enable all Survivable Core Servers

cluster n Number (1–999) of the cluster ID for the target Survivable Core Server or main server.

See 'Error Codes' for a description of possible error codes returned from the **enable ess** command.

status ess clusters

Use **status ess clusters** to see the state of the main server and all administered Survivable Core Servers. Under normal conditions, with full network connectivity, all Survivable Core Servers should register with the main.

Syntax

```
status ess cluster
```

When **status ess clusters** is run on a main server (Cluster ID 1), the Main server:

- knows the identities of all of its associated Survivable Core Server from the translations input to the main server.
- knows the state of all of the Survivable Core Servers that have successfully registered with it.
- shows its own state.

status ess clusters field descriptions

Note:

The field definitions are the same whether the **status ess** command is executed on a main server or Survivable Core Server.

Field	Description
Cluster ID (title line)	Cluster Identifier (1–999) of the server where status ess was run. In a duplex server environment, both the active and the standby server have the same cluster ID. Cluster ID is initially obtained from the license file (where it is called the Module ID or MID). Once save translation is executed, the cluster ID is saved in translations.
Cluster ID (detail line)	Cluster Identifier (1–999) of a server who's state is known to the server where status ess was run. The detail lines are shown in cluster ID order. When status ess is issued on a main server, there is one detail line for the main server itself and a detail line for every Survivable Core Server that is registered with the main server. When status ess is issued on a Survivable Core Server there is only one detail line since a Survivable Core Server only knows its own state.
Enabled	The Survivable Core Server enabled or disabled state of the server. • y — enabled. This server will connect to administered Procr. • n — disabled. This server will not connect to administered Procr. • unknown — the main server does not yet know the maintenance state of the Survivable Core Server. This may be because: - the Survivable Core Server is not registered with the main server - the Survivable Core Server has not yet acknowledged a maintenance state change request from the Main via an enable ess or disable ess command.
Active Server ID	The server identifier of the active server for each cluster, Survivable Core Server or main server (1–99). This is the Server ID that was entered for this server in the Set Server Identities page during configuration. • If the server is a simplex configuration, there is only one Server Identifier. • If the server is a duplex configurations, the A and B servers each have unique server identifiers. Because in a duplex configuration only the active server registers with the Main, only its server identifier is displayed. Only server IDs for registered Survivable Core Servers are displayed.
Registered	The registration state of the server. • y — registered • n — not registered The main server does not register with itself, but always displays its own registration as y.

Table continues...

Field	Description
Translations Updated	For a Survivable Core Server: The time and date of the latest translation update reported by the Survivable Core Server to the Main server over the registration link. For a main server (Cluster ID 1): The time and date of the latest successful save translation command of any kind.  Note: For a main server, this time stamp may be later than those shown for Survivable Core Servers. A save translation on the Main updates its time stamp. A save translation [ess all] updates the Survivable Core Server translations and time stamp.
Software Version	The software version of Communication Manager running on the server. For a Survivable Core Server, this is reported to the Main server over the registration link.

ethernet-options

get ethernet-options

Use **get ethernet-options** to generate a report about a specific Ethernet connection.

Syntax

```
get ethernet-options location
```

location The physical location of the media module.

get ethernet-options field descriptions

Field	Description
Auto Negotiation	Enter y for the system to automatically negotiate the highest possible network speed. Enter n to manually assign the Speed and Duplex fields.
Speed	10 Mbps 100 Mbps N/A (not available)
Duplex	Half Full N/A (not available)

Table continues...

Field	Description
Link Integrity	Active Inactive

list ethernet-options

Use `list ethernet-options` to see locations and settings for ethernet-enabled ports.

Syntax

```
list ethernet-options
```

set ethernet-options

Use `set ethernet-options` manually or automatically set the Ethernet connection parameters.

* Note:

The Ethernet port must be administered and busied out before you can issue `set ethernet-options`.

Syntax

```
set ethernet-options location
```

location The physical location of the media module.

set ethernet-options field descriptions

Field	Description
	y — the system automatically negotiates the highest possible network speed. n — you must manually assign the Speed and Duplex fields. If n, the Speed and Duplex fields do not appear.
Speed	10 Mbps/100 Mbps Appears when Auto Negotiation is y.
Duplex	Half/Full Appears when Auto Negotiation is y.

events

display events

Use **display events** to view the vector event logs. Vector event occurs when an unexpected vector-routing of the call takes place due to resource exhaustion or faulty vector programming. For example, route-step failures are typically due to the programming of an invalid extension. These types of failures are not due to faulty hardware or system software error and do not constitute incorrect feature operation.

An IP event occurs when an IP endpoint registration is denied.

You can see the detailed information about denial events on the System Logs page. Use **display events** to diagnose and correct IP registration denials, and vectoring problems due to resource exhaustion or faulty vector programming.

For more information about vectoring, see *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*.

Syntax

```
display events
```

display events field descriptions

Use the Event Report page to generate event report for a specific type of events and time period. You can specify the desired parameters and press **ENTER**.

Name	Description
Category	Specify the type of event to generate event report. The valid values are <code>all</code> , <code>contact-cl</code> , <code>data-error</code> , <code>denial</code> , <code>feat_event</code> , <code>meetme</code> , and <code>vector</code> .
Report Period	Select the time period for the vector events you want to see. If fields are blank, every recorded vector event is reported.
Interval	The time period for which events are reported: <code>m</code> (month), <code>d</code> (day), <code>h</code> (hour), <code>m</code> (minute), or <code>a</code> (all). Specify the date and time of day when you want to start and end the search. The following information message displays on the display events screen: IPv6 addresses are truncated, see System Logs web page for complete address.
SEARCH OPTIONS	
Vector Number	Specify a specific vector number to include in the report. The range for the vector number is 1 through 8000. If blank, events for every vector are reported. If the Category field is <code>meetme</code>, you can leave this field blank.
Event Type	Specify a event type to include in the report. The range for the vector number is 0 through 9999. If blank, all event types are reported.
Extension	Specify a specific extension or VDN to report on. If blank, all events for all extensions are reported.

Event Report field descriptions

For information about specific events, see *Avaya Aura® Communication Manager Denial Events*.

Name	Description
Event Type	Displays a unique number that identifies the type of event that occurred.
Event Description	Displays a 25-character string describing the event.
Event Data 1	Displays the data in one of the following format: • <i><number1>/<number2></i>, for example, 12/5, where, <i><number1></i> is the vector number associated with the vector event and <i><number2></i> is the step number associated with the vector event. • <i>Split<number></i>, for example, split 89, where <i><number></i> is the split number associated with the vector event. • For Meet-me Conference events, this is the port ID of the user associated with the event.
Event Data 2	Displays one of the following data: • The IP address of the station that is attempting to register. If more than two events with an identical identifier occur at the same time, the events are caused by the same call. • For Meet-me Conference events, this is the VDN of the Meet-me Conference used during the event.
First Occur	Displays the date and time when this event first occurred.
Last Occur	Displays the date and time when this event last occurred.
Evnt Cnt	Displays the number of occurrences of the event between the First Occur and Last Occur times. The system displays up to 255 events.

extended-user-profile

change extended-user-profile

Use **change extended-user-profile** to administer detailed access permissions for the vector and station forms.

Syntax

```
change extended-user-profile n
```

n The number of the extended profile to change.

change extended-user-profile field descriptions

Field	Description
User Profile Name	The name of the standard profile for which this is the extended profile. Display only.
Form	Category and type of form (SAT screen) that are administered for extended permissions. Display only.
Allow Only	Specify access to all, certain, or no instances of the form. • all = access to all instances of the form • blank = no access to the form List specific instances in a valid format as: • list separated by commas (1,2,3) • one or multiple pair separated by a dash (1000–2000). As many combinations can be administered as can fit in the field.

display extended-user-profile

Use **display extended-user-profile** to see the access permissions on an existing Extended User Profile.

Syntax

```
display extended-user-profile n
```

n Number of the extended user-profile to display.

See **change extended-user-profile** for screen and field descriptions.

extension-type

list extension-type

Use **list extension-type** to see the type of stations associated with specific extensions.

Syntax

```
list extension-type [ n | partial-string * | all | type ]
```

n Extension number.

partial-string * List all extensions that begin with the partial string, as in searching for all numbers that begin with a specific area code.

all List all extensions.

type Refer SAT command Help to see the list extension-type type entries.

failed-ip-network-region

display failed-ip-network-region

Use **display failed-ip-network-region** to see a list of the worst, first 100 network regions with broken connectivity rank ordered by the worst to least worst.

To troubleshoot broken connectivity, see **status ip-network-region** and **test failed-ip-network-region**.

Syntax

```
display failed-ip-network-region
```

test failed-ip-network-region

Use **test failed-ip-network-region** to initiate a real-time **ping** test for failed network-region connections.

The default is that all connections that failed the last background maintenance ping test are tested. If network region *x* is specified, then just failed connections from region *x* are tested. If a previously failed connection passes the ping test, then the associated minor alarm is cleared.

To troubleshoot broken connectivity, also see **display failed-ip-network-region** and **change ip-network-region**.

Syntax

```
test failed-ip-network-region [ all | x ]
```

all Test all failed IP network regions.

x Test the specified failed IP network region.

test failed-ip-network-region field descriptions

Field	Description
Region	Network region that had a connection failure to Dest. Region .
Dest. Region	A network region to which Region is connected, where the connection between the two regions is previously failed the ping test.
Maintenance Name	The name of the MO as it appears in the alarm and error logs.
Test No.	Test Number used to run ping test.

Table continues...

Field	Description
Result	Result of ping test — PASS or FAIL. If test failed, follow troubleshooting procedures in 'NR-CONN (Network-Region Connect)', <i>Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers</i> .
Error Code	ping test error code

file

remove file

Use **remove file** to request the board location to remove the file given by path. If the file does not exist on the source board's filesystem, an error message – `file not found` – appears on the SAT.

To remove a file in a subdirectory, specify the entire path starting at `/`.

Syntax

```
remove file [ gateway location ] [ filename ]
```

gateway location Location of the gateway.

filename Name of the file to remove using the entire path starting with `/`.

filexfer

enable filexfer

Use **enable filexfer** to enable FTP remote access protocols through login/password authentication on Media Gateways Integrated VAL board.

Syntax

```
enable filexfer location
```

location Location of the media module.

enable filexfer enables the Media Gateways Integrated VAL board as FTP servers (not client).

Note:

The gateway provides an SCP/HTTPS client to transfer announcement files securely.

enable filexfer field descriptions

Field	Description
Login	3–6 alphabetic characters
Password	7–12 alpha-numeric characters containing at least one letter and one number.
Renter Password	Re-enter the password.
Secure	n — enable FTP
Board Address	Location of the media module.

firmware download**change firmware download**

For information regarding firmware station downloads, see *Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers*.

hardware-group**cancel hardware-group**

Use **cancel hardware-group** to temporarily or permanently abort the execution of **test hardware-group**. Use **resume hardware-group**, to resume the same test, or start another test with **test hardware-group**. Press **CANCEL** to cancel a hardware group test executing in the foreground.

The status of a canceled **test hardware-group** is displayed as canceled on the status hardware-group screen.

When a hardware group test is executing in the foreground with the continuously option and **CANCEL** is pressed or **cancel hardware-group** is entered, the hardware group test is canceled, and for security reasons the MT running the hardware group test is logged off. Use **resume hardware-group** to restart the canceled hardware-group test after logging back on.

Syntax

```
cancel hardware-group
```

Scheduled and Periodic Maintenance

When **test hardware-group** is entered, all activity related to scheduled background maintenance, periodic background maintenance, and data audits is suspended for the duration of the execution of **test hardware-group**. All activity related to scheduled background

maintenance, periodic background maintenance, and data audits will restart if **test hardware-group** is canceled.

All-Ports Option

When **test hardware-group all-ports** is canceled, the internally generated port translations for ports that are otherwise untranslated are removed. If **resume hardware-group** is then entered, only customer-administered ports will subsequently be tested. Resume does not reinstate the port translations that were removed by the cancel.

If **test hardware-group** running in the foreground is successfully canceled with **cancel hardware-group** from another terminal, the following message is displayed on the terminal where the hardware group command was executing: Hardware-group command aborted with cancel; command entered from another terminal.

resume hardware-group

Use **resume hardware-group** to restart a hardware group test at the point where it was canceled. This capability is not available if another hardware group test has been started.

Halt a hardware group test (**test hardware-group**) temporarily or permanently with **cancel hardware-group** for a background test, or by pressing **CANCEL** for a foreground test. Use **status hardware-group** to see the status of a hardware group test.

When **test hardware-group all-ports** is canceled, the internally generated port translations for previously untranslated ports are removed. If **resume hardware-group** is then entered, only customer-administered ports are tested. Resume does not reinstate the port translations that were removed by cancellation of **test hardware-group all-ports**.

Syntax

```
resume hardware-group
```

When a test that was executing in the background is resumed, a success message is displayed. When a test that was executing in the foreground is resumed, test results are displayed.

status hardware-group

Use **status hardware-group** to see summary information about the active or last hardware group tests.

The information includes the number and percentage of maintenance objects tested, the percentage of tests passed/failed/aborted, the time elapsed since initiating the hardware group test, the specific hardware group test command (see **test ipserver-interface**) initiated, and the state (active/canceled/complete) of the hardware group test.

Syntax

```
status hardware-group
```

status hardware-group field descriptions

Field	Description
Hardware Group Command State	The state of a hardware-group command: • active — testing is in progress • canceled — testing has been canceled • complete — the command has completed and there is no testing going on.
Number of MOs Tested	The number of MOs in the specified group (see test ipserver-interface) that have had been tested by current hardware-group. This includes every MO that either was actually tested or was aborted due to resource contention.
Total Number of MOs to be Tested	The total number of MOs in the group that was specified in test hardware-group .
Percent Complete	A ratio of the number of MOs completed and the total number of MOs to test in the command.
Elapsed Test Time	The duration of the hardware-group test. If a test was canceled and then restarted this time excludes the cancel period. If hardware-group has finished it indicates the length of time it took to complete the command. The time is displayed as <i>HH:MM:SS</i> where <i>HH</i> is hours, <i>MM</i> is minutes, and <i>SS</i> is seconds.
Repetition Number	The number of iterations that have been completed corresponding to the 'repeat' or the 'continuously' option.
Percentage of Tests Passed	The percentage of tests that passed.
Percentage of Tests Failed	The percentage of tests that failed.
Percentage of Tests Aborted	The percentage of tests that were aborted.
Command	The hardware-group action/object and qualifiers that were entered.
Test Sequence	short/long.
Test Repetition	Displays either continuously or the keyword repeat along with the repeat value entered.
Output Options	Displays the selections that were chosen on the input screen: auto-page, background, or failures.
Hardware Options	Displays the selections that were chosen on the input screen (all-ports).

health

monitor health

Use **monitor health** to show the current system alarm summary, maintenance busy summary, user summary, critical system status, and cabinet status, that are updated every minute.

See the same information with **status health**. Press **CANCEL** to end **monitor health** and drop the management terminal login.

Syntax

```
monitor health
```

monitor health feature interaction

If standby Emergency Transfer Select Switches change and handshakes are down, the displayed Emerg Trans field is incorrect until handshake re-initializes. When monitor health terminates, users are logged off of the system.

status health

Use **status health** to list various performance measurements in the system. Measurements include the current system alarm summary, maintenance busy summary, user summary, critical system status, and cabinet status.

Syntax

```
status health
```

status health field descriptions

Field	Description
St	Percentage of CPU time dedicated to high priority items such as the operating system, rounded to the nearest whole number
Sm	Percentage of CPU time dedicated to system management or periodic and scheduled maintenance, rounded to the nearest whole number. If a large amount of periodic or scheduled maintenance testing is being performed, this number can be high without affecting service.
Cp	Percentage of CPU time dedicated to call processing, rounded to the nearest whole number. Call processing has priority over system management and will draw occupancy from the SM or IDLE categories.
Idl	Percentage of CPU time idle and available for use, rounded to the nearest whole number.
Maj	Number of major alarms logged.
Min	Number of minor alarms logged.

Table continues...

Field	Description
Wrn	Number of warning alarms logged.
Logins	Number of current users.
Trk	Number of maintenance busied-out trunks.
Stn	Number of maintenance busied-out stations.
Oth	Number of busied-out maintenance objects, excluding trunks and stations.
Cab	Cabinet number. Use list cabinet to relate cabinet numbers to port network numbers.
EmTr	Emergency Transfer shows the current setting of the switches on the PN's Maintenance media modules that control Emergency Transfer. See 'EMG-XFER (Emergency Transfer)' in the <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> . The following states are available: • auto- — Emergency Transfer is under system control and is not currently activated (normal operating state). • auto+ — Emergency Transfer is under system control and is in effect. • on — Emergency Transfer has been manually activated. This setting is in effect during an emergency. • off — Emergency Transfer is manually prevented from occurring. This setting is in effect when a technician is on site. • n.a. — The setting of the switch in this PN is not available to the switch. The Expansion Archangel Link (EAL) may be down. • NoEqp — The cabinet has media modules that do not support Emergency Transfer.
Maj, Min, Wrn	Number of major, minor or warning alarms associated with the cabinet. An asterisk indicates that the number exceeds 99 or 999.

history

list history

Use **list history** with no options to generate a log of the most recently completed data-affecting administration and maintenance commands. This includes the history of ACTR moves, which can be used to track moves and help reduce fraud.

Syntax

```
list history [ date | time | login x | action x | object x | qualifier x ][ schedule ]
```

date	MM or MM/DD
time	HH or HH:MM
login x	Login ID
action x	Action performed
object x	Object acted upon
qualifier x	Extension, etc.
schedule	Specify a time to run the command.

list history feature interactions

The translation log is written to memory as translation data when **save translation** is executed. The translation data is time stamped when saved. This time stamp is noted when translation is loaded from memory and included in every recent change history report.

When a user requests a recent change history report, there could be other users concurrently issuing data commands and altering the contents of the transaction log. Therefore, if the user pages the entire way through the report, the oldest entries in the transaction log (maximum 250 commands) may have been overwritten by data commands issued by these other users. If this occurs, the final entries of the report show the data commands issued by the other users since the recent change history report was originally requested.

Also, using **set time** to alter the system clock could make it look as if the recent change history report is not in true LIFO order.

list history field descriptions

Field	Description
Date	The date list history was issued (mm/dd).
Time	The time list history was issued (hh:mm).
Port	The port type to which the user was connected when list history was issued. - TTI, PSA, CTA and ACTR moves are recorded when the CTA/PSA/TTI Transactions in History Log field is y on the Feature-Related System Parameters screen. These transactions appear as two separate records: one recording the moved-from port, and the other one recording the moved-to port. - IP station registrations and unregistrations are recorded when the Record IP Registrations in History Log field is y on the Feature-Related System Parameters screen.

Table continues...

Field	Description
Login	Shows the user login or the feature that caused the logged event, such as: • actr for ACTR moves • cta for Customer Telephone Activation transactions • psa for Personal Station Activation transactions • tti for TTI transactions • ip-a or ip-u for IP registrations and events • pms for Property Management System events • ad for Abbreviated Dialing events • reboot for when the system rebooted
Actn	The action part of the command, specifying the operation to be performed. This field is truncated after four characters to allow enough space for objects and qualifiers and to uniquely identify each action.
Object	The qualifier (12 characters) specifying the object of the command. Where the object is multiple words in length, only the first word appears in the object field; every succeeding word is treated as a qualifier.
Qualifier	One or more qualifiers describing the characteristics of the Action/Object pair. This field is truncated after 31 characters to keep information for a command on a single line.

Communication Manager events are also logged in the Linux syslog. Syslog is a standard Linux service that supports storing event information in local files as well as sending events to an external syslog server. Syslog supports storing events in different files or 'logs' depending on the nature of the event.

Access the Communication Manager web interface log pages through Select Diagnostics > System Logs. For more information on 'Communication Manager web interface System Logs', see *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

The following types of activities are logged:

- Security-related events: Communication Manager logs all events related to security to the secure log. An administrator cannot disable or change parameters related to security events.
- System Administration Terminal (SAT) interface logging: Administration changes are logged to the command history log with the date and time, the unique identify of the person making the change, the value of the parameter that is changing and the status of the operation (successful or not). The administrator can configure the level of detail that is logged.

Communication Manager logs attempts by users to view information to which they are not permitted access or attempts to submit forms with invalid or non-acceptable values.

- Web page logging: Attempts to access the Avaya server's web pages and changes to a value in a web page are logged. Changes to a web page are logged only if the page is submitted, either successfully or unsuccessfully.

notify history

Use **notify history** to generate a continuous real-time log of the data-affecting administration and maintenance commands being executed currently.

Syntax

```
notify history
```

cmdHistoryLogConfig

Use **cmdHistoryLogConfig** command to define the number of months that the system must maintain the command history and to compress the command history file after execution of rotation action.

Syntax

```
cmdHistoryLogConfig[--numMonths <3-24>][--enableComp  
y | n][--minMonths][--maxMonths][--rclist][--rcode<number>][--help|-h]
```

- numMonths** number of months *commandhistory* log is to be retained.
- enableComp:** sets enabling (y) or disabling (n) of compression
- minMonths** displays the minimum number of months the command history log can be retained
- maxMonths** displays the maximum number of months the command history log can be retained
- rclist** list possible return code from this command
- rcode** obtain error string associated with return code
- help** displays usage

cmdHistoryLogConfig Field Description

Field	Description
numMonths	number of months commandhistory log is to be retained.
enableComp	This enables or disables the log compression. By default this value is set to <i>n</i> .
minMonths	The minimum number of months the command history log can be retained.
maxMonths	The maximum number of months the command history log can be retained
rclist	Possible return codes
rcode	This obtains the string associated with the return code entered.
--help	Provides help on the usage of the cmdHistoryLogConfig command.

hunt-group

display hunt-group

Use **display hunt-group** to see the hunt-group details.

Syntax

```
display hunt-group n, [number x] [to- number x] [count n] [schedule]
```

<i>n</i>	Group number between 1 and 8000.
<i>number x</i>	The starting hunt group number.
<i>to- number x</i>	The ending hunt group number.
<i>count n</i>	Number of hunt groups to appear on the page.
<i>schedule</i>	Specify a time to run the command.

list hunt-group

Use **list hunt-group** to see a list of hunt-group records

Syntax

```
list hunt-group [number x] [to- number x] [name x] [type x] [ext x] [to-ext n] [count n] [schedule]
```

initcauses

display initcauses

Use **display initcauses** to see a history of recovery steps taken by the system. **display initcauses** shows information for restarts of the active processor only. When the processor resets and the system is restarted, either by a technician command or by system software, information about the recovery is stored. If the reset is escalated, only the reset that successfully completes is recorded. The error log contains information about the reset. When a reset 4 (reload) occurs, the error log is saved on the disk.

Records of the last 16 restarts are retained in the initcauses log in chronological order.

Syntax

```
display initcauses [schedule ]
```

<i>schedule</i>	Specify a time to run the command.

display initcauses field descriptions

Field	Description
Cause	This gives the reason for the system reset as follows: • Craft Request — The reset was manually initiated using reset system. • Initialized — A power-up. Always the first entry in the log unless more than 15 restarts have occurred since the last power up. • Interchange — A State of Health change caused the arbiter process to initiate the restart. • Interchange-Craft — An administrative session (session -i command, on-demand interchange) caused the arbiter process to initiate the restart. • Internal Request — Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. • Software Request — Software requested the system restart.
Action	The level of recovery performed by the system. 1. Reset system 1 (Warm) — Communication Manager software is restarted, and active calls remain up. 2. Reset system 2 (Cold) — Communication Manager software is restarted, translations are preserved, and all calls are dropped. 3. Reset system 4 (Reload) — Communication Manager software is completely reloaded, and the hardware is reinitialized.
Escalated	y/n y — The restart was escalated to a higher level than originally attempted. The system's software escalation strategy can perform a higher level restart than the one initiated if problems prevent or conditions interfere with normal execution.
Mode	State of the server immediately after the interchange, at the time of the restart. Look for a change of mode to help determine when an interchange occurred. • Active — Mode of a simplex server and for a duplex server that is the active server. • Standby — Mode of a standby server in a duplex configuration. • Busyout — Mode of a standby server that has been placed out-of-service with a busyout command.
Time	The month, day, and time of the restart.

See **reset system** for details.

integ-annc-board

list usage integ-annc-board

Use `list usage integ-annc-board` to see information on the announcements and audio groups on an announcement media module.

For more information on 'Announcements/Audio Sources screens and integrated announcement boards', see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list usage integ-annc-board location
```

location Board location.

list usage integ-annc-board field descriptions

Field	Description
Used By	The type of announcement source on the announcement media module. • Audio Group with Audio Group number and Member number. • Announcement with Announcement number and Extension.

integ-annc-brd-loc

change integ-annc-brd-loc

Use `change integ-annc-brd-loc` to change all the currently administered 'from' board location to the **to** board location on the ANNOUNCEMENTS/AUDIO SOURCES and AUDIO GROUP screens.

Syntax

```
change integ-annc-brd-loc
```

The `change integ-annc-brd-loc` command does not physically move the announcement files. It only changes the administrative view on CM to the new location.

For example, you cannot use `change integ-annc-brd-loc` to change the location of the announcement files from an internal flash on the gateway to an external compact flash for backup and restore.

ip-media-parameters

display ip-media-set

Use **change ip-codec-set** to independently view codec sets used for media encryption or not.

Syntax

```
display ip-codec-set [ n ] OR display ip-media-parameter [ n ]
```

n Codec set number.

IP Media Parameter field descriptions — Page 1

Field	Description
Codec set	Specifies the codec set used between the network regions. If blank, there is no connectivity between the network regions.

Table continues...

Field	Description
Audio codec	Name of the audio codec in this codec-set: • G.711A (a-law) • G.711MU (mu-law) • G.722-64k • G.722.1-24k • G.722.1-32k • G.722.2 • G.723.5.3 • G.723.6.3 • G.726A-32k • G.729 • G.729A • G.729B • G.729AB • OPUS-NB12 • OPUS-NB16 • OPUS-WB20K • OPUS-WB24K • SIREN14-24k • SIREN14-32k • SIREN14-48k • SIREN14-S48k • SIREN14-S56k • SIREN14-S64k • SIREN14-S96kk
Silence Suppression	Specifies whether RTP-level silence suppression is enabled on the audio stream.
Frames Per Pkt	Number of frames per packet up to a packet size of 60 milliseconds (ms). 1–6 or blank. • G.711 default frame size is 2 (20 ms). • G.723 default frame size is 3 (30 ms). • G.729 default frame size is 2 (20 ms).
Packet Size (ms)	Size of the packet in milliseconds (ms).

Table continues...

Field	Description
Media Encryption	The options for each codec set apply to all codecs defined in that set. Appears when Media Encryption Over IP is <u>y</u> on the system-parameters customer-options screen.
Encrypted SRTCP	Specifies the Encrypted SRTCP is used to protect media control streams.

IP Media Parameter field descriptions — Page 2

Field	Description
Allow Direct-IP Multimedia	Specifies whether direct multimedia is allowed using the following codecs: • H.261 • H.263 • H.264 (video) • H.224 • H.224.1 (data, far-end camera control)
Clear-channel Mode	Specifies whether the support for this codec set for BRI data calls is enabled.
ECM	Specifies whether ECM-capable gateways use the T.38 protocol to relay T.30 ECM signaling and ECM frames between a local Group 3 fax machine and a far-end T.38 receiver.

Table continues...

Field	Description
FAX mode	• If you enter <code>off</code>, Communication Manager treats a fax call as an ordinary voice call. Turn off special fax handling. • If you enter <code>relay</code>, Communication Manager uses the relay mode for fax transmissions over IP network facilities only between Avaya devices. This mode may be coupled with Redundancy. • If you enter <code>pass-through</code>, Communication Manager uses the pass-through mode for in-band fax transmissions over IP network facilities only between Avaya devices. This mode may be coupled with Redundancy. • If you enter <code>T.38-standard</code>, Communication Manager uses the T.38 protocol for fax transmission over IP network facilities. • If you enter <code>T.38-G711-fallback</code>, Communication Manager uses the T.38 protocol for fax transmission only if the protocol can be successfully negotiated with the peer SIP entity. Otherwise, Communication Manager falls back to G.711 for transmission. This mode requires a G.711 codec to be administered on the <code>ip-codec-set</code> screen.  Note: If you have a telephone on an IP trunk that is close to a fax machine, the telephone can pick up the tones from the fax machine and change into the fax mode. To prevent this, turn off FAX mode and place fax machines in an Automatic Route Selection (ARS) partition that uses only circuit switched trunks, even for inter-gateway fax calls.
Maximum Call Rate for Priority Direct-IP Multimedia	The system displays this field only if Allow Direct-IP Multimedia is set to <code>y</code> .
Maximum Call Rate for Direct-IP Multimedia	The system displays this field only if you set the Allow Direct-IP Multimedia to <code>y</code> .

Table continues...

Field	Description
Modem Mode	• Enter <code>off</code> if you want to use this mode to treat a modem call as an ordinary voice call. Turn off special modem handling. The default mode for new installations and upgrades is <code>off</code>. • Enter <code>relay</code> if you want to use this mode for transporting modem traffic over IP using V.32 relay only between Avaya devices. • Enter <code>pass-through</code> if you want to use this mode for transporting modem traffic over IP network facilities only between Avaya devices. • Enter <code>v150mr</code> if you want to use this mode to use V.150.1 protocol to transmit modem signals between modems and telephony devices. The V.150.1 Modem-over-IP feature is used to interoperate with secure terminals and third-party SIP gateways.
Redundancy	Specifies the number of duplicate or redundant packets that must be sent in addition to the primary packet.
TDD/ TTY Mode	• Enter <code>off</code> to turn off special TTY handling when using this codec set. In this case, the TTY transmission is treated like an ordinary voice call. With a codec set that uses G.711, this setting is required to send TTY calls to non-Avaya systems. However, there might be errors in character transmissions. • Enter <code>US</code> to use U.S. Baudot 45.45 mode for TTY transmissions over IP network facilities. This is the default for new installations and upgrades. • Enter <code>UK</code> to use U.K. Baudot 50 mode for TTY transmissions over IP network facilities. • Enter <code>pass-through</code> to use pass-through mode for TTY transmissions over IP network facilities.

IP Media Parameters field descriptions — Page 3

The system displays this page only when you set the **Modem Mode** field to `v150mr`.

Field	Description
Modem Relay Preferred (NoAudio)	Specifies whether Communication Manager includes the NoAudio codec in the SIP SDP offer/answer message. You must enable this feature when a gateway interoperates with the devices that support offer/answer NoAudio codec. The default value is n.
Modulation Mode	Avaya V.150.1 supports the V.32, the V.34, the V.90, and the V.92 modem modulations. For users who need other modulations, you must set the Modem Mode field to pass-through. The following fields determine whether V.150.1 is enabled to transport the respective modulations as Modem Relay.
V. 32	Specifies whether the V.32 digital modem modulation is enabled
V.34	Specifies whether the V.34 digital modem modulation is enabled
V.90	Specifies whether the V.90 digital modem modulation is enabled
V.92	Specifies whether the V.92 digital modem modulation is enabled
SPRT Retransmissions	Specifies the maximum number of data retransmissions to Transport Channel 1 (TC1) and Transport Channel 2 (TC2).
SPRT TC0 Payload Size	Specifies the maximum payload size to SPRT Transport Channel 0.
SPRT TC1 Payload Size	Specifies the maximum payload size for SPRT Transport Channel 1.  Note: Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware version.
SPRT TC1 Window Size	Specifies the window size to SPRT Transport Channel 1. You can enter a value from 32 to 96. The default value is 32 bytes.
SPRT TC2 Payload Size	Specifies the maximum payload size to SPRT Transport Channel 2. You can enter a value from 132 to 256. The default value is 132 bytes.  Note: Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware versions.

Table continues...

Field	Description
SPRT TC2 Window Size	Specifies the window size to SPRT Transport Channel 2. You can enter a value from 8 to 32. The default value is 8 bytes.
SPRT TC3 Payload Size	Specifies the maximum payload size to SPRT Transport Channel 3. You can enter a value from 140 to 256. The default value is 140 bytes.  Note: Maximum SPRT payload sizes might vary across different gateways depending on the firmware and the hardware version.
SPRT Timer TC1-TA01	Specifies the value of the acknowledgement timer of Transport Channel 1. You can enter a value from 50 to 150 in increments of 10. The default value is 90.
SPRT Timer TC1-TA02	Specifies the value of the acknowledgement update timer of Transport Channel 2..
SPRT Timer TC1-TR03	Specifies the value of the retransmit timer of Transport Channel 1.
SPRT Timer TC2-TA01	Specifies the value of the acknowledgement timer of Transport Channel 2.
SPRT Timer TC2-TA02	Specifies the value of the acknowledgement update timer of Transport Channel 2.
SPRT Timer TC2-TR03	Specifies the value of the retransmit timer of Transport Channel 2.
SSE Inter-Packet Interval	Specifies an interval between the State Signaling Events (SSE) packets.
SSE Repetition Redundancy (Packets)	Specifies the number of redundant SSE packets for transmission. The redundancy option provides robust transport of data packets across an IP-based network.
V.42 error correction	V. 42 is an error correction protocol for V.150.1 media transport between modems. If you set this field to y, the gateways to use the V.42 error correction protocol. The default value is n.
Media Connection IP Address Type Preference	Specify the IP address type as IPv4 or IPv6.

ip-interface

change ip-interface

Use **change ip-interface** to see the IP-Interfaces report.

Syntax

```
change ip-interface [ procr ]
```

procr Status of administered v4 and v6.

change ip-interface field descriptions

Field	Description
Network Region	Network region in which the processor interface is placed.
Allow H.323 Endpoints?	Should we allow H.323 endpoints to register through this processor interface.
Allow H.248 Gateways?	Should we allow G4xx Media Gateways to register using this processor interface.
RT Delay (ms)	Elapsed time for a packet to reach remote location and revert. (Round Trip Delay)

ip-network-region

change ip-network-region

Use **change ip-netowrk-region** to change the audio and Quality of Service (QoS) attributes of IP network region *x*, where *x* is a network region number, or to change the codec set used for connections from network region *x* to other network regions.

To troubleshoot broken inter-network region connectivity, see **status ip-network-region**, **display failed-ip-network-region** and **test failed-ip-network-region**.

Syntax

```
change ip-network-region x
```

x Region number.

See *Administering Network Connectivity on Avaya Aura® Communication Manager* for administration guidelines.

list ip-network-region

Use **list ip-network-region** to list the administered network connections.

Syntax

```
list ip-network-region[monitor | direct-wan x]
```

monitor List the administered network connections.

direct-wan x List the network regions that are directly connected to the network region. The network region number ranges from **1** to **2000**.

status ip-network-region

Use **status ip-network-region** to see the status of the administered network connections between network region *x* and other network regions.

Syntax

```
status ip-network-region x ]
```

x IP network region number.

status ip-network-region field descriptions

Field	Description
Src Rgn	The source region number.
Dst Rgn	The destination region number.
Conn Type	The type of connection: • direct • indirect
Conn Stat	The status of connection: • pass • fail
BW-Limits	The bandwidth and limits as administered with add ip-network-region
BW-Used (kbits) Tx	The bandwidth used for transmission, direct connections only
BW-Used (kbits) Rx	The bandwidth used receiving, direct connections only
# Connections Tx	The number of transmission connections, direct connections only
# Connections Rx	The number of receiving connections, direct connections only
#Times BW-Limit hit Today	The number of times the CAC threshold limits reached since the previous midnight, direct connections only
IGAR Now IGAR Today	The number of active IGAR connections for the pair of Network Regions The number of times IGAR has been invoked for the pair of Network Regions since the previous midnight.

 Note:

If you set the **BW Management Option** field to `shared-SM`, you cannot run this command. The system displays the message: `Consult SMGR for bandwidth status.`

duplicate ip-network-region

Use `duplicate ip-network-region` to create duplicate network regions of an existing stub network region.

Syntax

```
duplicate ip-network-region x ] ['start' number] ['count' 1-16]
```

x Stub network region to duplicate.

start number Starting number of the new stub network region.

count 1-16 Number of duplicate stub network regions (same as NR 'x') you want to create. You can duplicate a maximum of 16 stub network regions.

For example the command: `duplicate ip-network-region 6 start 20 count 16`

Starting network region 20, will administer another 16 stub network regions same as network region 6.

 Note:

The duplicate network region command is not allowed for the stub network regions with dynamic BW units.

ip-stations

reset ip-stations

Use `reset ip-stations` to simultaneously unregister and reset all IP endpoints on a system, or a certain group of IP stations. You can limit the reset to only IP phones, to IP phones in a specific network region, to all IP endpoints in a specific network region, or within a range of IP addresses. Each defined IP station receives a reset message and is unregistered.

Use `reset ip-stations` to initiate simultaneous firmware upgrades to many IP stations, or a certain group of IP stations. You can reset IP stations on one ip-network region to prevent overloading a system with large numbers of IP station resets.

Syntax

```
reset ip-stations
```

reset ip-stations field descriptions

Field	Description
Reset Type	Specify the type of IP phones that you want to reset: • ip-phones: Resets IP phones. • tti: Resets phones in TTI state. • unauthenticated: Resets all unauthenticated IP stations. • all-ip: Resets all IP endpoints. • set-type: Resets a specified IP phone type. Enter the phone type in the Phone Type field. • status: Verifies if the reset ip-stations command is completed in the background.
Phone Type	Specify the phone model of the IP phones that you want to reset. The system displays this field when you set the Reset Type field to <code>set-type</code>.
Reset Type Option	Specify whether you want to reset the IP phones in a particular network region, all network regions, or within an IP address range: • ip-address: Resets IP endpoints within an IP address range. • ip-network-region: Resets IP endpoints in specified IP network region. • all-region: Resets IP endpoints in all IP network regions.
Starting IP Address	Specify the starting IP address of the range in which you want to reset the IP phones. The system displays this field when you set the Reset Type Option field to <code>ip-address</code>.
Ending IP Address	Specify the ending IP address of the range in which you want to reset the IP phones. The system displays this field when you set the Reset Type Option field to <code>ip-address</code>.
IP Network Region Number	Specify the IP network region in which you want to reset the IP phones. The system displays this field only when you set the Reset Type Option field to <code>ip-network-region</code>.

reset ip-stations feature interactions

Network regions

When setting up IP-network regions, you must consider into account the number of IP endpoints assigned to each region. Network regions are associated with specific media processing resources. Administer IP-network regions to a size that DHCP and TFTP servers can handle, and limit the performance impacts of simultaneously resetting large numbers of IP stations.

ip-synchronization

status ip-synchronization

Use **status ip-synchronization** to see the information about the status of the various gateways that are part of IP synchronization.

Syntax

```
status ip-synchronization [ master | member [ media-gateway ] n | oos-members |
source [ media-gateway ] n | system-information ]
```

master	Master sync sources in the system.
member media-gateway port-network n	Timing source for a given gateway or port-network.
oos-members	Members who are not synchronized and their service states.
source media-gateway port-network n	All gateways whose sync is sourced by the given gateway.
system-information	Global status of the sync over IP feature.

status ip-synchronization field descriptions — system information

Field	Description
Master domain count	Number of master IP sync domain count
Total domain count	Number of overall IP sync system count
Member count	Number of gateways in sync domains
Max level	Highest hop count by any member
Out of Sync	Number of members not in sync
Building domains	Indicates whether the new sync domains are created after the feature flag is turned on. When the field is set to n , the process is finished.
Removing domains	Indicates if the feature is removing the IGC streams and sync domains when the feature is turned off.

status ip-synchronization field descriptions — source | member [media-gateway | port-network]

Field	Description
Member	Displays all master sources of the system
Ref Stat	Displays the health of the reference board, whether the member is in service and setup to source IGC streams
DSP Status	Displays the status of the DSP
Input	Provides information about the incoming IGC stream
Inp	• R – Receiving stream • N – No stream detected • D – Stream detected
Jit	Jitter detected
Bad	Bad packets detected
Ord	Out of order packets detected
Dup	Duplicated packets detected
Loss %	Percentage loss of incoming stream
Output Lock	Provides information about the outgoing IGC stream. • Yes – Locked to input • No – Not locked, no output • Pnd – Pending lock • S – (sync) Indicates if the sync lead is connected
Sync ref	Displays whether the clock is synchronized to the synch lead of the MG
Tandem	Displays whether the member is a tandem clock

status ip-synchronization field descriptions — oos-members

Field	Description
Member	Displays all master sources of the system
Ref Stat	Displays the health of the reference board, whether the member is in service and setup to source IGC streams
DSP Status	Displays the status of the DSP
Input	Provides information about the incoming IGC stream
Inp	• R – Receiving stream • N – No stream detected • D – Stream detected
Jit	Jitter detected
Bad	Bad packets detected

Table continues...

Field	Description
Ord	Out of order packets detected
Dup	Duplicated packets detected
Loss %	Percentage loss of incoming stream
Output Lock	Provides information about the outgoing IGC stream. • Yes – Locked to input • No – Not locked, no output • Pnd – Pending lock • S – (sync) Indicates if the sync lead is connected
Sync ref	Displays whether the clock is synchronized to the synch lead of the MG
Role	Displays the role of the member
Reason fail	Displays why the member is out of synch with other members

isdnpri-testcall

clear isdnpri-testcall

Use `clear isdnpri-testcall` to cancel in-progress ISDN-PRI test calls. Once a running test call is cleared, another can begin.

Syntax

```
clear isdnpri-testcall [ group number / member number ]
```

group number Trunk group number.

member number Member within the trunk group.

Example

```
clear isdnpri-testcall 80 / 1
clear isdnpri-testcall 78 / 2
```

list isdnpri-testcall

Use `list isdnpri-testcall` to display the ISDN-PRI trunks currently in use for outgoing ISDN test calls.

Syntax

```
list isdnpri-testcall [ schedule ]
```

schedule Specify a time to run the command.

list isdnpri-testcall field descriptions

Field	Description
B-Channel	The trunk-group number and member number of the trunk in use.
Start Time	Day of the month, hour and minute when the test call began.
Duration	Expected duration, in minutes, of the test call.
M/T Port	Cabinet, carrier, slot and circuit number of the port on the Maintenance/Test media module in use for the outgoing test call.

status isdnpri-testcall

Use **status isdnpri-testcall** to display the progress of an outgoing ISDN-PRI test call on the specified trunk. The tested ISDN-PRI B-channel's port number, bit error rate, number of bits transmitted, block error rate, number of blocks transmitted, start time, duration specified, duration of test call, and reason of termination are displayed on the status screen.

Syntax

```
clear isdnpri-testcall [ group number / member number ]
```

group number Administered trunk group number.

group member number Administered group member within the trunk group.

status isdnpri-testcall feature interactions

If the bit error rate or block error rate is greater than zero, the ISDN-PRI trunk **may** be in a troubled state. Based on the statistical information displayed on the terminal, it can be decided to take the ISDN trunk out of service. This is subjective data because the ISDN trunk may be used for data or voice. If the trunk is used for data and the rates are high, the trunk should be taken out of service. If the trunk is used for voice, the trunk may not have to be taken out of service. High rates may also be due to some type of power hit on the line.

status isdnpri-testcall field descriptions

Field	Description
Port	This field specifies the physical address of the ISDN-PRI B-channel.
Bit Error Rate	The measured bit error count according to the comparison of the sent and received bit pattern. The number appears in scientific notation.
Number of Bits Generated	The number of bits generated. The number appears in scientific notation.
Block Error Rate	The measured block error count according to the comparison of the sent and received bit pattern. The number appears in scientific notation.
Number of Blocks	The number of blocks generated. The number appears in scientific notation.
Start Time	The time the test call started (dd/hh:mm).

Table continues...

Field	Description
Duration Specified	The duration specified in minutes for how long the test call should run. Valid durations are 1-120 (minutes) or blank (to indicate the default amount of minutes was used to run the test).
Duration of Test	The duration specified in minutes for how long the test call has been running. A blank indicates that the default amount of time was used to run the test.
Reason of Termination	The reason of termination indicates why the test call has terminated. Valid reasons of termination are: • finished — the test finished in the specified time. • canceled — the test call has been canceled with clear isdnpri-testcall. • overflow — the bits transmitted have overflowed buffer allocation. • no bits — no bits have been received because the ISDN-PRI test call circuit connection is bad. • transmission — there has been a data transmission interruption, probably caused from a power hit. • internal fail — there is an internal error on the Maintenance/Test media module. • in progress — the test is still running. • data corrupt — used for any other error condition.

Example

```
status isdnpri-testcall 78 / 1
```

test isdnpri-testcall

Use **test isdnpri-testcall** to start an outgoing ISDN-PRI test call.

Only one ISDN trunk in each port network can be tested at one time. The maximum number of asynchronous outgoing test calls that can be run simultaneously depends on the number of maintenance/test media modules in the system.

Syntax

```
test isdnpri-testcall [ group number / member number ] [ minutes num-minutes ] [ schedule ]
```

group number Administered trunk group number.

member number Administered member within the trunk group.

minutes num-minutes Specify the duration of the test call in minutes from 1 to 120. The duration defaults to 8.4 or 9.6 seconds.

schedule Specify a time to run the command.

For more information, see 'Test #258 under the ISDN-TRK (DS1 ISDN Trunk)' section in the *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Example

```
test isdnpri-testcall 78 / 2 minutes 10
```

Table 4: test isdnpri-testcall output field descriptions

Field	Description
Result	PASS — The test call was successfully initiated. ABORT — Resources were not available (for example, a B-channel or maintenance/ test media module). FAIL — An outgoing test call could not be initiated.

journal-link

status journal-link

Use **status journal-link** to see the operational status of a wakeup-log or a pms-log printer link. If the link is down, the number of times the switch has tried to re-establish the link will be shown.

A journal printer is used to document automatic wake-up events, emergency access to attendant events and, if the Property Management System is not functional, housekeeping events. When the system includes two printers, one is for the housekeeping events and the other is used for automatic wake-up events and emergency access events.

See **status link** for more details on links.

Syntax

```
status journal-link [ wakeup-log | pms-log ]
```

wakeup-log Status the printer that handles automatic wakeup events, emergency access events, and scheduled reports.

pms-log Status the printer that handles housekeeping events while the PMS is down.

status journal-link field descriptions

Field	Description
Link State	The operational status of the link: • up — normal operational state, the link is established and is capable of supporting the application. • down — link is physically down. • extension not administered — extension number for the printer has not been assigned on the hospitality system parameters.
Maintenance Busy	Whether there is any maintenance testing being performed upon the link.

Example

```
status journal-link wakeup-log
status journal-link pms-log
```

journal-printer

busyout journal-printer

Use **busyout journal-printer** to put the link to the Property Management System log or wakeup log printers in a maintenance busy state. When busied out, the link is dropped and no data transfer can take place over it.

Use **busyout journal-printer** to prevent unwanted interference between different maintenance processes. Maintenance software may put a component that is part of a link in a busy state, causing link setup to fail, and resulting in attempts by the system to reestablish the link. If a maintenance test requires that the component be idle, frequent attempts at re-setup may delay the recovery of a faulty component. Busyout the link to prevent re-setup attempts.

Syntax

```
busyout journal-printer [ pms-log | wakeup-log ]
```

pms-log Busies out the link to the Property Management System printer.

wakeup-log Busies out the link to the Wakeup Log printer.

release journal-printer

Use **release journal-printer** to return to service a busied out link to the Property Management System (PMS) log or wakeup log printers. See Busyout and Release Commands.

Syntax

```
release journal-printer[ wakeup-log | pms-log ]
```

wakeup-log The printer that handles automatic wakeup events, emergency access events and scheduled reports.

pms-log The printer that handles housekeeping events while the PMS is down.

For general information on journal printer links, see **busyout pms-link**. For information on journal printers, see **status journal-link**.

 Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

test journal-printer

Use **test journal-printer** to perform hardware diagnostics on the link between the switch and a specified journal printer link to either the pms-log printer or the wakeup-log printer.

Syntax

```
test journal-printer pms-log | wakeup-log [ short | long ] [ repeat # | clear ]
[ schedule ]
```

pms-log Test the link to the Property Management System printer, whose maintenance name is PMS-PRNT.

wakeup-log Test the wakeup-log printer, whose maintenance name is JNL-PRNT.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # The number of times to repeat the command. The default is 1.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

led

test led

Use **test led** to verify that a specified switch node is recognized by the system. Also use **test led** to identify a media gateway.

When **test led** is entered, the red, green and yellow media module LEDs are turned on until all administered carriers in the specified group have been lit for 2 seconds. They are turned off in the same order in which they came on. The cycle can be repeated a number of times with the **repeat** option. After every repeat cycle is completed, every affected LED is restored to reflect its current status.

Syntax

```
test led [ media gateway # | a-pnc | b-pnc ] [ repeat # ]
```

all Parameter description.

media-gateway # Gateway number.

repeat # (Optional) The number of times to repeat the command. The default is 1.

license

test license

Use **test license** to run a license file check on the server so you do not have to wait for the next hourly update to see if certain license errors have been cleared.

Syntax

```
test license [ long | short ]
```

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

short Execute a series of nondestructive diagnostic tests.

If the test results are:

- **PASS** — the system is in License-Normal mode.
- **FAIL** — the system is in License-Error or No-License mode, depending on the **Error** value.

link

busyout link

Use **busyout link** to put a specified packet gateway link in a maintenance busy state. For more information, see Busyout and Release Commands.

Caution:

Busyout of a link drops all calls and packet traffic dependent on that link. The application, adjunct, or switch connected to the link will be inaccessible and the link will have to be re-established later when returned to service. See status link on page 360 for more details on links.

Syntax

```
busyout link link#
```

link# A number assigned to the link on the Communication Interface Links screen.

status link

Use **status link** to see:

- Static information about the link.
- Data extension and port used, connect speed, and protocol information.
- Time information for PPP and Ethernet links, including the time of the last reset.
- Type and number of active applications.

Syntax

```
status link [link# | procr]
```

link# Number of the administered link.

procr Status of administered v4 and v6.

status link field descriptions, page 1

Field	Description
Link Number	Administered link number (assigned by add/change data-module)
Link Status	no, yes, unavail, connected, disconnected, enabled, out-of-service, or restarting
Link Type	The type of interface according to the physical/link protocol(s) immediately below the network layer in the protocol stack (Ethernet or PPP)

Table continues...

Field	Description
Link Name	Administered link name (assigned by add/change data-module)
Service Port Location	Administered port location (assigned by add/change data-module)
Service Port Data Extension	Administered extension number (assigned by add/change data-module)
Service State	in-service/idle, in-service/active, disconnected, out-of-service, maintenance busy, in-service, inactive, active, idle
Node Name	Administered node name for TCP/IP endpoint (assigned by add/change data-module)
Source IP Address	IP address administered for node name (assigned with change node-name or add/change data-module)
Enabled	y/n
Maintenance Busy	y/n
Active Channels	Number of active channels

status link field descriptions, page 2

Field	Description
Incoming received Unicast packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Incoming received multicast packets	The number of non-unicast (subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
Incoming dropped octets	The total number of octets received on the interface, including framing characters.
Incoming errored packets	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Incoming packets discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Outgoing Transmitted unicast packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Outgoing multicast packets	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Outgoing transmitted octets	The total number of octets transmitted out of the interface, including framing characters.
Outgoing errored packets	The number of outbound packets that could not be transmitted because of errors.

Table continues...

Field	Description
Outgoing packets discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

status link field descriptions, page 3

The processor or hop channel status information can take either 1 or 2 pages on this screen, depending on the number of links being reported and their condition.

 Note:

A dash (–) or a colon (:) between numbers indicates all numbers including and between the indicated numbers.

Field	Description
UP	Channels are up.
DOWN	Channels are down.
PND	Channels are in a pending state from the down to the up state (processor channels only)

status link field descriptions, page 4

The following is an example of the output of page 4 of **status link**. The screen displays every TCP/IP socket link that is currently up and active and that is using the Ethernet link n through the Processor Ethernet interface. Note that the service type of DOLAN reflects the total of IP endpoints and H323 signaling groups on that processor.

Field	Description
Service Type	
Sessions	

test link

Use **test link** to verify that the specified link is administered and performs a series of tests on the link. See **status link** for more details on links.

Syntax

```
test link link# [ short | long ] [ repeat # | clear ] [ schedule ]
```

- link#** Each link is identified by a number (1–16) assigned on the communication-interface links screen. **display communication-interface links** shows the location and identification of each link.
- short** Execute a series of nondestructive diagnostic tests.
- long** Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

- repeat #** Number of times to repeat the test.
- clear** Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
- schedule** Specify a time to run the command.

locations

list locations

Use `list locations` to view a list of administered locations.

Syntax

```
list locations
```

location-parameters

list location-parameters

Use `list location-parameters` to display a subset of fields for location-parameter sets 1 to 50.

Syntax

```
list location-parameters x
```

x x is the count.

list location-parameters field descriptions

Name	Description
Long Distance Access Code	The long distance access code that the system prefixes to the telephone number. This field accepts up to five digits. The default value is blank.
International Access Code	The International Access Code. This field accepts up to five digits. The default value is blank.
Local E.164 Country Code	The E.164 Country Code. This field accepts up to five digits. The default value is blank.
Off-PBX Feature Name Extension Set	The Feature Name Extension (FNE) set location-based FNEs. The value can be 0 to 10 for a medium configuration or 1 to 99 for a large configuration. The default value is blank.

Table continues...

Name	Description
Country code for CDR	The country code for the Call Detail Recording information of a location. The default value is one.
Line Load Control (LLC)	Line Load Control (LLC) indicates the level of restriction per location. If the restriction level is set, then users with the same or higher restriction level set on their COR will be restricted from originating calls. The default value of this field is 0.  Note: The location parameter index can be associated with multiple locations. If the restriction level is modified on the location parameter, it will apply to all the associated locations.
Date Format on Terminals	The field to set the date format on the terminals. The system displays this field only if you set the Multinational location field on the System Parameter Customer Options screen to <i>y</i>. The valid entries for this field are: 1. mm/dd/yy 2. dd/mm/yy 3. yy/mm/dd

logging-levels

change logging-levels

Use `change logging-levels` to control how much information is logged for SAT activity.

Syntax

```
change logging-levels
```

change logging-levels field descriptions

Field	Description
Enable Command Logging	y/n Enter y to enable SAT activity logging. Enter n to disable SAT activity logging.

Table continues...

Field	Description
Log Data Values	This value applies to EVERY field on a form. • both — causes both the value prior to a change and the value after a change to be logged. • new — causes only the value following a change to be logged. The value prior to the change is not logged. • none — neither the value prior to the change nor the value after the change is logged. However the form access is logged.
Display Logging Levels	y/n Enter y to log these commands and transactions to the Command History log. The Command History log is stored via syslog and is available from the server web pages only.

display logging-levels

Use **display logging-levels** to see what SAT activities are being logged to the Command History log.

Syntax

```
display logging-levels
```

See **change logging-levels** for screen and field descriptions.

login-id

reset login-id

Use **reset login-id** to terminate a SAT session on a TCP/IP link, or other traditional connection. Use **status logins** to see the ID number of all active SAT sessions.

Syntax

```
reset login-id n ]
```

n The number (0–999) of the SAT session.

Example

```
reset login-id 9
```

logins

status logins

Use **status logins** to see information about all of the users that are currently using the Communication Manager SAT.

The screen does not automatically update, and is a reflection of the system at the time the request was made. Users may have logged off, or on, or the command may have finished executing while the information is being displayed. This screen shows only those users who have a SAT session active. It does not show users that may be accessing the server but have no SAT session active. This screen also displays the IPv6 addresses.

Syntax

```
status logins
```

status logins field descriptions

Field	Description
Login	Login name.
Profile	The user profile number assigned to the login.
User's Address	User's IP address (correct regardless of whether the user is connected through a processor interface).
Active Command	Current or last command issued by the login. This field may not be accurate, and updates are not reflected until the next execution of status logins.
Session ID	The session number assigned by the system, in chronological order of access.

marked-ports

list marked-ports

Use **list marked-ports** to list every port that has been marked unusable with **mark port**.

Syntax

```
list marked-ports [ schedule ]
```

schedule Specify a time to run the command.

list marked-ports field descriptions

Field	Description
Port	The physical location (media gateway slot port circuit) of the marked port.
Board-Type	The type of media module with the marked port.

mct-history

list mct-history

Use `list mct-history` to display the data associated with the Malicious Call Trace (MCT) feature chronologically, with latest to oldest data displaying the last 16 records.

MCT enables customers to collect information that could be used to identify a calling party whose conversation is deemed to have a malicious intent. Several scenarios are possible:

- Communication Manager software records information about the caller, including the Calling Number whenever possible for incoming trunk calls. This information can be viewed using the Malicious Call Trace History report.
- If the Communication Manager server is connected directly to a public ISDN that follows the ETSI protocol standard, Communication Manager software sends a message to the network requesting that the source of the incoming call be identified and the call be registered.
 1. If the public ISDN sends an acknowledgment, the ISDN Notification field on the MCT History report will show `acknowledged`.
 2. If the public ISDN sends a rejection (perhaps because the feature was not subscribed), the ISDN Notification field on the MCT History report will show `rejected`.
 3. If the public ISDN does not send any response, the ISDN Notification field on the MCT History report will show `no response`.
- If the Communication Manager server is **not** connected directly to a public ISDN that follows the ETSI protocol standard, the ISDN Notification field on the MCT History report will display `not sent`. Note that this includes the following two cases:
 1. If the Communication Manager server is directly connected to a public ISDN that follows the Australian ISDN protocol standard (Country Protocol 2), the public ISDN is notified when MCT is activated, but the ISDN Notification field displays `not sent`.
 2. If the Communication Manager server is **indirectly** connected via a QSIG or DCS private network to a public ISDN that follows the ETSI or Australian ISDN protocol standard, a message is sent through the private network to the gateway server. The gateway server then notifies the public ISDN that MCT has been activated, but the ISDN Notification field displays `not sent`. Note that in the QSIG case, the private-network message is proprietary, so all servers between the user activating MCT and the gateway must be Communication Manager servers.

Syntax

```
list mct-history
```

list mct-history field descriptions

Field	Description
Date	The date of the occurrence.
Time	The time of the occurrence.
Contr Ext	Controlling Extension: The extension of the user who enabled the MCT control feature. The controlling extension user then has access (via display messages) to the information regarding the malicious call.
Active Ext	The extension of the user that activated the MCT feature.
Recorder Port	The port of a voice recorder being used to record the malicious call.
Redir From	For redirected calls, the party from which the malicious call was redirected (for example, coverage, forwarding).
Actual Party	The extension of the user who received the malicious call.
Parties on Call	The extensions of other parties connected to the malicious call when the MCT feature was activated.
ISDN Notification	Whether an ISDN notification was sent to the PSTN notifying them of the call, and whether the network responded.

measurements

list measurements aca

Use `list measurements aca` to identify possible trunk malfunctions.

Syntax

```
list measurements aca
```

For more information about using ACA, refer to 'Automatic Circuit Assurance' in *Avaya Aura® Communication Manager Feature Description and Implementation*.

list measurements ds1

Use `list measurements ds1` to list performance measurements on a DS1 link. The performance measurements of a DS1 link indicate the quality of the DS1's physical interface between the system and a far-end system.

Use `list measurements ds1-facility` to see link performance measurements on a DS1 Converter facility. The DS1 Converter complex consists of two DS1Cs connected by one to four DS1 facilities. Using this complex, you can extend the distance between two port networks up to 100 miles, thereby extending the range of the optical fiber link within limited bandwidth (96

channels). A DS1C complex can be used in a direct connectivity configuration or a Center Stage Switch configuration. The DS1 converters may be connected to an Expansion Interface (EI) or a Switch Node Interface (SNI) through a metallic connection.

Syntax

```
list measurements ds1 [ ds1-log ] location [ schedule ]
```

```
list measurements ds1-facility location [ log | summary ][ schedule ]
```

log Detailed report generated.

summary Summary report generated.

location The physical location of a DS1 media module entered as media gateway slot, or of a DS1 converter facility where location of the media module is entered and f is a letter (a-d) designating one of the four DS1 facilities.

schedule Specify a time to run the command.

Examples

```
list measurements ds1 log 2a18
list measurements ds1 summary
list measurements ds1-fac summary 2a18
```

list measurements ds1 field descriptions

Field	Description
Counted Since	The start time and date when the associated measurement counters were cleared or the DS1 media module or facility was administered.
Valid 15-Minute Intervals in Last 24 Hours	The total number of 15-minute intervals in the past 24-hour period that contain valid data. (0–96)
Seconds Elapsed In Current Interval	The number of seconds from the beginning of the current 15-minute interval. (0–900)
ESF Error Events	
Test	
Pattern	
Synchronized	
Loopback/Span Test Bit-Error Count	
Test Duration	
Worst 15-Minute Interval (Date, Time, Count)	The date, end time, and error count (from 0 to 900 in increments of four) of the 15-minute interval in the previous 24-hour period that contains the maximum value for each error category.
24-Hour Count	The sum of all valid 15-minute counts for the previous 24-hour period for each error category. (0–65535)

Table continues...

Field	Description
Current Interval Count	The error count for the current (incomplete) 15-minute interval for each of the four error categories. (0–900 or N/A if data for the 15-minute interval is invalid)
Category	The categories correspond to measurement error counters: • Errored Seconds — the value of the errored seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • Bursty Errored Seconds — the value of the bursty errored seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • Severely Errored Seconds — the value of the severely errored seconds counter for the specified 15-minute interval(0 - 900 or N/A if data for the 15-minute interval is invalid). • Unavailable/Failed Seconds — the value of the failed seconds counter for the specified 15-minute interval (0 - 900 or N/A if data for the 15-minute interval is invalid). • Controlled Slip Seconds • Loss of Frame Count

list measurements ip codec

Use `list measurements ip codec` to see IP media processing codec resource measurements. The `list measurements ip codec` command works on media gateway and Avaya Aura® Media Server.

The IP media processing codec resource measurements are listed by software. The report output may span multiple media gateways or Avaya Aura® Media Server. A single report output combines statistics from media module. Codecs are part of a common pool.

To estimate the amount of IP traffic used on IP trunks versus IP stations, compare the `list measurements ip codec` report with the lines of the `list measurements trunk-group`, `list performance trunk-group`, `list measurements outage-trunk`, and `monitor traffic trunk-groups` reports corresponding to IP trunk groups. It is required that the switch not have mixed IP and non-IP ports in a single trunk group.

Syntax

```
list measurements ip codec hourly-region# [ summary | detail ][ yesterday-peak | today-peak | last-hour ][ reg# ]
```

hourly-region#

Lists the measurements for the last 24 hours, from current hour backwards, for the indicated region. If the switch clock is changed, the report shows asterisks.

summary [yesterday-peak | today-peak | last-hour]

Lists the measurements for the previous day's peak, for every region with MEDPRO resources administered on the IP Interfaces screen. The peak hour in a given region is the hour at which [G.711 Usage (Erl) + G.711 Usage (Erl)] is a maximum for that region. If the switch clock is changed, the report shows asterisks.

detail [yesterday-peak | today-peak | last-hour]

Lists the measurements for the previous day's peak for the indicated region. If the switch clock is changed, the report shows asterisks.

list measurements ip codec field descriptions

Field	Description
Meas Hour	The hour the measurement was taken. Switches in multiple time zones are treated as in the current MMI reports. Do not assume that the customer has made any correlation between LAN regions and time zones. Range: 0000–2300.
Region	The network region that the IP Media Processors and Medpros for this measurement are in.
G.711 Usage (ERL)	Usage in Erlangs of G.711 codecs during the measurement interval. Includes time that the voice channels are on a call. Usage shall be measured from the time the voice channel is allocated until it is released. Calculated by: $(\text{Total Call Seconds}) / 3600$ where Total Call Seconds is a sum of the following: total time (in seconds) that a G.711 resource on a Medpro is in use total time (in seconds) that a G.711 resource on an IP Media Processor is in use
G.711 In Reg Peg	Total number of times an IP media processor port in the region was allocated to a G.711 call.
G.711 Out of Reg peg	The total number of times an IP media processor port was needed in the region for a G.711 call, but was successfully allocated to a resource in another region. Out of Region does not include denials. If "Network regions are interconnected" is n, Out of Region is always 0.
G.723/9 Usage (ERL)	Usage in Erlangs of G.723 or G.729 codecs during the measurement interval. Includes time that the voice channels are on a call. Usage shall be measured from the time the voice channel is allocated until it is released. Calculated by: $(\text{Total Call Seconds}) / 3600$ where Total Call Seconds is a sum of the following: total time (in seconds) that a G.723 or G.729 resource on a Medpro is in use twice the total time (in seconds) that a G.723 or G.729 resource on an IP Media Processor is in use
G.723/9 In Reg peg	Total number of times an IP media processor port in the region was allocated to a G.723 or G.729 call.

Table continues...

Field	Description
G.723/9 Out of Reg peg	The total number of times an IP media processor port was needed in the region for a G.723 or G.729 call, but was successfully allocated to a resource in another region. Out of Region does not include denials. If Network regions are interconnected is n , Out of Region is always 0 .

list measurements ip dsp-resource

Use `list measurements ip dsp-resource` on media gateway and Avaya Aura® Media Server to see the following:

- IP media processing DSP resource measurements
- G.711 equivalent peak usage at the network region level

The `list measurements ip dsp-resource` measurements are displayed by software. The report output may span multiple media gateway and Avaya Aura® Media Server. A single report output combines statistics from both media gateway and Avaya Aura® Media Server. Codecs are part of a common pool.

Syntax

```
list measurements ip dsp-resource hourly [summary|detail] [yesterday-peak|today-peak|last-hour] [reg#] [pn summary] [gn summary]
```

hourly

Lists the measurements for the last 24 hours, from current hour backwards, for the indicated region. If the switch clock is changed, the report shows stars.

summary [yesterday-peak | today-peak |last- hour]

Lists the measurements for the previous day's peak DSP Usage (Erl) for every regions with media gateway and Avaya Aura® Media Server. The peak hour in a given region is the hour at which DSP Usage (Erl) is a maximum for that region. If the switch clock is changed, the report shows stars. If you are running 3FQ08 Communication Manager software or later, the `list measurements ip dsp-resource summary` report shows G.711 equivalent peak usage at the network region level. It shows the peak hour of DSP resource activity per network region.

detail reg# [yesterday-peak | today-peak |last- hour]

Lists the measurements for the previous day's peak for the indicated region. If the switch clock is changed, the report shows stars.

gn summary

Lists the gateway summary report that shows the peak hour DSP usage for a specific H.248 branch gateway.

list measurements ip dsp-resource hourly report field descriptions

Field	Range	Description
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the media gateway and Avaya Aura® Media Server. The region number is assigned on the media gateway and Avaya Aura® Media Server during switch administration.
Meas Hour	0000–2300	Hour for which data is collected.
G711 Equivalent DSP Rsrc Capcty	0–99999 *	DSP resource capacity indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given network region. The asterisk (*) indicates that the media processor capacity changed during the measurement hour.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour. The “spike” traffic pattern helps to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
Endpoint In Reg Pegs	0–65535	The total number of times an IP media processor port in the region was allocated to a call/request within that same network region during the measurement hour. Endpoint calculations also include IP/SIP trunks and IGCs.

Table continues...

Field	Range	Description
Endpoint Out Reg Pegs	0–65535	The total number of times an endpoint request for an IP media processor port from a specific network region was allocated to a media processor in a different region. This might occur when there are no available resources in the requested network region, a call has been re-directed to another port network. If the Region fields on the Inter Network Region Connection Management screen are blank, then this measurement will always be 0.
Endpoint Denied Pegs	0–65535	The total number of times an IP media processor port was requested for a call, but was denied because there were no media processing resources available in the system.  Note: Calls that were re-directed are not counted as denied calls Denied peg counts are against the network region or the IP endpoint that is requesting the resource. Denied peg counts for IGCs are against the network region of the cabinet that is requesting the resource.

list measurements ip dsp-resource summary report field descriptions

Field	Range	Description
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for a specific network region.
G711 Equivalent DSP Rsrc Capcty	0–99999 *	DSP resource capacity indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given network region. The asterisk (*) indicates that the media processor capacity changed during the measurement hour.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour. The “spike” traffic pattern helps to determine when resources should be added.

Table continues...

Field	Range	Description
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
Endpoint In Reg Pegs	0–65535	The total number of times an IP media processor port in the region was allocated to a call/request within that same network region during the measurement hour. Endpoint calculations also include IP/SIP trunks and IGCs.
Endpoint Out Reg Pegs	0–65535	The total number of times an endpoint request for an IP media processor port from a specific network region was allocated to a media processor in a different region. This might occur when there are no available resources in the requested network region, a call has been re-directed to another port network. If the Region fields on the Inter Network Region Connection Management screen are blank, then this measurement will always be 0.
Endpoint Denied Pegs	0–65535	The total number of times an IP media processor port is requested for a call, but was denied because there were no media processing resources available in the system.  Note: Calls that were re-directed are not counted as denied calls Denied peg counts are against the network region or the IP endpoint that is requesting the resource. Denied peg counts for IGCs are against the network region of the cabinet that is requesting the resource.

Table continues...

Field	Range	Description
% Denied	0–99	Percentage Denied: The percent of pgs which were denied during the measurement period.  Note: It is possible to have denied calls even though Peak DSP usage has not been exceeded. For example, Peak DSP is 479 out of 480. The next call that comes in could be denied because it needs two DSP resources and only one is available (for example, if the call used a G.729 codec).
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource pn summary report field descriptions

Field	Range	Description
PN#- Type	1–64 F(iber) or I(P)	Indicates the port network of the media processor being measured. A port network number followed by F (for example, 1–F) indicates that this is a fiber-connected PN. Similarly, a port network number followed by I (for example 4–I) indicates that this is a IP-connected PN. Up to five rows of data is shown for each PN, based on the five lowest network region numbers administered. C — Cumulative total of all fiber connected PNs (that is, CCS).
Net Reg	All 1–250 or 1–2000 = future develmt	Shows data for a given PN across all network regions in that PN (note that typically media processors in a port network are administered for a single network region. However, that is not always the case). The network region column represents the network region of the IP media processors being measured; not the network region of the cabinets. The region number is assigned on the ip-interfaces screen during switch administration.
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific port network/network region combination.

Table continues...

Field	Range	Description
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Totals are shown for all fiber- and IP-connected PNs in cases where a port network has multiple media processors across different network regions.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with spike traffic patterns to determine when resources should be added.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
G711 Equivalent DSP IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints through an IGC (this is a subset of total DSP pegs).
PN Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the port network for a call, but was denied because there were no media processing resources available in that port network.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period.

Table continues...

Field	Range	Description
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource hourly pn summary report field descriptions

Field	Range	Description
PN#- Type	1–64 F(iber) or I(P)	Indicates the port network of the media processor being measured. A port network number followed by F (for example, 1–F) indicates that this is a fiber-connected PN. Similarly, a port network number followed by I (for example 4–I) indicates that this is a IP-connected PN. Up to five rows of data is shown for each PN, based on the five lowest network region numbers administered. C — Cumulative total of all fiber connected PNs (that is, CCS).
Meas Hour	0000–2300	The hour for which data is collected for the port network.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Totals are shown for all fiber- and IP-connected PNs in cases where a port network has multiple media processors across different network regions.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with spike traffic patterns to determine when resources should be added.

Table continues...

Field	Range	Description
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on).
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints through an IGC (this is a subset of total DSP pegs).
PN Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the port network for a call, but was denied because there were no media processing resources available in that port network.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval.

list measurements ip dsp-resource gw summary report field descriptions

Field	Range	Description
GW Num	G001–G250	Indicates the number of the administered H.248 branch gateway for which DSP resource usage is being reported for the given measurement hour.

Table continues...

Field	Range	Description
GW Type	g430 g450 ig550 trm480	Indicates the H.248 branch gateway type containing the DSP resource being used.
Peak Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific gateway.
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with spike traffic patterns to determine when resources should be added. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

Table continues...

Field	Range	Description
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints through an IGC (this is a subset of total DSP pegs). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
GW Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the gateway for a call, but was denied because there were no media processing resources available in that gateway. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

list measurements ip dsp-resource hourly gw summary report field descriptions

Field	Range	Description
GW Num	G001–G250	Indicates the number of the administered H.248 branch gateway for which DSP resource usage is being reported for the given measurement hour.
GW Type	g430 g450 ig550 trm480	Indicates the H.248 branch gateway type containing the DSP resource being used.
Meas Hour	0000–2300	The measurement hour with the highest Erlang usage for the specific gateway.
Net Reg	1–2000 or 1–250 depending on server configuration	The network region represents the network region of the IP media processors being measured. The region number is assigned on the ip-interface screen during switch administration.
G711 Equivalent DSP Rsrc Capcty	0–99999	G.711 Equivalent Digital Signaling Processor Resource Capacity. Indicates the maximum number of unencrypted, simultaneous G.711 DSP resources that could be supported for a given port network. The asterisk (*) in this column indicates that media processor capacity changed during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
G711 Equivalent DSP Rsrc Peak	0–99999	Indicates the maximum number of G.711 equivalent DSP resources used at any point in time in the measurement hour for that port network. This is helpful to customer with spike traffic patterns to determine when resources should be added. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

Table continues...

Field	Range	Description
G711 Equivalent DSP Usage (ERL)	0–9999.9 Erlangs	G.711 Equivalent DSP Usage. Total G.711 equivalent usage for all codecs that were in use during the measurement period. The time is measured from the time the voice channel is allocated until it is released, including the time that the voice channel is on a call. Depending on the media processor being used usage counts may vary per codec (for example, TN2302 counts G.729/3 as 2, encryption counts as 1.25 and so on). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Usage	0–999.9 Erlangs	Total usage of a port-network or gateway for its involvement in Inter-PN or Inter-GW connections. Channel usage may be from IP endpoints or an IGC. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
Total DSP Pegs	0–65535	The total number of times media processor resources were allocated in a network region during the measurement hour. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
IGC Pegs	0–65535	Inter-Gateway Connection Pegs. The number of times media processor resources were allocated in a port network to connect two endpoints through an IGC (this is a subset of total DSP pegs). Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
GW Denied Pegs	0–65535	The total number of times an IP media processor port is needed in the gateway for a call, but was denied because there were no media processing resources available in that gateway. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

Table continues...

Field	Range	Description
% Den	0–99 (pegs)	Percentage Denied: The percent of pegs which were denied during the measurement period. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.
% Out of Srv	0–99	Percentage Out of Service: The percent of total resource time that ports were out of service during the measurement period. This percent includes ports that were manually busied out or maintenance busy during the measured interval. Gateways with older firmware that do not support this feature display the capacity data as n/a, indicating that data is not available.

list measurements ip signaling-groups

Use **list measurements ip signaling-groups** to see the 10 worst signaling groups for each hour of today, starting with the most recent whole hour. The forms for the today and yesterday qualifiers are 24 pages, one for each hour. The groups for each hour will be rank-ordered from worst to least worst based on the Hour Average Latency.

Syntax

```
list measurements ip signaling-groups [ current-hour | last-hour | today yesterday ]
```

current-hour Shows the 10 worst signaling groups for the current hour.

last hour Shows the 10 worst signaling groups for the last full hour.

today yesterday Shows the 10 worst signaling groups for each hour of today, starting with the most recent whole hour, or yesterday.

list measurements ip signaling-groups field descriptions

Field	Description
Sig Grp No	The group number, rank ordered.
Region	The network region of the group.
Hour Average Latency (ms)	The average latency for the whole hour.
Hour Packets Sent	The number of packets sent during the whole hour.
Hour Packets Lost (%)	The percent lost packets for the whole hour (if 100% the corresponding latency is shown as ****).
Hour/Worst Interval	The hour and worst 3 minute interval within the hour. (The interval is identified by the last minute of the interval.)
Interval Average Latency (ms)	The average latency for the interval.

Table continues...

Field	Description
Interval Packets Sent	The number of packets sent during the interval.
Interval Packets Lost (%)	The percent lost packets during the interval (if 100% the corresponding latency is shown as ****).

media-gateway

add media-gateway

Use `add media-gateway` on the primary server to add a gateway to the system.

Syntax

```
add media-gateway [ x | next ]
```

x Number of the assigned gateway.

next Next available number.

add media-gateway field descriptions

Field	Description
Controller IPv4 Address / Controller IPv6 Address	(Display only) Blank until the gateway registers for the first time. The Controller IP Address field supports the IPv6 addresses. This is the IP address that the gateway is registered to on the server. • For Duplex servers and other External Call Controllers (ECC), this is a Procr address. • For Simplex servers, Survivable Remote Server, and other servers providing Processor Ethernet (PE), this is the native NIC address.
Enable CF?	Appears only for G450 and G430 gateways and only when the announcement module is administered in the V9 slot. The Enable CF? field indicates if you have enabled a compact flash to backup or restore the announcement files. The valid responses are y and n , where n is the default response. Enter y to enable a Compact Flash. If you are using a G450 Release 1.x, where the compact flash is not a valid option, the Enable CF? field is display-only and the value is set to n .

Table continues...

Field	Description
Encrypt Link	The valid values are y and n. Enter y to encrypt the H.248 link on the gateway. y is the default value when the gateway is added.
FW Version / HW Vintage	(Display only) Current firmware and hardware versions on the gateway.
IP Address	(Display only) The IP address of the gateway. Blank until the gateway registers for the first time. Once the gateway has registered, that IP address always appears, even if the gateway becomes unregistered until a gateway with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots.
Link encryption type	 Note: This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). The following are the valid entries for this field: • none: No encryption • any-ptls/tls: any-ptls/tls is the default value when Communication Manager is in the non-FIPS mode. • ptls-only: ptls is Avaya Proprietary Encryption Algorithm. • tls-only: tls-only is the default value when Communication Manager is in the FIPS mode.
Location	1 through 250 — (Depending on your server configuration, see <i>Avaya Aura® Communication Manager System Capacities Table</i>.) Refers to a time-zone offset, day-light savings rule, and number plan area code. See <i>Avaya Aura® Communication Manager Feature Description and Implementation</i>, for the other ways, and for a list of features that use location.  Warning: If you change the Location field while the gateway is registered, you must reboot the gateway to ensure optimal audio quality. Blank — The location is obtained from the gateway that the endpoint registered with. By default, the value is blank.

Table continues...

Field	Description
MAC Address	(Display only) MAC address of the gateway. Blank until the gateway registers for the first time. Once the gateway has registered, that MAC Address appears, even if the gateway becomes unregistered, until a gateway with a different MAC Address is validly registered with the same administered identifier.
Max Survivable IP Ext.	Appears when there is a Type such as G450 and J2320. Limits the number of simultaneous endpoint registrations for the gateway in SLS mode. VoIP resources in SLS can handle a limited number of simultaneous endpoint registrations. Administering this field above the default value can result in system performance problems.
MGP IPv4 Address / MGP IPv6 Address	This is the IP address of the H.248 branch gateway platform. The platform could reside in a network component that has its IP address. The field supports the IPv4 and IPv6 addresses.
Module Type	Type of Avaya Media Module in the slot. Refer to the administration guide of the gateway added for valid media modules and slot configuration. If an administered Media Module conflicts with the inserted Media Module, a pound sign (#) appears to the left of the Module Type field on the Media Gateway screen.
Mutual Authentication	 Note: This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). If the Link Encryption Type field is set to <code>none</code> or <code>ptls-only</code>, the Mutual Authentication field is unavailable. The Mutual Authentication field is optional. If Communication Manager is configured to operate in the FIPS mode, the Mutual Authentication field determines whether the gateway must send the Identity Certificate to Communication Manager as part of the TLS protocol certificate sharing. When the value of this field is set to <code>required</code>, during the TLS handshake Communication Manager requires the gateway to authenticate using a digital certificate. The Communication Manager server as the TLS host and the gateway as the TLS client have to exchange valid Identity certificates. When the value of this field is set to <code>optional</code>, Communication Manager accepts a TLS registration without the gateway Identity certificate. The default value of this field is <code>optional</code>.
Name	Name assigned to the gateway.
Name (Controller)	Name assigned to the controller.

Table continues...

Field	Description
Network Region	Network Region assigned to the gateway. Used by the primary server to allocate resources from the nearest gateway. The number of characters is dependent upon the type of primary server.
Number	(Display only) Number assigned to the gateway.
Recovery Rule	Number of the auto-fallback recovery rule that applies to this gateway. The recovery rule is set on the system-parameters mg-recovery-rule screen. none — no automatic fallback registrations are accepted. For more information about recovery rules, see <i>Administering Avaya Aura® Communication Manager</i> and <i>Administering Network Connectivity on Avaya Aura® Communication Manager</i> .
Registered?	(Display only) • y - The gateway is currently registered with the primary server. • n - The gateway is not currently registered with the primary server. • pd - The gateway registration is pending, subject to the Recovery Rule assigned on the set on the system-parameters mg-recovery-rule screen.
Gateway Mode	The Gateway Mode field is a display-only field. • Edge - The Communication Manager is connected to Session Border Controller. The Session Border Controller acts as an H.248 proxy server to convert the enterprise address for the Gateway of Communication Manager into a Public IP address and a NAT's IP address. Public IP address is used for routing and NAT's IP address is used for the final destination to operate in a NAT's branch office within a cloud-based service strategy, depending on the gateway configuration. • Enterprise - The Communication Manager is connected to the Gateway by using the enterprise network, also known as the enterprise address method.
Serial No	Used for the controller to identify the gateway.
Site Data	General site information.
Slot	(Display only) Slot number for the identified Media Module. Slots V8–V9, for virtual media modules, are listed after Slots V1–V4.
Type	Type of gateway. Use the help key to see the list of valid gateway types.
Use for IP Sync	Appears when the Synchronization over IP field is enabled. Indicates whether or not the G430 and G450 branch gateways are exempted from IP sync. By default, this field is enabled.

change media-gateway

Use **change media-gateway** to change the administration of a gateway.

Syntax

```
change media-gateway x
```

x Number of the assigned gateway.

See **add media-gateway** for an explanation of the field descriptions.

display media-gateway

Use **display media-gateway** to see information for a specific gateway.

Syntax

```
display media-gateway x [ schedule ]
```

x Number of the assigned gateway.

schedule Specify a time to run the command.

display media-gateway field descriptions

Field	Description
Registered?	(Display only) ad — The gateway is in a network region that was automatically disabled by the split registration solution feature. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. rd — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status rd. To enable the network region, the administrator must run the enable nr-registration command. ap — The gateway is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. rp — The gateway is in a network region that was manually disabled by the disable nr-registration command and is now communicating with CM. If a network region is both manually and automatically disabled, the status form shows only the manual status rp. To enable the network region, the administrator must run the enable nr-registration command.

list media-gateway

Use `list media-gateway` from the primary server to see all administered gateways.

Syntax

```
list media-gateway [ type x ] [ region # ] [ schedule ]
```

type x Type of gateway (g250, g430, g450).

region # Region number.

schedule Specify a time to run the command.

list media-gateway field descriptions

Field	Description
Number	The number assigned to the gateway by the primary server administration.
Name	The name given to the gateway by the user.
Serial No	The serial number of the gateway. Use the <code>show system gateway CLI</code> command or see the sticker on the back of the unit to locate the gateway serial number.
Rec Rule	Recovery Rule that applies to the gateway, as set on the system-parameters mg-recovery-rule screen. For more information about recovery rule, see <i>Administering Avaya Aura® Communication Manager</i> and <i>Administering Network Connectivity on Avaya Aura® Communication Manager</i> .
FW Ver/ HW Vint	Firmware version and hardware vintage.
Cntrl IP Addr	IP address of the Procr.
IPv4 Address/ IPv6 Address	The IP address of the gateway. The IP address field is blank until the gateway registers for the first time. Once the gateway registers, the IP address appears, even if the gateway becomes unregistered. That IP address changes when a gateway with a different IP address is validly registered with the same administered identifier. The populated IP address is persistent over reboots. The IPv6 addresses of the gateways are supported.
Type	Type of gateway. Use the help key to list the valid types of gateways.
NetRgn	The network region number assigned to the gateway.

Table continues...

Field	Description
Reg?	y — A gateway is currently registered with the primary server. n — A gateway is not currently registered with the primary server. pd — A gateway registration is pending, subject to the Recovery Rule as assigned on the set on the system-parameters mg-recovery-rule screen. ad — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and the gateway 2 is in a network region that was manually disabled by the disable nr-registration command. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. rd — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status rd. To enable the network region, the administrator must run the enable nr-registration command. ap — The gateway is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action. The region re-enables itself. rp — The gateway is in a network region that was manually disabled by the disable nr-registration command and is now communicating with CM. If a network region is both manually and automatically disabled, the status form shows only the manual status rp. To enable the network region, the administrator must run the enable nr-registration command.

reset media-gateway

Use **reset media-gateway** from the primary server to add a gateway to the system.

Syntax

```
reset media-gateway [ x | all ] [level 1|2|3]
```

x Number of the gateway to reset.

all Reset all registered gateways.

level 1 Forces a reset of the entire platform and is destructive to user connections. The gateway attempts to register with the gateway controllers on its MGC list.

level 2 Resets the H.248 link and does not tear-down calls. The gateway attempts to register with the gateway controllers on its MGC list. Use **reset media-gateway level 2** to force a gateway off of a Survivable Remote Server.

level 3 Resets all media modules and tears down all calls.

status media-gateway

Use **status media-gateway** to see the alarm status of the administered gateways.

status media-gateways lists alarms, busyout summary, and H.248 link status for the gateways. The alarms are associated only with board-type alarms on the media modules. Status for VoIP and MGP alarms are provided via the Media Gateway Processor CLI.

Syntax

```
status media-gateway
```

status media-gateway field descriptions

Field	Description
ALARM SUMMARY	Current number of alarms (Major/Minor/Warning) for all administered gateways
BUSYOUT SUMMARY	Current number of trunks/stations in a busy-out state for all administered gateways
H.248 LINKSUMMARY	Current number of H.248 links that are down and up for all administered gateways
GATEWAY STATUS Alarms (Mj, Mi, Wn)	Number of major alarms, minor alarms, and warnings that exist on each administered gateways.

Table continues...

Field	Description
GATEWAY STATUS Lk	Status of the H.248 link on each administered gateways up — the link is up dn — the link is down pd — the gateway has not yet returned to the primary call controller after having at least one registration request denied. ad — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and the gateway 2 is in a region that was manually disabled by the disable nr-registration command. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. rd — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status rd. To enable the network region, the administrator must run the enable nr-registration command. ap — The gateway 1 is in a network region that was automatically disabled by the split registration solution feature and is now communicating with CM and the gateway 2 is in a network region that was manually disabled by the disable nr-registration command and is now communicating with CM. To enable the network region (if the network region has a gateway administered for time-day-window), the administrator does not need to perform any action . The region re-enables itself. rp — The gateway is in a network region that was both manually and automatically disabled. In this case, the status form shows only the manual status rp. To enable the network region, the administrator must run the enable nr-registration command.

test media-gateway

Use **test media-gateway** from the primary server to run a board audit, an H.248 link audit, and an H.248 context audit.

- The link (test 1527) and context audits run successfully and no error codes are associated with the tests. Use **test media-gateway** to run an H.248 link audit when there is an alarm against a gateway for being unregistered when it actually is registered. If there is an interchange while a gateway is registering or unregistering, the alarm may appear and **status media-gateway** and **list media-gateway** may incorrectly show the gateway to be unregistered.
- Results of **test media-gateway** vary depending upon the configuration of the gateway.

Syntax

```
test media-gateway x
```

x Number of the assigned gateway

test media-gateway results

Gateway operating as	and is	Test result
main server	registered	pass
survivable remote server	registered	fail with error code 257
main server	unregistered, and the Link Loss Delay Timer period has not expired (link bounce is occurring)	fail with error code 769
main server	unregistered, and the Link Loss Delay Timer period has expired	fail with error code 1

Media Server

list media-server

Use the **list media-server** command to list all the administered media servers in Communication Manager.

Syntax

```
list media-server [starting media-server number] [count]
```

starting media-server number starting number of media-server in the list.

count number of media-server in the list.

list media-server field description

Field	Description
Num	The media-server number (1-250)
Sig-grp	Represents the SIP signaling group, which is used to connect with a specific media server.
Node-name	Represents a 15 character node-name, which is the node-name of the specific Avaya Aura® Media Server.
VoIP Channel License Limit	Represents a limit on the number of media channels that can be simultaneously established on this AMS. The field represents an upper limit, a limit on the number of media channels that can be simultaneously established on Avaya Aura® Media Server (MS). The field must be populated with a value from 1 to 9999 or left blank. Blank indicates no limit.

Table continues...

Field	Description
Dedicated VoIP Channel Licenses	The number of channel licenses that can be used by only the specific media-server.
VoIP Chls In-Use	The number of media server connections that are currently active.
NetRgn	The Far-End Network Region of the SIP signaling Group (1-250).
State	The current state of the media server as determined by Communication Manager. The current values are: • Out-of-Service (OOS): Avaya Aura® Media Server (MS) is Out-of-Service because the associated SIP signaling group is unable to ping Avaya Aura® Media Server (MS), or the signaling group is busied out. • In-service (INS): Avaya Aura® Media Server (MS) is in-service and fully functional and available for the establishment of audio channels. • Locked (LOCK): Avaya Aura® Media Server (MS) is locked through Avaya Aura® Media Server (MS) Element Manager (EM). No sessions are established when Avaya Aura® Media Server (MS) is in the LOCK state. Use Avaya Aura® Media Server (MS) EM to unlock this media-server. • Pending-lock (PLOCK): Avaya Aura® Media Server (MS) is placed into pending-lock through Avaya Aura® Media Server (MS) EM. Existing sessions remain active, however, no new sessions are created on Avaya Aura® Media Server (MS) by Communication Manager. • Pending In-Service (PINS): Avaya Aura® Media Server (MS) has not obtained license from WebLM server, the Communication Manager displays PINS state. • Not-Applicable (N/A): This state means that Communication Manager is not attempting to contact a specific media server. This state is only applicable for survivable processors.  Note: The Main server attempts to contact all Media servers. • Auto Disabled (AD): In an automatically disabled network region. • Region Disabled (RD): In a manually disabled network region by system administrator.

```
list media-server
```

MEDIA SERVERS REPORT

Num	Sig-grp	Node-Name	License Limit	Dedicated Licenses	Licenses In-Use	Net Rgn	Loc	State
1	300	B3h1-ams1	1		0	1	1	INS
2	301	B3h1-ams2	1		1	2	2	PEND-LOCK

add media-server

Use the **add media-server** command to add media servers in Communication Manager.

Syntax

```
add media-server xxx
```

xxx xxx can be 1 to 250

* Note:

Executing the command **add media server n** will pick the next available number.

Field	Description
Signaling Group	Identifies the signaling-group used by Communication Manager to communicate with the specific media server. The specific signaling-group must be of SIP type and peer server must be of Avaya Aura® Media Server. The signaling-group number cannot be assigned to another media server. The signaling group number is from 1 to 999.
VoIP Channel License Limit	Represents the maximum number of VoIP channel licenses, which can be used on this media server. The field represents an upper limit and must be populated with a value 1 to 9999 or can be left blank. Blank means there is no upper limit on the number of VoIP channels that can be used on the server.
Node Name	Identifies the Node Name of the media server, which is obtained from the far-end Node Name of the signaling group form. This is a read only field.
Network Region	Identifies the Network Region of the media server, which is obtained from the Far-end Network Region field of the associated Avaya Aura® Media Server (MS) signaling-group . This is a read only field.
Location	Displays the location obtained from the Network Region form. This is a read only field.

Table continues...

Field	Description
Announcement Storage Area	Displays where the announcements used on a specific Communication Manager are stored. Another Communication Manager, which shares a specific media server displays a different Announcement Storage Area.
Dedicated VoIP Channel Licenses	Represents the number of VoIP channel licenses, which are dedicated to the media server. The field must be populated with a value from 1 to 9999. A value of blank shows that no licenses are dedicated to this media server.

change media-server

Use the **change media-server** command to change the media server values in Communication Manager.

Syntax

```
change media-server xxx
```

xxx is integer range from 1–250. It indicates the media server is to be changed. If an argument X is for a media server that has not been added, then error message “X identifier not assigned” is displayed.

Field	Description
Signaling Group	Identifies the signaling-group used by Communication Manager to communicate with the specific media server. The specific signaling-group must be of SIP type and peer server must be of Avaya Aura® Media Server. The signaling-group number cannot be assigned to another media server. The signaling group number is from 1 to 999.
VoIP Channel License Limit	Represents the maximum number of VoIP channel licenses, which can be used on this media server. The field represents an upper limit and must be populated with a value 1 to 9999 or can be left blank. Blank means there is no upper limit on the number of VoIP channels that can be used on the server.
Node Name	Identifies the Node Name of the media server, which is obtained from the far-end Node Name of the signaling group form. This is a read only field.

Table continues...

Field	Description
Network Region	Identifies the Network Region of the media server, which is obtained from the Far-end Network Region field of the associated Avaya Aura® Media Server (MS) signaling-group . This is a read only field.
Location	Displays the location obtained from the Network Region form. This is a read only field.
Announcement Storage Area	Displays where the announcements used on a specific Communication Manager are stored. Another Communication Manager, which shares a specific media server displays a different Announcement Storage Area.
Dedicated VoIP Channel Licenses	Represents the number of VoIP channel licenses, which are dedicated to the media server. The field must be populated with a value from 1 to 9999. A value of blank shows that no licenses are dedicated to this media server.

display media-server

Use the **display media-server** command to display an assigned media server in Communication Manager.

Syntax

```
display media-server x
```

- x** is integer range from 1–250. It indicates the media server is to be displayed. If an argument X is for a media server that has not been added, then error message “X identifier not assigned” is displayed.

Field	Description
ID	Identification number of the media server.
Signaling Group	Identifies the signaling-group used by Communication Manager to communicate with the specific media server. The specific signaling-group must be of SIP type and peer server must be of Avaya Aura® Media Server. The signaling-group number cannot be assigned to another media server. The signaling group number is from 1 to 999.

Table continues...

Field	Description
VoIP Channel License Limit	Represents the maximum number of VoIP channel licenses, which can be used on this media server. The field represents an upper limit and must be populated with a value 1 to 9999 or can be left blank. Blank means there is no upper limit on the number of VoIP channels that can be used on the server.
Node Name	Identifies the Node Name of the media server, which is obtained from the far-end Node Name of the signaling group form. This is a read only field.
Network Region	Identifies the Network Region of the media server, which is obtained from the Far-end Network Region field of the associated Avaya Aura® Media Server (MS) signaling-group . This is a read only field.
Location	Displays the location obtained from the Network Region form. This is a read only field.
Announcement Storage Area	Displays where the announcements used on a specific Communication Manager are stored. Another Communication Manager, which shares a specific media server displays a different Announcement Storage Area.
Dedicated VoIP Channel Licenses	Represents the number of VoIP channel licenses, which are dedicated to the media server. The field must be populated with a value from 1 to 9999. A value of blank shows that no licenses are dedicated to this media server.

Command output is shown below:

```

display media-server 1                                     Page 1 of 1
                                     MEDIA SERVER
Media-Server ID: 1
Signaling Group: 22
VoIP Channel License Limit:
Dedicated VoIP Channel Licenses:
Node Name: AMS-HQ-1
Network Region: 23
Location: 1
Announcement Storage Area: ANNC-00181f86-2730-e401-0100-54043b700000

```

remove media-server

Use the **remove media-server** command to remove a media server that was previously added in Communication Manager.

Syntax

```
remove media-server x
```

x is integer range from 1–250 that indicates the media server number to be removed.

Field	Description
ID	Identification number of the media server.
Signaling Group	Identifies the signaling-group used by Communication Manager to communicate with the specific media server. The specific signaling-group must be of SIP type and peer server must be of Avaya Aura® Media Server. The signaling-group number cannot be assigned to another media server. The signaling group number is from 1 to 999.
VoIP Channel License Limit	Represents the maximum number of VoIP channel licenses, which can be used on this media server. The field represents an upper limit and must be populated with a value 1 to 9999 or can be left blank. Blank means there is no upper limit on the number of VoIP channels that can be used on the server.
Node Name	Identifies the Node Name of the media server, which is obtained from the far-end Node Name of the signaling group form. This is a read only field.
Network Region	Identifies the Network Region of the media server, which is obtained from the Far-end Network Region field of the associated Avaya Aura® Media Server (MS) signaling-group . This is a read only field.
Location	Displays the location obtained from the Network Region form. This is a read only field.
Announcement Storage Area	Displays where the announcements used on a specific Communication Manager are stored. Another Communication Manager, which shares a specific media server displays a different Announcement Storage Area.
Dedicated VoIP Channel Licenses	Represents the number of VoIP channel licenses, which are dedicated to the media server. The field must be populated with a value from 1 to 9999. A value of blank shows that no licenses are dedicated to this media server.

status media-server

Use the **status media-server** command to display the current status of a particular media server.

Syntax

```
status media-server x
```

x is the media server number that's status is displayed.

Field	Description
Media Server Number	The media-server number (1-250).

Table continues...

Field	Description
State	The current state of the media server as determined by Communication Manager. The current values are: • Out-of-Service (OOS): The displayed string is Out-of-Service. Avaya Aura® Media Server is Out-of-Service because the associated SIP signaling group is unable to ping Avaya Aura® Media Server (MS) or the signaling group is busied out. • In-service (INS): The displayed string is in-service. Avaya Aura® Media Server (MS) is in-service and fully functional and available for the establishment of audio channels. • Locked (LOCK): The displayed string is locked. Avaya Aura® Media Server (MS) is locked through Avaya Aura® Media Server (MS) Element Manager (EM). No sessions exist when Avaya Aura® Media Server (MS) is in the locked state. Communication exists between Communication Manager and Avaya Aura® Media Server (MS). However, Avaya Aura® Media Server (MS) rejects all Communication Manager channel establishment requests. Communication Manager does not use a locked Avaya Aura® Media Server (MS). When Avaya Aura® Media Server (MS) is unlocked, it is placed into service and is usable by Communication Manager. • Pending-lock (PLOCK): The displayed string is pending-lock. Avaya Aura® Media Server (MS) is placed into pending-lock through AMS Element Manager. Existing sessions remain active. However, no new sessions are created on Avaya Aura® Media Server (MS) by Communication Manager. • Pending-In-Service (PINS): Avaya Aura® Media Server (MS) has not obtained licence from the WebLM server. PINS state is displayed on Communication Manager. • Not-Applicable (N/A): This state means that Communication Manager is not attempting to contact a specific media server. This state is only applicable for survivable processors.  Note: The Main server attempts to contact all Media servers. • Auto Disabled (AD): In an automatically disabled network region. • Region Disabled (RD): In a manually disabled network region by system administrator.

Table continues...

Field	Description
Sig-grp	The SIP signaling group.
Node-name	The node-name of Avaya Aura [®] Media Server (MS).
IP Address	The actual IP address of the media server.
NetRgn	The Far-End Network Region that is used to communicate with the media-server of the SIP signaling Group (1-250).
SW-Version	The software version of the media-server.
VoIP Channel License Limit	A limit on the number of media channels that can be simultaneously established on Avaya Aura[®] Media Server (MS). The field must be populated with a value from 1 to 9999 or left blank. Blank indicates no limit.
Dedicated VoIP Channel Licenses	The number of channel licenses that can be used by only a specific media server. The field displays a value of blank or values from 1 to 9999. Blank indicates no limit.
VoIP Channel Licenses In-Use	The number of media server connections that are currently active.
Load Factor	Current load as measured by Avaya Aura[®] Media Server (MS). The load factor has a range of 0 to 100%. A load factor approaching 100 implies that the media server is pushed to the limits of its processing capacity.
Estimated VoIP Channel Capacity	An estimate of the maximum number of audio channels that can be established on the specific Avaya Aura [®] Media Server (MS).
Announcements Present	The number of announcement files administered on Communication Manager that exist on the media server in the announcement storage area used by the specific Communication Manager.

status media-server 1

Page 1 of 1

MEDIA-SERVER STATUS

```

Media Server Number: 1
    State: in-service
    Sig-grp: 1
    Node Name: AMS-HQ-1
    IP Address: 10.129.48.150
    Network Region: 1
    SW-Version: 7.6.0.354
    VoIP Channel License Limit:
Dedicated VoIP Channel Licenses:
    VoIP Channel Licenses in-use: 853
    Load Factor: 22%
Estimated VoIP Channel Capacity: 3250
Announcements Present: 124

```

meet-me-vdn

reset meet-me-vdn

Administrators use the **reset meet-me-vdn** command to disconnect all the members of a given meet-me conference and then place that conference back into an idle/active state. The maintenance commands **status meet-me-vdn xxxx** and **reset meet-me-vdn xxxx** are added for the meet-me conference VDNs; where xxxx is the extension.

Type the command **reset meet-me-vdn xxxx** and then type the command **status meet-me-vdn xxxx**.

Syntax

```
reset meet-me-vdn  xxxx
```

xxxx Extension number.

mg-announcements

status mg-announcements

Use **status mg-announcements** to see the status of the announcements of the administered gateways.

Syntax

```
status mg-announcements
```

status mg-announcements field descriptions

Field	Description
Announcements Enabled?	Displays whether the announcements for the gateway have been enabled by using the enable announcement-board command. If Announcements Enabled? is y, announcements for the gateway have been enabled. If Announcements Enabled? is n, announcements for the gateway have not been enabled.

Table continues...

Field	Description
CF Storage Usage (MB)	If the gateway is G450 or G430 and the Enable CF? field on the change media-gateway screen is y, the memory data of the compact flash is displayed. If CF Storage Usage(MB) field is not applicable for a gateway, n/a is displayed. CF Storage Usage (MB) has the following fields: • Total — displays the total memory of the compact flash • Annc — displays how much memory of the compact flash is currently used for the announcements • Avail — displays how much memory of the compact flash is left for use There could be other things along with the gateway announcements which are stored on the compact flash. So, it is not necessary that the total memory of Annc and Avail adds up to to the total memory of the compact flash. Also, the numbers that are represented are block-sized numbers and different compact flash cards could have different block sizes.
CF Status	Displays the status of the compact flash. The status of the compact flash is displayed as one of the following: • Ins — the compact flash is inserted on the gateway and is recognizable. • Act — the compact flash is being used. • Err — The compact flash: - is either not present or not recognized - does not have sufficient space on the compact flash - does not have sufficient RAM available for usage

mg-return

enable mg-return

Use **enable mg-return** to perform automatic return of gateways to the main or Survivable Core Server without needing to reset each Survivable Remote Server.

The administrator can force the main or Survivable Core Server to accept the gateways and telephones.

Syntax

```
enable mg-return network-region R | all
```

network-region *R* Enable all gateways within network region *R*.

all Enable all the gateways.

The **enable mg-return** command overrides the gateway recovery rules that block registration if Survivable Remote Servers are active or inactive. Such overriding can be applied per region.

If there are no gateways in the region and the command **enable mg-return network-region *R*** is run, the following error message is shown:

```
IP network region has no gateways administered.
```

The administrator can run the command **disable nr-registration** on any region. If the status of a gateway in that region is already **ad** or **ap**, the status changes to **rd**. For information on the gateway registration statuses — **ad**, **ap**, and **rd** — see the field descriptions of **display media-gateway**, **list media-gateway**, and **status media-gateway**.

Important:

The **enable mg-return** command remains active for a period of 60 minutes. During this period of 60 minutes, if you want to move the gateways and phones from server to server, you must run the **disable mg-return** command first to end the 60 minutes timer. If you do not run the **disable mg-return** command, the timer either ends itself after a period of 60 minutes or after the Survivable Remote Server reports to the main Communication Manager server that the gateways have unregistered from the Survivable Remote Server.

mis

busyout mis

Use **busyout mis** to busyout a management information system.

Syntax

```
busyout mis [ processor-channel identifier | all]
```

processor-channel identifier Busyout an MIS link.

all Busyout all MIS links.

release mis

Use **release mis** to activate management information systems. Hardware tests are executed to verify that equipment is functioning properly.

Syntax

```
release mis [ processor-channel identifier | all ]
```

processor-channel identifier	Release an individual MIS link.
all	Release all MIS links.

modem-pool

release modem-pool

Use **release modem-pool** to deactivate specified modem pool groups or group members. Specify group numbers and member numbers to release single group members. Specify modem pool group numbers to release members in a modem pool group.

For more information see Busyout and Release Commands.

Syntax

```
release modem-pool group # | member #
```

group # 1–5.

Pair of analog and digital line ports (or two pairs for the Integrated modem-pool case).

member # 1–32.

test modem-pool

Use **test modem-pool** to performs hardware diagnostic tests on the specified modem pool group or an individual member of a specified group (Combined or Integrated). A combined modem-pool group consists of pairs of analog and digital line ports. One pair of analog and digital line ports used for modem-pooling is called a conversion resource. An Integrated group consists of modem-pool media modules, each containing two conversion resources. Therefore, when a member number is specified for a combined modem-pool group, one conversion resource is tested, and when a member number is specified for an integrated modem-pool group, two conversion resources are tested.

Syntax

```
test modem-pool[ group # | member # ][ short | long ][ repeat # | clear ][ schedule ]
```

group # The administered group number (1–5).

member # 1–32.

short Execute a series of nondestructive diagnostic tests.

- long** Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.
- repeat #** Number of times to repeat the test.
- clear** Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.
- schedule** Specify a time to run the command.

moh-analog-group

list moh-analog-group

Use **list moh-analog-group** to list **Music On Hold** groups and see how many members (audio sources) are in each group.

For more information on the Music On Hold Groups screen, see *Administering Avaya Aura® Communication Manager*.

Syntax

```
list moh-analog-group {[ 1-Max ] ( number n | ( to-number n ) | count n ) } [ schedule ]
```

- 1-Max** Music On Hold number.
- number *n* to-number *n*** Range of Music On Hold group numbers to see on the page.
- count *n*** Number of Music On Hold groups to see on the page.
- schedule** Specify a time to run the command.

list moh-analog-group field descriptions

Field	Description
Number	Number of the Music On Hold group.
Name	Name of the Music On Hold group.
Number of Sources	Number of members (sources) in the Music On Hold group

monitored-station

list monitored-station

Use `list monitored-station` to see information on stations controlled by domain-controlled associations. Each station can have a maximum of eight domain-controlled associations.

Syntax

```
list monitored-station [ start extension] [countxxxx ]
```

start extension Starting extension for the list.

count xxxx Number of stations on the list.

list monitored-station field descriptions

Field	Description
Ext	Station extension number
CTI Link	ASAI CTI link number associated with the CRV
CRV	ISDN Call Reference Value

mst

clear mst

Use `clear mst` before a trace. If `clear mst` is active during a trace, it clears unwanted data.

Syntax

```
clear mst
```

change mst

Use `change mst` for a trace. If `change mst` is active during a trace, it changes the data.

Syntax

```
change mst
```

Table 5: Change mst field descriptions

Field	Description
Log Mst	Set Log Mst to <code>y</code> to send trace both to MST buffer in memory and to log files in <code>/var/log/ecs</code> .
Trace Analyzer	Set Trace Analyzer to <code>y</code> to interpret the trace on the server itself.

disable mst

Use **disable mst** to stop the message trace facility. If the trace was not already disabled, the command inserts a GAP marker into the trace. The user should execute **disable mst** when the trace is complete. If left enabled, the trace continues to use CPU time until the time limit expires. Entering **disable mst** has no effect on the system if the trace is already disabled. To view the results of the trace, enter **list mst**.

Syntax

```
disable mst
```

display mst

Use **display mst** to provide message tracing for SIP.

Syntax

```
display mst
```

display mst field descriptions

Field	Description
Signalling Group	The assigned signaling group number which provides message tracing for all SIP messaging on the signaling group. The signaling group number is from 1 to 999, or leave blank.
Message Bodies	Indicates if SDP encoding is included in the trace. The default value is y .
Calling User	Allows entry for user portion of incoming URI. The length of the URI is from 0 to 20, or leave blank.
Called User	Allows entry for user portion of outgoing URI. The length of the URI is from 0 to 20, or leave blank.

list mst

Use **list mst** to see the messages in the trace buffer while a trace is active or disabled. If the trace is active, older messages may be sporadically omitted if wraparound is selected and the message rate is high. The integrity of the buffer remains intact even when **list mst** is used repeatedly.

Syntax

```
list mst [ from message number ] [ count number ] [ continuous | LIFO | FIFO | auto-  
page ]
```

from message number

First message in the list. List indicates if the number is not in the buffer, and no additional messages appear.

If no message number is entered, the list begins with the oldest FIFO message.

count number	The number of messages in the list. Use this number to limit the trace.
continuous	Display updates as new messages enter the trace buffer (FIFO). This option is most useful in conjunction with auto-page . The command terminates when canceled by the user.
LIFO	Show newest message first.
FIFO	Show messages in the order received.
auto-page	The screen will automatically page when full. Use with continuous to see messages arrive.

MST message descriptions

The terminology Message [n] used in this section refers to the byte at offset n in the message being displayed.

MST message types contain a version number. When the structure of the MST message changes, the version field in the MST buffer also changes. Version 1 displays a blank in the version field immediately after the MST message type field. Subsequent versions display the version number after the MST message type field and are connected with a hyphen (-). For example: Version 2 of the X.25 Application error/notification message added the text of the pm state table stimulus, which was ignored.

list mst field descriptions

Field	Description
Number	The sequence number for the message.
Date/Time	The date/time of the message.
Type	MST message type: 60 = ISDN uplink 62 = ISDN downlink 6C = ISDN level 2 primitive
Message	Message text in hexadecimal.

Example

```
list mst continuous
list mst continuous auto-page
list mst LIFO
list mst from 222 count 7
```

multimedia

list multimedia

Use **list multimedia** to see the list of multimedia endpoints, h.320-multimedia endpoints, multimedia IP endpoints, or unregistered multimedia IP endpoints.

Syntax

```
multimedia [ endpoints | h.320-stations | ip-stations | ip-unregistered ] [ ext x ] [ to-ext x ] [ count n ] [ schedule ]
```

- endpoints** List multimedia endpoints.
- h.320 endpoints** List multimedia H.320 endpoints.
- ip-endpoints** List multimedia IP endpoints.
- ip-unregistered** List unregistered multimedia IP endpoints.
- ext x** List information for a specific extension.
- to-ext x** when used with [ext x], list information for all multimedia endpoint types beginning with one extension and ending with another.
- count n** List a certain number (*n*) of multimedia endpoints.
- schedule** Specify a time to run the command.

list multimedia field descriptions

Field	Description
IP STATION	
Ext	Extension of the IP station.
Registered	Show the current registration status of the endpoint.
Port	Port information for the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.
Registered	Shows the current registration status of the endpoint.
MEDIA COMPLEX	
Ext	Extension of the endpoint.
Port	Port information for the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.
Registered	Shows the current registration status of the endpoint.

network-region-group

list members network-region-group

Use the `list members network-region-group` command to list the network regions that are administered to the network region group.

Syntax

```
list members network-region-group [x] [schedule]
```

x: Network region group number.

schedule Specify a start time for the command.

Field	Description
Network Region Group	The network region group number.
Name	The name of the network region group.
Network Regions	The name of the network regions that are administered to the network region group.

list network-region-group

Use the `list network-region-group` command to list the administered network region groups. The system displays the Network region group screen only if any of the network regions that are assigned to the network region group are in use. That is, the network region is used in an IP network region, a signaling group, a media server, an IP interface, an IP network map, a cabinet, or a media gateway.

Syntax

```
list network-region-group [schedule]
```

schedule Specify a start time for the command.

Field	Description
Name	List of the network region groups available in the system.

night-service

list night-service attendant

Use `list night-service attendant` to see all the attendants that are in night service.

Syntax

```
list night-service attendant
```

list night-service attendant field descriptions

Field	Description
No.	The night service attendant number.
Extension	The extension of the voice or data endpoint associated with the night service attendant.
Name	The name of the night service attendant.
Group NO	The attendant group number.

list night-service hunt-group

Use `list night-service hunt-group` to see all the hunt groups that are in night service.

Syntax

```
list night-service hunt-group
```

list night-service hunt-group field descriptions

Field	Description
No.	The night service hunt group number.
	The night service destination. The night service destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or attnd if you want to direct calls to the attendant.

list night-service trunk-group

Use `list night-service trunk-group` to see all the trunk groups that are in night service.

Syntax

```
list night-service trunk-group
```

list night-service trunk-group field descriptions

Field	Description
No.	The night service trunk group number.
Destination	The night service destination. The night service destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or attnd if you want to direct calls to the attendant.

node-names

display node-names

Use **display node-names** to see a list of the administered node names.

Syntax

```
display node-names [ schedule ]
```

schedule Specify a time to run the command.

display node-names field descriptions

Field	Description
Name	Identifies the name of the adjunct or switch node. Enter 1–7 characters for audix or msa; Enter 1–20 characters for others. Default is blank. Node name for CMS nodes, DCS nodes, and so forth.
IP Address	IP address for the adjunct or switch. Enter 0–255 or leave blank.

nr-registration

disable nr-registration

Caution:

disable nr-registration can cause momentary service disruption. It causes all gateways and IP phones in a network region to unregister from the server where the command is executed. **disable nr-registration** is automatically saved across system restarts even without **save translation**.

Use **disable nr-registration** to deny gateways and IP-phones within a specified IP Network Region from registering on the primary server or survivable processor. This causes the gateways and IP phones to register instead with an alternate server or Survivable Remote Server. This is useful when network outages cause gateways and IP phones to disconnect and reregister with the primary server in an interval that is too short for the endpoints to fail over to a Survivable Remote Server.

Use **disable nr-registration** on a primary server and a Survivable Core Server. The disabled network region registration state on the primary server is not file-synced to the Survivable Remote Server or associated Survivable Core Server.

A gateway must be assigned to the specified network region.

If you have set the value of the Force Phones and Gateways to Active LSPs? field in the system-parameters ip-options screen as **y** and then run the **disable nr-registration** command on one network region, Communication Manager applies this command to all the network regions associated with the Survivable Remote Server. For example, a single Survivable Remote Server is the backup server for multiple network regions—network region 1 and network region 2. A system administrator runs the **disable nr-registration 1** command. The Communication Manager server disables region 2. A gateway in network region 1 is unregistered from the Communication Manager server and registers to the Survivable Remote Server. The Survivable Remote Server reports to the main Communication Manager server that the Survivable Remote Server is active. The Communication Manager server then automatically disables network region 2.

The **disable nr-registration** command causes a disable network region warning alarm to appear in the alarm log.

 Note:

When the Enable Detection and Alarms field is **y** on the system-parameters ip-options screen (**change system-parameters ip-options**) the detection of the hyperactive link bounce is enabled which will cause associated gateway and network region alarms.

Syntax

```
disable nr-registration x
```

x IP network region number. A gateway must be assigned to the network region.

enable nr-registration

Use **enable nr-registration** to end an active **disable nr-registration** command.

This enables the gateways and IP-phones within the specified IP Network Region to register with the primary server or survivable processor.

However, the **enable nr-registration** command can only end an active **disable nr-registration** command. This command cannot override any other condition that prevents the gateways and IP phones to register with the primary server or survivable processor.

For example, if the time-day-window prevents the gateways and IP phones to register with the primary server, you cannot use the **enable nr-registration** command to register the gateways and IP phones with the primary server.

If you have set the value for the Force Phones and Gateways to Active LSPs? field in the system-parameters ip-options screen as **y** and then run the **enable nr-registration** command when the Survivable Remote Server is active, the command does not immediately enable the network region. Instead, the **enable nr-registration** command puts the network region into an

auto-disabled state. Communication Manager does this so that if the Survivable Remote Server is backing up more than one region, the **enable nr-registration** command does not cause a split registration by allowing endpoints in that one region to return to the Communication Manager server while endpoints in other regions backed up by the same Survivable Remote Server stay on the Survivable Remote Server.

Use **enable nr-registration** on a primary server, a Survivable Core Server, and a Survivable Remote Server. The enabled network region registration state on the primary server is not file-synced to the Survivable Remote Server or associated Survivable Core Server.

Syntax

```
enable nr-registration x
```

- x** IP network region number.
A gateway must be assigned to the network region.

status nr-registration

Use **status nr-registration** to view information about the status of the network regions and the link status of the gateways in the network regions.

* Note:

To disable network regions manually, use the command **disable nr-registrations [network region number]**. To enable a network region manually, use the command **enable nr-registrations [network region number]**.

The Split Registrations Prevention Feature (SRPF) automatically disables certain network regions when those regions are controlled by a Survivable Remote Server which has gone active.

To enable SRPF, set Force Phones and Gateways to Active LSPs? to **n** on the system-parameters ip-options screen. For more information about SRPF, see *Administering Avaya Aura® Communication Manager*.

status nr-registration all-regions

Use **status nr-registration all-regions** to view the status of the network regions.

Syntax

```
status nr-registration all-regions
```

all-regions Status of all network regions.

status nr-registration all-regions field descriptions

Field	Description
NR	Displays the network region number.

Table continues...

Field	Description
St	Displays the status of a network region. The following are the available values for a network region: • en — network region is enabled • rd — network region manually disabled • prd — pending manual disable • pen — pending manual enable • pa — pending auto-enable • pad — pending auto-disable • ad — network region auto-disabled

status nr-registration network-region

Use **status nr-registration network-region** to view the link status of the gateways in a specific network region.

Syntax

```
status nr-registration network-region x
```

network-region x Network region number.

status nr-registration network-region field descriptions

Field	Description
MG	Displays the gateway number.
St	Displays the status of a gateway. The following are the possible values for the link status of a gateway: • n — not registered • y — gateway is registered • p — attempting to fallback from a Survivable Remote Server or other backup server • rd — network region disabled, link status unknown • ad — the region is auto-disabled, link status unknown • ap — the region is auto-disabled and the gateway is attempting to fallback from a Survivable Remote Server or other backup server

* Note:

If the status of all the gateways is in a **p** or **ap** state, the gateways fall back to the server according to the recovery rules. The user can run **enable mg-return** to enable the gateways to register to the network regions immediately. This command allows the user to override any recovery rules including the case where none are defined. The command has two arguments: all and network-region NR-num.

status nr-registration survivable-processor node-name

Use **status nr-registration survivable-processor node-name** to view the link status of the gateways using a survivable processor.

If the Split Registration Prevention Feature (SRPF) is enabled, a survivable processor, which can either be a Survivable Remote Server or a Survivable Core Server acting as a Survivable Remote Server, can cover multiple network regions. **status nr-registration survivable-processor node-name x** displays the status of all the gateways for all the network regions on the server.

Syntax

```
status nr-registration survivable-processor node-name x
```

x Node name of the survivable processor.

status nr-registration survivable-processor node-name field descriptions

Field	Description
MG	Displays the gateway number.
St	Displays the status of a gateway. The following are the possible values for the link status of a gateway: • n — not registered • y — gateway is registered • p — attempting to fallback from a Survivable Remote Server or other backup server • rd — network region disabled, link status unknown • ad — the region is auto-disabled, link status unknown • ap — the region is auto-disabled and the gateway is attempting to fallback from a Survivable Remote Server or other backup server

 Note:

If the status of all the gateways is in a **p** or **ap** state, run **enable mg-return** to enable the gateways to register to the network regions.

options

set options

Use **set options** to administer the levels of alarm reporting.

Syntax

```
set options
```

set options field descriptions

Field	Description
Major	Set the alarm reporting type for the following major alarms: • On-board station alarms • Off-board station alarms • On-board trunk alarms (Alarm group 1) • Off-board trunk alarms (Alarm group 1) • On-board trunk alarms (Alarm group 2) • Off-board trunk alarms (Alarm group 2) • On-board trunk alarms (Alarm group 3) • Off-board trunk alarms (Alarm group 3) • On-board trunk alarms (Alarm group 4) • Off-board trunk alarms (Alarm group 4) • On-board adjunct link alarms • Off-board adjunct link alarms • Off-board DS1 alarms • Off-board TCP/IP link alarms • Off-board alarms (other)

Table continues...

Field	Description
Minor	Set the alarm reporting type for the following minor alarms: • On-board station alarms • Off-board station alarms • On-board trunk alarms (Alarm group 1) • Off-board trunk alarms (Alarm group 1) • On-board trunk alarms (Alarm group 2) • Off-board trunk alarms (Alarm group 2) • On-board trunk alarms (Alarm group 3) • Off-board trunk alarms (Alarm group 3) • On-board trunk alarms (Alarm group 4) • Off-board trunk alarms (Alarm group 4) • On-board adjunct link alarms • Off-board adjunct link alarms • Off-board MASI link alarms • Off-board DS1 alarms • Off-board TCP/IP link alarms • Off-board alarms (other) • Off-board ATM network alarms

Alarm reporting options

Option	Description
Minor	Alarms are raised as maintenance testing discovers them and the severity of the alarm is upgraded or downgraded to a minor. Alarmed resources that are normally taken out of service are still taken out of service. LEDs on the port board and maintenance board follow the normal minor alarm LED strategy and there is a call to the receiving OSS.
Warning	Alarms are raised as maintenance testing discovers them, and the severity of the alarm is downgraded to a warning. The advantage is that the Alarm Log can still be used to pinpoint trunk or station problems. Alarmed resources that are normally taken out-of-service are still taken out-of-service. Alarm LEDs light on the media module pack and Maintenance media module as before, but no attendant LEDs or stations reporting alarms are affected. There is no call to INADS.
Report	Downgrade the alarm to a warning and report the warning to INADS. This is not supported by Avaya.

Table continues...

Option	Description
Yes	Alarms are raised in the normal manner. There is no filtering of alarm data.
No	Alarms raised on a trunk, station, or adjunct in this category are dropped. Error information is provided, but there is no trace of an alarm. There is no LED activity and no call to INADS. Because resources are taken out-of-service without any record, you must use this option only when other options do not provide the desired result.

off-pbx-telephone

status off-pbx-telephone station

Use **status off-pbx-telephone station** to see the service state and connected ports of an Extended Access (off-PBX and on-PBX) station.

 Note:

The on-PBX station support only applies to One-X application types.

Extended Access applications include:

- Extension to Cellular
- Cellular Service Provider (CSP)
- Session Initiation Protocol (SIP)
- Seamless Converged Communications Across Network (SCCAN)
- Avaya One-X® Client Enablement Services (Avaya One-X® CES)

Syntax

```
status off-pbx-telephone station x
```

x Station extension.

status off-pbx-telephone station field descriptions

Field	Description
No.	The order in which the Extension to Cellular, EC500 application was administered on the Stations with Off-PBX Telephone Integration (add off-pbx-telephone station-mapping) screen.
Type	The type of Extended Access application.

Table continues...

Field	Description
Trunk/Member Group	The number of the Trunk Group and Trunk Group member associated with the station. If there is no active outside call, the message appears: No trunks associated with this off-pbx telephone station
Port	The port connected to the physical station. This physical station is mapped to an Extended Access telephone such as a cellular phone.
Connected Ports	The connected ports of Extended Access calls.

list off-pbx-telephone station-mapping

Use **list off-pbx-telephone station-mapping** to see the application associated with administered stations.

Syntax

```
list off-pbx-telephone station-mapping x[count n] [schedule]
```

x is phone number or the partial phone number followed by '*'.

count n An optional parameter to specify the number of stations that you want the system to display.

schedule An optional parameter to print the output.

list off-pbx-telephone station-mapping field descriptions

Name	Description
Station Extension	The extension assigned to the user.
Appl	The type of application used for mapping the OPTIM station to off-PBX telephone and on-PBX telephone. • CSP - Mobile phone with Extension to Cellular provided by the cellular service provider • EC500 - Mobile phone with Extension to Cellular • HEMU - Home Enterprise Mobility User • OPS - SIP Enablement Services (SES) enabled phone • PBFMC - Public Fixed Mobile Convergence • PVFCM - Private Fixed Mobile Convergence • SCCAN - Wireless SIP Enablement Services (SES) phone and mobile phone • VEMU - Visited Enterprise Mobility User • VIEMU - Visited Initial Enterprise Mobility User • One-X - Avaya one-X® Client Enablement Services

Table continues...

Name	Description
CC	The country code associated with the off-PBX telephone.
Phone Number	The phone number of the off-PBX telephone or the extension of the on-PBX telephone.
Config Set	The configuration set used for mapping. This field can be blank if not administrable.
Trunk Select	The trunk group that connects to the off-PBX telephone or the extension when applicable for the on-PBX telephone.
Mapping Mode	The direction of calls on off-PBX and on-PBX telephones. The mapping mode on on-PBX telephones is always set to termination-only.
Calls Allowed	The number of simultaneously active calls on the off-PBX telephone.

For more information, see *Avaya Aura® Communication Manager Screen Reference*.

periodic-scheduled

status periodic-scheduled

Use **status periodic-scheduled** to see summary information about currently active and recently completed background testing. Periodic tests run every hour, and scheduled tests run daily. Starting and stopping times, and other parameters for daily scheduled testing, are administered with **change system-parameters maintenance**.

Syntax

```
status periodic-scheduled
```

status periodic-scheduled field descriptions

Field	Description
PERIODIC MAINTENANCE section	This data reflects the status of periodic maintenance which is performed hourly, according to the selections made on the change system-parameters maintenance screen. See <i>Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers</i> for more information.
Pre-SCHEDULED MAINTENANCE section	The data in this section reflects the status of pre-scheduled maintenance. Pre-scheduled maintenance can include interchanges of duplicated components and backup of translation data. It is performed according to selections made on the change system-parameters maintenance screen.

Table continues...

Field	Description
SCHEDULED MAINTENANCE section	The data in this section reflects the status of scheduled maintenance which is performed daily. Scheduled maintenance is performed according to the selections made on the change system-parameters maintenance screen.
System Critical	System-critical resources are those whose health affects the entire system such as the processor. These are always tested first.
Shared Resource	Shared resources are those that are used by many users, such as trunks. These are tested after system critical resources.
Single User	Single-user resources are those whose health affects only one user, such as voice stations.
Total	Total duration of previous periodic or scheduled maintenance cycle. Note: Scheduled maintenance total does not include pre-scheduled maintenance duration.
Current Cycle % Complete	The ratio of the number of maintenance objects tested to the total number of maintenance objects tested during a cycle. For periodic tests, the ratio is for the current cycle, if active; or for the last completed cycle if not. For scheduled tests, the ratio is for the last completed cycle.
Current Cycle Active	Reflects whether the current cycle of periodic, pre-scheduled or scheduled maintenance is currently running. Value is <code>y</code> if currently running or <code>n</code> if it is not.
Previous Cycle Duration	Reflects how long the system critical, shared resource, or single user maintenance activities took for the previous cycle of maintenance.
Rate of Completed Cycles	Reflects how often maintenance cycle is performed.
Start Time of Current or Previous Cycle	Time at which maintenance cycle began in <i>month/day/hour:minute:second</i> format. For scheduled maintenance, this time reflects when the pre-scheduled maintenance began.

pin

change pin

Use **change pin** to change the PIN for the dadmin login or for the second craft login. The PIN should be a minimum of seven characters and a maximum of 32 characters. You can use only upper and lower case characters, numbers, and special characters. PINs do not expire. PINs must conform to the minimum and maximum lengths and must contain at least one letter and one number. PINs are not displayed when typed on the screen or when changed.

The dadmin and init logins can change the PIN for dadmin or the second craft login.

The second craft login can change the PIN for only the second craft login.

Syntax

```
change pin [dadmin] | [second craft login name]
```

dadmin	The dadmin login.
<i>second craft login name</i>	The craft2 login.

reset pin

The **reset pin** command resets the PIN for the dadmin login or the second craft login. The old PIN is not required. When a PIN is reset, it returns to the state where the PIN must be re-created on the next SAT access. The PIN of the second craft login can be changed but cannot be reset to an uninitialized value.

The command is accessible only to the init and dadmin logins, and either login may reset the PIN. When the command is typed, the system displays the `Command completed successfully` message.

Syntax

```
reset pin [dadmin] | [second craft login name]
```

dadmin	The dadmin login.
<i>second craft login name</i>	The craft2 login.

ping

ping

When debugging connectivity problems, **ping** command helps to indicate the low-level connectivity. If an external ping works but higher-level applications such as DCS, CMS, or INTUITY do not, there is probably low-level connectivity to the board. Interrogate the switch for other clues as to why the higher-level application is not working.

The ping command checks low-level connectivity between the two IP-connected peers: a destination and a source.

- The destination can be:
 - an IP address (ip-address addr)
 - a node (node-name name)
- The source can be:
 - a Softphone, IP telephone, or Remote Office (R300) telephone (source port-id).

Use this test to check the circuitry in the data path for a peer-to-peer IP layer connection. This test is nondestructive.

 Caution:

Repeated ping tests can consume a lot of bandwidth and can bog down a network. If the network is already loaded, a ping test can fail even if there is a connectivity between the source and the destination.

The two ping command options are as follows:

- ip-address
- node-name

The syntax for both the commands are as follows:

Syntax 1

```
ping ip-address
```

Syntax 2

```
ping node-name name [ source port-id ] [ packet-length len ] [ repeat # ]
```

IP Address to ping Specify a valid IPv4 or IPv6 address of the device to ping.

node-name name The name of the node to ping. Use **display node-names ip** to see what IP nodes are administered.

source port-id The virtual endpoint port ID to use as the source of the ping. This can be the virtual endpoint port ID of a softphone, IP telephone, or Remote Max (R300) telephone. Use **status station ext** to determine the virtual endpoint port ID of a telephone.

packet-length len The packet length of the ping packet, from 64 to 1500. If packet-length is not given, the default packet length is 64 bytes. Specifying a longer packet length in the command line can show:

- if a router or host has a problem fragmenting or reassembling transferred packets.
- a more complete indication of the link status.

repeat # The number of times to repeat the **ping** test. See **Caution** above before using.

ping field descriptions

Field	Description
End-pt IP or End-pt Node-name	The destination of the ping command.
Port	The slot or port of the source.
Port Type	The maintenance object name of the source.
Result	PASS, FAIL, or ABORT.

Table continues...

Field	Description
Time (ms)	The round-trip time (in milliseconds) of the ping.
Error Code	Identifies problems associated with the circuitry in the data path for a peer-to-peer IP layer connection. For the meaning of the error code and troubleshooting procedures, see the Port Type's maintenance object description in the <i>Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> . The MO description indicates the type of ping test used and the meaning of that ping test's error codes.

Error messages

Message	Description
www.xxx.yyy.zzz IP address not assigned	The system cannot find the IP address.
IP address not reachable from this board	The IP address is not in the route table of the specified board.
"xxxx" Invalid IP address	Invalid IP address parameter. Must be in www.xxx.yyy.zzz format.
"CCcss" is an invalid identifier; please press HELP	Invalid board location (when using board).
Error encountered, could not complete request	An internal error, the port through which the IP address is reached could not be found.
Invalid range	The packet size is greater than 1500 or less than 64 bytes in length, or there are invalid or unrecognized parameters.

Example

```
ping ip-address 192.68.3.26
ping ip-address 2001:0db8:3333:4444:5555:6666:7777:8888
ping ip-address 192.68.3.26 board 1C05
ping ip-address 168.24.3.66packet-length 1500
```

pms-down

list pms-down

Use **list pms-down** to see every event that has meaning to the Property Management System (PMS) that has occurred while the link between the switch and the PMS was down. For example, room status codes entered by hotel housekeeping staff during a PMS outage is displayed in this report.

Syntax

```
list pms-down [ start-time ] [ stop-time ]
```

start-time The starting time in 24-hour notation from which events are to be listed.

stop-time The time in 24-hour notation up to which events are to be listed.

list pms-down field descriptions

Field	Description
Extension	The extension associated with the reported event.
Event	The PMS event that was reported to the switch, but which could not be sent to the PMS.
Reason	The reason that the event could not be reported by the switch to the PMS.
Time	The time at which the event was reported.

pms-link

busyout pms-link

Use **busyout pms-link** to place every maintenance object associated with a property management system link in the maintenance busy state. No periodic or scheduled maintenance is performed on the busied out maintenance objects until they are released. When the object is maintenance busy the object is deactivated (no call processing activity may include the busied object) and the link is dropped. Warning alarms (error type 18) are generated on each busied out maintenance object, so that the Initialization and Administration System (INADS) can determine the state of the objects. Use **release pms link** to reactivate the busied out objects on the link.

These links provide asynchronous data connections from switches to peripherals, and they are composed of the following:

- Far-end data module
- Simulated data channel
- Manager that initiates and maintains the link
- Controller/protocol that services the link

For information about what a property management system (PMS) is and what it does, see **status pms-link**. See **status link** for more details on links.

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

Syntax

```
busyout pms-link
```

release pms-link

Use **release pms-link** to reactivate the busied out maintenance objects on the property management system (PMS) link. The **busyout pms-link** command places all maintenance objects associated with a PMS link in the maintenance busy state. Once released, periodic and scheduled maintenance can be performed on the maintenance objects.

See Busyout and Release Commands. See **status link** for more details on links.

Use **release pms-link** to deactivate MOs that are associated with a property management system link. These links provide asynchronous data connections from switches to peripherals; they are composed of a

- Far end data module
- Simulated data channel on a NETCON board
- Manager that initiates and maintains the link
- Controller/protocol that services the link

Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

Syntax

```
release pms-link
```

status pms-link

Use **status pms-link** to see the status of the property management system interface link.

Status of the property management link will be up, a data base swap is taking place between the switch and PMS. If the link is down, the number of attempts made to set up the link is displayed. A property management system (PMS) is a stand alone computer system that can be integrated with the switch to enhance the service capability for a hotel/motel.

For general information on PMS links, see **busyout pms-link**. See **status link** for more details on links.

Syntax

```
status pms-link
```

status pms-link field descriptions

Field	Description
Physical Link State	up, down, extension not administered. The PMS link is listed as administered if an extension is given in the System Hospitality screen.
Protocol State	up, down The state of the Procor. Blank if not administered.
Number of Retries	Number of times the switch has tried to set up the link. Displayed when the link is down.
Maintenance Busy	y, n If y, maintenance testing is being performed on the link.

test pms-link

Use **test pms-link** to verify that the link to the Property Management System (PMS) is administered and performs a series of tests on the link.

See **status pms-link** for information about the PMS and interpreting its status. See **busyout pms-link** for information on PMS links. See **status link** for more details on links.

Syntax

```
test pms-link [ short | long ] [ repeat # | clear ] [ schedule ]
```

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

 Note:

Specific component maintenance performed on a link sometimes conflicts with link maintenance, because busied-out objects create link setup failure. Frequent link re-setup attempts may delay component recovery. For best results, busyout the link to disable attempted link re-setup.

port

busyout port

Use **busyout port** to busyout a specified port on a media module.

Syntax

```
busyout port location
```

location port address (PCSS)
 marked port: PPSSpp

Busyout port location on a specific SIP B-channel:

- drops any active call that exists on the B-channel
- reduces the trunk group's capacity by one
- the physical piece of hardware is removed from service

Example

```
busyout port 001v201
busyout port 010v404
```

clear port

Use **clear port** to remove marks from ports and free the ports for service. **clear port** works with **mark port**.

Syntax

```
clear port location
```

location Port location: PCSSpp.

Example

```
clear port 001v201
```

display port

Use **display port** to see a port's equipment type and identification number.

Syntax

```
display port location [ schedule ]
```

location Address of the port.

schedule Specify a time to run the command.

Example

```
display port
001v201
```

display port field descriptions

Field	Description
Port	Port address location
Equipment Type	Type of hardware that is physically connected to the specified port, or TTI port for a telephone in a TTI state. Softphone Restore Port — soft phone registration originated from this port. No new extensions can be assigned to this port location. Use list registered-ip-stations for more information on the IP soft phone extension assigned to this port.
Identification	Depending on the equipment type, identifies: • extension • trunk group number and member number • modem pool group number • IP address of an IP telephone that is in TTI state

mark port

Use **mark port** to make a port unusable by normal call processing. The port can be tested but calls are not attempted through the port. A marked port is saved as part of translation. Use **clear port** to restore the port to service.

Syntax

```
mark port location
```

location Location of the port to be marked.

Example

```
mark port
001v701
```

release port

Use **release port** to activate specified ports on media module.

For more information see Busyout and Release Commands.

Syntax

```
release port location
```

location Physical location of the port, PCSS.

Release port location on a specific SIP B-channel:

- increases the trunk group's capacity by one
- the physical piece of hardware is added to service.

test port

Use **test port** to perform hardware diagnostic tests on an individual port circuit. Usually, tests are performed on hardware connected to the port.

Syntax

```
test port location [ long | short ] [ repeat n | clear ]
```

location Location of the port, PCSSpp.

long Run the long test sequence.

short Run the short test sequence.

repeat # (Optional) The number of times to repeat the command. The default is 1.

clear Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Example

```
test port 001v701 1
```

Warning:

Because **test port location clear long** clears all counters if tests pass, firmware counters may be cleared even when a problem exists. Sometimes customer service may degrade because calls may be routed over defective equipment.

pri-endpoint

busyout pri-endpoint

Use **busyout pri-endpoint** to busyout all PRI endpoint ports (B-channels) associated with the specified PRI endpoint.

Syntax

```
busyout pri-endpoint extension #
```

extension # PRI endpoint extension number.

busyout pri-endpoint feature interactions

Active calls on busied out PRI endpoints are dropped.

Call attempts from far-end PRI terminal adapters are denied with a cause value of 17.

release pri-endpoint

Use **release pri-endpoint** to remove PRI endpoint ports (B-channels) associated with specified PRI endpoint from maintenance busy states. Periodic and scheduled tests resume on released ports. The switch attempts to negotiate with the far-end PRI terminal adapter activating PRI endpoint port (B-channel). Maintenance does background initialization testing on released ports.

Syntax

```
release pri-endpoint extension #
```

extension # PRI endpoint extension number.

status pri-endpoint

Use **status pri-endpoint** to display the internal software state information for diagnosis and to help locate facilities with which a PRI endpoint is communicating. Status information for each of the B-channels which make up the PRI endpoint is displayed in addition to some overall PRI endpoint information.

Syntax

```
status pri-endpoint extension #
```

extension # PRI endpoint extension number.

* Note:

A PRI endpoint can initiate and receive a call on any one or more of the B-channels making up the PRI endpoint.

Example

```
status pri-endpoint 25012
status pri-endpoint 77868
```

status pri-endpoint field descriptions

Field	Description
Extension	PRI endpoint extension.
Width	Administered number of B-channels associated with the specified PRI endpoint.
Signaling Group ID	ID number of the signaling group that handles the signaling for the ports in the specified PRI endpoint.

Table continues...

Field	Description
Originating Auto Restoration	Administered option for the auto restore feature (restores calls originated from this PRI endpoint in the case of network failure): • y — restoration option enabled • n — restoration option disabled
B-Channels Active	The number of B-channels active on a call
B-Channels Idle	The number of B-channels in the in-service/idle state
Port	Port locations (cabinet-carrier-slot-circuit) for each of the B-channels making up the PRI endpoint.
Service State	Service state of the B-channels: • in-service/active • in-service/idle • out-of-service-NE • out-of-service-FE • maint-NE/active • maint-FE/active • maint-NE/idle • maint-FE/idle NE (Near End) and FE (Far End) refer to which end of the B-channel has placed the facility in the current state. NE refers to the switch and FE refers to the PRI terminal adapter (or any device that terminates the D-channel signaling on the facility).
Test In Progress	Whether or not there is any current maintenance testing on the port.
Connected Port	Connected port location (cabinet-carrier-slot-circuit) for each of the B-channels active on a call.

test pri-endpoint

Use **test pri-endpoint** to perform hardware diagnostic tests on all port circuits (B-channels) that are associated with the specified PRI endpoint.

Syntax

```
test pri-endpoint extension # [ short | long ] [ repeat # | clear ]
```

extension # PRI endpoint extension to be tested (must conform to dial-plan).

short Run the short test sequence.

long Run the long test sequence.

repeat # (Optional) The number of times to repeat the command. The default is 1.

clear Repeat the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

Example

```
test pri-endpoint 25012
test pri-endpoint 45002 sh
test pri-endpoint 45892 l
test pri-endpoint 24389 sh r 2
test pri-endpoint 34899 l r 6
```

profile-base

display profile-base

Use **display profile-base** to see the Linux Group number that corresponds to Communication Manager user profile 0.

The screen name is User Profile Base.

Syntax

```
display profile-base
```

display profile-base field descriptions

Field	Description
Profile Base	Linux Group number that corresponds to Communication Manager user profile 0. Profile Base default number is 10000.

psa

status psa

Use **status tti** to see the TTI/PSA status screen and check if the TTI background maintenance task is active. If the TTI background maintenance task is active, the screen shows whether TTI ports are being generated or removed, the number of TTI-supported boards that have been processed, and the number of TTI-supported boards that have not yet been processed. The screen also shows the elapsed time since the background maintenance task started.

To activate the TTI background maintenance task, enter **y** in the TTI field on the Feature-Related System-Parameters screen.

Use **status psa** to also see the TTI/PSA status screen. It shows that the status of PSA is dependent on the state of TTI.

Syntax

`status psa`

status psa field descriptions

Field	Description
TTI Background Task State	• generating TTI ports • removing TTI ports • suspended • not active • completed – all ports translated — The last background maintenance task completed normally. • completed – some ports not translated — The last background maintenance task stopped when resources were exhausted, and some ports were not translated.
TTI State	off — TTI is disabled voice, data shows the type of TTI ports that are being generated or removed.
media modules completed	Number of TTI-supported media modules that were processed by the background maintenance task. The ports on a completed media module: • if unadministered, were translated as TTI ports • if administered, the administration was removed
# of media modules left to process	The number of TTI-supported media module that were not processed by the background maintenance task.
Percent Complete	Ratio of the of number of media modules completed to the total number of media module.
Elapsed Time Since Task Started	Elapsed time in <i>hours:minutes:seconds</i> since the TTI background task was started. This field is blank if the task is not active. If the task is completed or suspended, this field shows the elapsed time up to when the job finished or was suspended.

public-unknown-numbering

change public-unknown-numbering

Use `change public-unknown-numbering` to administer the desired digits for name and number display on display-equipped stations in an ISDN network.

Syntax

```
change public-unknown-numbering n [ ext-digits x ][ trunk-group # ]
```

n Number of digits (extension length, Ex-Len) in the extension being administered.
Enter 0 for attendant.

ext-digits x First extension on the screen.

trunk-group # The trunk-group option displays valid results only when used in conjunction with the ext-digits option. Otherwise, an error message is returned.

See *Administering Avaya Aura® Communication Manager* for a screen example and field descriptions, and for more information on ISDN Call Identification Display and Numbering-Public/Unknown.

Example

```
change public-unknown-numbering 5change public-unknown-numbering 5 ext-digits 10010
```

display public-unknown-numbering

Use **display public-unknown-numbering** to see the administration for name and number display on display-equipped stations in an ISDN network.

Syntax

```
display public-unknown-numbering n [ ext-digits x ]
```

n Number of digits (extension length, Ex -Len) in the extension being administered.
Enter 0 for attendant.

ext-digits x First extension on the screen.

Example

```
display public-unknown-numbering 5
display public-unknown-numbering 5 ext-digits 10010
```

list public-unknown-numbering

Use **list public-unknown-numbering** to list all entries in the public-unknown-numbering table, used to specify desired digits for name and number display on display-equipped stations in an ISDN network.

Syntax

start n Starting point for the extension digits you want to see.

ext x The first extension on the screen.

count *n* Number of output lines.

list public-unknown-numbering field descriptions

Field	Description
CPN Prefix	The number that is added to the beginning of the extension to form a Calling or Connected Number. • blank — the extension is sent unchanged. Use in countries where the public network is able to insert the appropriate CPN Prefix to form an external DID number. • If the CPN Prefix length matches the Total CPN Len, the extension number is not used to formulate the PN number. • If the CPN Prefix length plus the extension length exceeds the Total CPN Len, excess leading digits of the extension are deleted when formulating the CPN. • If the CPN Prefix length plus the extension length is less than the Total CPN Len, the entry is not permitted • If the Total CPN Len is 0, no calling party number information is provided to the called party and no connected party number information is provided to the calling party.
Ext Code	Can be up to 7 digits, but cannot be greater than the Ext Len field. • attd — attendant • 0 — Ext Len field must be 1 and the DDD number must be 10 digits • 0 to 9 or blank Example: When Ext Len is 4, Ext Code of 12 represents all extensions of the screen 12xx, excluding any explicitly listed longer codes. If code 123 is also listed, the Ext Code 12 represents all extensions of the screen 12xx except extensions of the screen 123x.
Ext Len	Number of digits for the extension, as entered on the command line (list public-unknown-numbering n).
Total CPN Len	Total number of digits to send. 0 — no calling party number information is provided to the called party and no connected party number information is provided to the calling party.
Trk Grp(s)	Number of the ISDN trunk group carrying the call, or the range of trunk groups that use the same CPN Prefix. blank — IEs are not dependent on which trunk group carries the call.

registered-ip-stations

list registered-ip-stations

Use **list registered-ip-stations** to see specific information about registered ip stations. Sort registered ip-station information by:

- gatekeeper address
- network region
- product ID
- station type
- TCP socket registration

Syntax

```
list registered-ip-stations [all] [v4] [v6] [ext x] [type x] [id x] [release x] [region x] [port x] [gatekeeper x] [tcp y | n] [authenticated x] [count n]
```

all	Displays the v4 and v6 registered IP stations.
v4	Displays the v4 registered IP stations.
v6	Displays the v6 registered IP stations.
ext x	Extension number of the registered stations.
type x	Administered set type (xxxxxx).
id x	Product type (x.yyy) of the registered extension.
release x	Release number of the registered stations.
region x	Network region of the registered stations.
port x	Port number of the registered stations.
gatekeeper x	Processor's IP address (xxx.xxx.xxx.xxx).
tcp y n	TCP signaling socket registration established.
authenticated x	Displays the V4 and V6 registered IP stations.
count n	Number of stations to list.

list registered-ip-stations field descriptions

Field	Description
	For shared-control endpoints (an IP telephone and IP soft phone are in service on the same extension simultaneously), both endpoints register. The records for each endpoint are displayed vertically adjacent to each other.
Station Ext or Orig Port	First line: Station extension number. Second line: Port number assigned to the extension that is now under the control of the specified endpoint, for example, a soft phone. For an IP endpoint, this is the circuit-switched port that was assigned to this extension number before the IP endpoint registered to the extension. For a shared-control extension where the Telephone is a DCP set, this is the port of the shared-control's DCP set. If a soft phone is not taking over a DCP set, no second line is displayed.
Set Type	Administered set type for the extension.
Net Rgn	Network region number assigned to the endpoint.
Prod ID	Product ID of the registered endpoint. For example, this can be the product ID of a soft phone that is registered to a hard phone extension, and the release information, provided from the endpoint during registration.
Prod Release	Release number of the endpoint, provided from the endpoint to the gatekeeper during registration.
TCP Skt	y/n Indicates the TCP signaling socket is established for the IP station.
Station IP Address	Location of the registered station, as the processor IP address or port location.
Gatekeeper IP Address	The IP address of the server, or other device that is performing the role of the H.323 gatekeeper for this endpoint.

remote-access

status remote-access

Use `status remote-access` to see information about remote access calls.

Syntax

```
status remote-access
```

status remote-access field descriptions

Field	Description
Remote Access Status	Whether the feature is enabled or not
Barrier Code	Remote access barrier code
Date Modified	Remote access modification date
Expiration Date	Barrier code expiration date
No. of Calls	Number of calls from barrier code
Calls Used	Number of times barrier code was used
Status	Enable/disable state of remote access
Date/Time Expired	Date/time barrier code expired
Cause	Reason for the expiration

remote-office**add remote-office**

Use **add remote-office** to administer a new remote office on your system.

Syntax

```
add remote-office nn ]
```

nn The number assigned to the remote office.

add remote-office field descriptions

Field	Description
Node Name	Node Name or IP address assigned to the remote office
Network Region	Network Region number assigned to all stations supported on this remote office. This network region may be used to override the default region obtained from the Procor used for signaling to and from the stations.
Location	Location number of the remote office
Site Data	Text information specific to your company.

change remote-office

Use **change remote-office** to change the administration of a specific remote office on your system.

Syntax

```
change remote-office nn
```

nn The number assigned to the remote office.

display remote-office

Use **display remote-office** to see the information for a specific remote office administered on your system.

Syntax

```
display remote-office nn[ schedule ]
```

nn The number assigned to the remote office.

schedule Specify a time to run the command.

list remote-office

Use **list remote-office** to list all of the currently administered remote offices on the system. Information includes the remote-office number, node name, network region, location number, and IP address of the remote office.

Syntax

```
list remote-office [ schedule ]
```

schedule Specify a time to run the command.

list remote-office field descriptions

Field	Description
Node Name	Node Name assigned to the remote office
Net Region	Network Region number
Location	Location of the remote office
IP Address	IP Address of the remote office

remove remote-office

Use **remove remote-office** to remove a specific remote office from your system.

Syntax

```
remove remote-office nn
```

nn The number assigned to the remote office.

status remote-office

Use **status remote-office** to see information about a specified remote-office.

Syntax

```
status remote-office nn
```

nn The number assigned to the remote office.

status remote-office field descriptions

Field	Description
Node Name	Node Name assigned to the Remote Office
IP Address	IP Address of the node name assigned to the Remote Office
Network Region	Network Region number assigned to the Remote Office
Location	Location number for the Remote Office
Trunk Signaling Groups	Trunk Signaling Group assigned to the Remote Office
Stations Registered	Extensions of the stations on the Remote Office that are currently registered.

security-violations

monitor security-violations

Use `monitor security-violations` to view information about failed attempts to access the system.

Syntax

```
monitor security-violations [authorization-code | remote-access | station-security-codes]
```

authorization-code Monitors the number of failed attempts of accessing the system resources due to an invalid authorization code.

remote-access Monitors the number of failed attempts of dialing into the system using remote access due to an invalid barrier code or authorization code.

station-security-codes Monitors the number of failed attempts of accessing the system resources due to an invalid station security code.

Description

Use `monitor security-violations` to see the following information about failed attempts to access the system:

- the time of the violation
- trunk-group number
- member number

- extension

A total of 16 entries are maintained for each type of access. The monitor security-violations report is automatically updated every 30 seconds until the command is canceled by pressing CANCEL. Canceling does not log off the terminal.

monitor security-violations field descriptions

Field	Description
Authorization code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
Origin	The source of the call: internal or external.
Auth-Cd	The dialed authorization code.
TG No.	The trunk group involved in the security violation.
Mbr	The trunk-group member number involved in the security violation.
Bar-Cd	The dialed barrier code, if required.
Ext	The extension used to access the system.
CLI/ANI	The calling party number.
Remote access barrier code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
TG No.	The trunk group that carried the incoming remote access attempt.
Mbr	The trunk-group member number associated with the trunk from which the remote access attempt terminated.
Ext	The extension used to access the system.
Bar-Cd	The dialed barrier code, if required.
CLI/ANI	The calling party number.
Station security code violations	
Date	The date of the security violation in the MM/DD format.
Time	The time of the logged security violation in the HH:MM format.
TG No.	The trunk group involved in the security violation.
Mbr	The trunk-group member number involved in the security violation.
Port/Ext	The port or extension used to access the system.
FAC	The dialed feature access code.
Dialed digits	The dialed digits.

set-data

list set-data

Use `list set-data` to see telephone information administered from the Site Data and Station screens.

Syntax

```
action object [ schedule ]
```

schedule (Optional) Specify a start time for the command.

list set-data field descriptions

Field	Description
Ext	station extension number, administered on the Station screen
Name	name used in the system directory
Building, Floor, Room	physical location of the station
Cable	identifies the cable that connects the telephone jack to the system
Jack	identifies the jack where the telephone is plugged in
Color	color of telephone
Cord Len	length of the cord attached to the receiver
Speaker	y/n
Headset	y/n
Mounting	desk or wall
Set Type	type of telephone

shell

go shell

Use `go shell` to get SAT access to the Linux bash shell of the server.

Syntax

```
go shell
```

Description

1. Type `go shell` at the SAT command prompt and press **ENTER**.

The screen displays:

Suppress alarm origination? (y/n) [y]

2. Enter `y` to suppress alarms if you are logged into a server via an analog modem that is also the server's only alarm-reporting interface.

This prevents the other server logging an occurrence of SME Event ID #1.

3. Enter your terminal type, or press **ENTER** for the default terminal type.

The Linux prompt is displayed. It is the login and the server name followed by `>`.

4. At the Linux prompt, enter a Linux command.

signaling-group

display signaling-group

Use **display signaling-group** to see the properties of a specific signaling group, designated by the qualifier.

Syntax

```
display signaling-group x
```

x is the number of signaling group to display.

Description

Signaling groups are groups of B-Channels for which a given D-Channel (or D-Channel pair) carries the signaling information.

display signaling-group field descriptions

Field	Description
Grp No	The signaling group number
Group Type	The type of signal format (ISDN-PRI, , H.323, SIP)
Max NCA TSCs	Maximum number of Non-Call Associated (NCA) Temporary Signaling Connections (TSCs) - virtual connections established within a D-Channel in the facility so that users can transport non-call control user-user information.
Max CA TSCs	Maximum number of Call Associated (CA) TSCs.
Remote Office	The number of NCA TSCs that are administered.
Trunk Group for NCA TSC	The ISDN-PRI trunk group number whose incoming call-handling table handles incoming NCA-TSCs through this signaling group
Trunk Group for Channel Selection	If more than one trunk group is assigned to this signaling group, this trunk group is the one that can accept incoming calls

Table continues...

Field	Description
TSC Supplementary Service Protocol	This field is displayed when trunk Group Type is ISDN, and for signaling group types , H.323, and ISDN-PRI. a = AT&T Customer Supplementary Services when Country Code is 1A on the DS1 screen. a = Bellcore Supplementary Services when Country Code is 1B on the DS1 screen a = Nortel Proprietary Supplementary Services when Country Code is 1C on the DS1 screen. b = ISO Q SIT c = ETSI. Use to support ETSI-ISDN Completion of Calls (Auto Callback) functionality. d = ECMA QSIG e allows DCS with rerouting, when DCS with Rerouting is y, and Used for DCS on the trunk group screen is y. f = Feature Plus g = ANSI.
T303 Timer (sec)	The number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. Displayed when the Group Type field is isdn-pri on the DS1 Media Module screen or h.323 on the Signaling Group screen.
Near-end Node Name	The node name for the Procor interface on this switch, administered on the Node Names screen and the IP Interfaces screen.
Far-end Node Name	The node name for the far-end Procor interface used for trunks assigned to this signaling group, administered on the Node Names screen.
Near-end Listen Port	A port number assigned to both near-end and far-end systems for signaling. 1719 is used when LRQ is y.
Far-end Listen Port	The same port number assigned to the near-end listen port.
Far-end Network Region	The network region number that is assigned to the far-end of the trunk group. It is displayed only for H.323 signaling groups. A blank indicates the region of the near-end node
LRQ Required	n when the far-end PBX uses a Communication Manager server y when the far-end PBX uses a server that is not a Communication Manager server, and requires a location request to obtain a signaling address in its signaling protocol
RRQ Required	y when the signaling group serves a remote office (gateway) n when the signaling group serves a gatekeeper
Calls Share IP Signaling Connection	y = inter-Communication Manager server connections n = the local and/or remote PBX uses a non-Avaya server.

Table continues...

Field	Description
Bypass if IP Threshold Exceeded?	y = the system automatically removes from service trunks assigned to this signaling group, when IP transport performance falls below limits administered on the Maintenance-Related System-Parameters screen.
Direct IP-IP Audio Connection	y enables direct audio connections between IP endpoints, and saves on bandwidth resources and improves sound quality of VoIP transmissions.
Interworking Message	Determines what message the switch sends when an incoming ISDN trunk call interworks (is routed over a non-ISDN trunk group). PROGress causes the public network to cut through the B-channel and enable the caller to hear tones, such as ringback or busy tone, over the non-ISDN trunk. ALERTing causes the public network in many countries to play ringback tone to the caller. Select this value if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk.

list signaling-group

Use **list signaling-group** to see a list of signaling groups, which are groups of B-Channels for which a given D-Channel (or D-Channel pair) will carry the signaling information.

Syntax

```
list signaling-group count x
```

count x The number of signaling groups to be displayed.

Example

```
list signaling-group count 6
```

list signaling-group field descriptions

Field	Description
Grp No	The signaling group number
Group Type	The type of signal format (ISDN-PRI, H.323)
FAS	Facility Associated Signaling (FAS), in which a D-Channel carries signaling information for only those B-Channels on the same facility as the D-Channel. This is identical to a DS1 interface. If the parameter is "n", this is referred to as Non-Facility Associated Signaling (NFAS), in which a B-Channel can belong to any signaling group as long as the maximum number of DS1's for a signaling group is not exceeded.
No. Trunk Brds	The number of trunk boards having members belonging to this signaling group

Table continues...

Field	Description
Primary D-Channel	The D-Channel administered to be the primary channel. If, during the backup procedure, both channels are in the same state, switches at opposite ends of the PRI select the primary D-Channel to be put into service.
Secondary D-Channel	This channel will only display if the signaling group is an NFAS signaling group. This D-Channel is administered to be the secondary D-Channel. If, during the backup procedure, both channels are in the same state, switches at opposite ends of the PRI select the primary D-Channel to be put into service.
Max NCA TSCs	Maximum number of Non-Call Associated (NCA) Temporary Signaling Connections (TSCs) — virtual connections established within a D-Channel in the facility so that users can transport non-call control user-user information.
Max CA TSCs	Maximum number of Call Associated (CA) TSCs.
No. Adm'd NCA TSCs	The number of NCA TSCs that are administered.

list usage signaling-group

Use the **list usage signaling-group** command to display the specific media server, which uses the signaling-group.

The command displays who is using a signaling-group. If the signaling-group is used by a media-server, it displays Used By Media-Server Server-Number X.

Syntax

```
list usage signaling-group xx
```

xx is an integer ranging from 1–999 that indicates the number of the signalling group for which the usage report is displayed.

```
list usage signaling-group 22
```

```

                                LIST USAGE SIGNALING-GROUP REPORT
Used By
Trunk Group      Group Number      198      Trunk Member 18
Trunk Group      Group Number      198      Trunk Member 19
Trunk Group      Group Number      198      Trunk Member 20
Trunk Group      Group Number      198      Trunk Member 21
Trunk Group      Group Number      198      Trunk Member 22
Trunk Group      Group Number      198      Trunk Member 23
Media Server     Media Server Number    1
```

Command successfully completed

list usage signalling-group field description

Field	Description
Group Number	The signalling group number
Used by	The type of server that is using the signalling-group
Trunk Member	The number of Trunk member

remove signaling-group

Use the **remove signaling-group** command to remove the signaling-group.

If the **signaling-group** type is SIP and the **Peer Server** is set to Avaya Aura® Media Server (MS), and the **Signaling Group** is administered on a media-server form, then:

- The **Signaling Group** field on the media-server form must be changed to some other **signaling-group** value.
- The media-server must be removed before the **remove signaling-group** command is executed.

Syntax

```
remove signaling-group x
```

x is integer range from 1–999 that indicates the signaling-group to be removed.

remove signaling-group field descriptions

Field	Description
Grp No	The signaling group number
Group Type	The type of signal format (ISDN-PRI, , H.323, SIP)
Max NCA TSCs	Maximum number of Non-Call Associated (NCA) Temporary Signaling Connections (TSCs) - virtual connections established within a D-Channel in the facility so that users can transport non-call control user-user information.
Max CA TSCs	Maximum number of Call Associated (CA) TSCs.
Remote Office	The number of NCA TSCs that are administered.
Trunk Group for NCA TSC	The ISDN-PRI trunk group number whose incoming call-handling table handles incoming NCA-TSCs through this signaling group
Trunk Group for Channel Selection	If more than one trunk group is assigned to this signaling group, this trunk group is the one that can accept incoming calls

Table continues...

Field	Description
TSC Supplementary Service Protocol	This field is displayed when trunk Group Type is ISDN, and for signaling group types , H.323, and ISDN-PRI. a = AT&T Customer Supplementary Services when Country Code is 1A on the DS1 screen. a = Bellcore Supplementary Services when Country Code is 1B on the DS1 screen a = Nortel Proprietary Supplementary Services when Country Code is 1C on the DS1 screen. b = ISO Q SIT c = ETSI. Use to support ETSI-ISDN Completion of Calls (Auto Callback) functionality. d = ECMA QSIG e allows DCS with rerouting, when DCS with Rerouting is y, and Used for DCS on the trunk group screen is y. f = Feature Plus g = ANSI.
T303 Timer (sec)	The number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. Displayed when the Group Type field is isdn-pri on the DS1 Media Module screen or h.323 on the Signaling Group screen.
Near-end Node Name	The node name for the Procor IP interface on this switch, administered on the Node Names screen and the IP Interfaces screen.
Far-end Node Name	The node name for the far-end Procor IP interface used for trunks assigned to this signaling group, administered on the Node Names screen.
Near-end Listen Port	A port number assigned to both near-end and far-end systems for signaling. 1719 is used when LRQ is y.
Far-end Listen Port	The same port number assigned to the near-end listen port.
Far-end Network Region	The network region number that is assigned to the far-end of the trunk group. It is displayed only for H.323 signaling groups. A blank indicates the region of the near-end node
LRQ Required	n when the far-end PBX uses a Communication Manager server y when the far-end PBX uses a server that is not a Communication Manager server, and requires a location request to obtain a signaling address in its signaling protocol
RRQ Required	y when the signaling group serves a remote office (gateway) n when the signaling group serves a gatekeeper

Table continues...

Field	Description
Calls Share IP Signaling Connection	y = inter-Communication Manager server connections n = the local and/or remote PBX uses a non-Avaya server.
Bypass if IP Threshold Exceeded?	y = the system automatically removes from service trunks assigned to this signaling group, when IP transport performance falls below limits administered on the Maintenance-Related System-Parameters screen.
Direct IP-IP Audio Connection	y enables direct audio connections between IP endpoints, and saves on bandwidth resources and improves sound quality of VoIP transmissions.
Interworking Message	Determines what message the switch sends when an incoming ISDN trunk call interworks (is routed over a non-ISDN trunk group). PROGress causes the public network to cut through the B-channel and allow the caller to hear tones, such as ringback or busy tone, over the non-ISDN trunk. ALERTing causes the public network in many countries to play ringback tone to the caller. Select this value only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk.

set signaling-group

Use **set signaling-group** to set the secondary D-channel in the specified signaling group to be the primary D-channel.

Syntax

```
set signaling-group group#
```

group# The number assigned to the signaling group.

Description

The primary D-channel becomes the secondary D-channel. A signaling group is a collection of B-channels signaled for by a designated single D-channel or set of D-channels over an ISDN-PRI link.

status signaling-group

Use **status signaling-group** to see the service state, type, and port location of the primary and secondary D-channels within an ISDN-PRI signaling group.

Syntax

```
status signaling-group group#
```

group# The administered number associated with each signaling group.

Description

A signaling group is a set of B-channels signaled for by a designated single D-channel, or combination of D-channels over an ISDN-BRI.

status signaling-group field descriptions

Field	Description
Group ID	An administered number that identifies the signaling group.
Type	For information about signalling group types, see <i>Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways Servers</i>. • facility associated signaling: Every member is carried on a single DS1-associated facility. Facility-associated signaling groups support only simplex D-channel configurations. • non-facility associated signaling: Members can include trunks on several different associated DS1 facilities. • An explicit identifier specifies members of the DS1 trunk group across its ISDN-PRI link. A single D-channel on one facility provides signaling for every member. With D-channel backup, a second D-channel is assigned to assume control of signaling if the primary D-channel fails.
Group State	in-service: one of the D-channels signaling for the group is in service out-of-service: neither D-channel in the group is in service If there is no D-channel backup and the primary D-channel is out-of-service, the signaling group is in an out-of-service state.
Link	Link transporting the D-channel
Port	Address of the port transporting either the primary or secondary D-channel
Q-SIP Reference Signaling Group	Displayed only when the Group Type field is sip or h.323. If a signaling group is used as a QSIG over SIP signaling group, the Q-SIP Reference Signaling Group field displays the reference signaling group.

Table continues...

Field	Description
Level 3 State	State of the primary or secondary D-channels: • in-service: the D-channel is in the multiple-frame-established state at layer 2 carrying normal call-control signaling at layer 3. • standby: the D-channel is in the multiple-frame-established state at layer 2, and not carrying any layer 3 call-control messages on logical link 0,0. • wait: an attempt has been made by one side of the interface to establish layer 3 peer communications as part of the process of going to the “in-service” state, which is transitional in nature. Only when the ISDN SERVICE message is sent over the interface, and the far end of the interface responds with a SERVICE ACKnowledge message is the D-channel placed in the “in-service” state. • maintenance-busy: the D-channel is not in the multiple-frame-established state at layer 2. This state is entered automatically when an active D-channel is declared failed. A D-channel that has been placed in the “maintenance-busy” state may be placed in the “out-of-service” state without system technician intervention. • manual-out-of-service: system technician intervention has caused the D-channel to be placed in the TEI-assigned state at layer 2. System Technician intervention is required to retrieve a D-channel from this state. • out-of-service: the D-channel is in the TEI-assigned state at layer 2, but is periodically requested by layer 3 to attempt to establish the link. • no-link: no link is administered for the D-channel

test signaling-group

Use **test signaling-group** to validate the administration of a signaling group, and run a series of diagnostic tests on it.

Syntax

```
test signaling-group group# [ short | long ] [ repeat repeat# | clear ] [ schedule ]
```

- group#** The station extension (must conform to dial-plan)
- short** Run short test sequence. This is the default.
- long** Run long test sequence.
- repeat #** (Optional) The number of times to repeat the command. The default is 1.
- clear** Repeats the test sequence until any active alarms against the maintenance object are cleared by the passing of tests, or until any test in the sequence fails.

schedule (Optional) Specify a start time for the command.

Description

An ISDN-PRI signaling group is a set of B-channels whose signaling messages are carried together on a designated D-channel or set of D-channels. See **status signaling-group** for information on how to access the additional data after running **test signaling-group**.

Example

```
test signaling-group 1
test signaling-group 1 repeat 10
test signaling-group 2 short
test signaling-group 4 long
test signaling-group 4 long clear
```

skill-status

list skill-status

Use **list skill-status** to see administration and status data for skilled hunt groups.

Syntax

```
list skill-status [ starting-number xx ] [ count num-groups yy ] [ schedule ]
```

starting-number xx The starting hunt group number.

count num-groups yy The number of hunt groups to be displayed.

schedule Specify a time to run the command.

list skill-status field descriptions

Field	Description
Group No.	The number of the hunt group/skill group being reported
Group Name	Communication Manager name associated with the hunt group/skill group as administered with change hunt-group (not the CMS name)
Group Type	Call distribution method for the hunt group/skill group
SLS	Service level supervisor
CSO	Call selection override
OCW	(Activate on) Oldest call waiting
DTA	Dynamic threshold adjustment
DPA	Dynamic percentage adjustment

Table continues...

Field	Description
DQP	Dynamic queue position
SO	Service objective
Extension Service Level	Extension number of the hunt group/skill group and the assigned service level targets (represents percentage of calls answered in a specific number of seconds)
Level 1 Threshold	First wait time threshold; when value is exceeded, calls queued to group of reserve agents.
Level 2 Threshold	Second wait time threshold; when exceeded, calls routed to contingency reserve agents
EWT	Estimated wait time for calls queuing to hunt group/skill group
OCW	Oldest call waiting time in queue for the hunt group/skill group

Table 6: Skilled hunt group details

Group Number	Group Name	Group Extension	Group Type
Service Level Supervisor	Call Selection Override	Activate on Oldest Call Waiting	Dynamic Threshold Adjustment
Dynamic Percent Adjustment	Dynamic Queue Position	Service Objective	Weighted Service Level (status)
Service Level Target (percentage and time)	Level 1 Threshold	Adjusted Level 1 Threshold (status)	Level 2 Threshold
Adjusted Level 2 Threshold (status)	SLS State (status)	Expected Wait Time (status)	Time in Queue of Call at Head of Queue (status)

socket-usage

monitor socket-usage

Use **monitor socket-usage** to show how many IP endpoints are registered and how many of those registered IP endpoints have their TCP signaling channels established (connected). The monitor socket-usage screen is periodically updated until the user cancels out of the command.

Syntax

```
monitor socket-usage
```

monitor socket-usage field descriptions

Field	Description

Table continues...

Total registered IP Endpoints	The number of IP endpoints registered with the server
Registered IP Endpoints with TCP Signaling Socket Established	The number of registered IP endpoints that have their TCP signaling channels established.
Registered IP Endpoints with TLS Signaling Socket Established	The number of registered IP endpoints that have their TLS signaling channels established.

status socket-usage

Use **status socket-usage** to show a snapshot of the individual socket usage for Processor Ethernet information, and to list the system's:

- number of registered IP endpoints
- number of registered IP endpoints with TCP signaling sockets established
- number of sockets used
- number of sockets on the system

status socket-usage .

Syntax

```
status socket-usage [ schedule ]
```

schedule Specify a time to run the command.

status socket-usage field descriptions

Field	Description
Total Registered IP Endpoints	The number of IP endpoints registered with the server.
Registered IP Endpoints with TCP Signaling Socket Established	The number of registered IP endpoints that have their TCP signaling channels established.
Registered IP Endpoints with TLS Signaling Socket Established	The number of registered IP endpoints that have their TLS signaling channels established.
Total Socket Usage	The number of TCP signaling sockets currently in use by Processor Ethernet.
Intf Type	Type of interface: • procr — Processor Ethernet media module • procr6 — Displays the socket count for the procr6 node name
Loc	The Processor Ethernet

sp-link

busyout sp-link

Use **busyout sp-link** to put the system printer link into a maintenance busy state and prevent access to the system printer.

The system printer link is a link from the switch to an external printer. This link is created by administering the system printer extension and setting up a call to the system printer.

Syntax

```
busyout sp-link
```

See **status link** for more details on links.

release sp-link

Use **release sp-link** to release the system printer link from a maintenance busy state and enable access to the system printer.

Syntax

```
release sp-link
```

See **busyout sp-link** for more information, and Busyout and Release Commands. See **status link** for more details on links.

status sp-link

Use **status sp-link** to see a summary of the operational state of the system printer link.

Syntax

```
status sp-link
```

See **status link** for more details on links.

status sp-link field descriptions

Field	Description
Link State	The operational state of the link: • up — call is currently set up to the system printer. • down — link is administered but a call is not currently set up to the printer. • extension not administered — extension is not administered on the features-related system parameters screen for the system printer.

Table continues...

Field	Description
Number of Retries	The number of times the switch tried to establish the link since a request to set it up was received. This field is displayed only when the link is down.
Maintenance Busy	Whether maintenance testing is being performed on the system printer link. Blank if the system printer link is not administered.

test sp-link

Use **test sp-link** to perform tests on the system printer link to determine if the link is up, down, or if an extension was not administered. The system printer link is a link from the switch to an external printer.

Syntax

```
test sp-link [ long | short ][ schedule ]
```

- long** Run the long test sequence.
- short** Run the short test sequence.
- schedule** Specify a time to run the command.

See **status pms-link** for more information. See **status link** for more details on links.

station

add station

Use **add station** to administer a new station.

Syntax

```
add station x | next
```

- x** Extension number of the new station.
- next** Assigns the next available extension number to the new station.

For more information about the fields, see *Administering Avaya Aura® Communication Manager*.

busyout station

Use **busyout station** to busyout an installed or uninstalled station extension.

Syntax

```
busyout station x
```

x Extension number per dial plan.

Example

```
busyout station 12345
```

change station

Use **change station** to change an installed extension.

Syntax

```
change station x
```

x Extension number per dial plan.

For field descriptions, see *Administering Avaya Aura® Communication Manager*.

list station

Use **list station** to list the installed extensions.

Syntax

```
list station [ ext x ][ to-ext x | port x | type x | movable x | actual x | count  
n ][ schedule ]
```

ext x First extension in the list.

to-ext x Last extension in the list.

port x Port number. Shows IP Telephone port when IP Softphone and IP Telephone are in shared control.



Note:

The Port field shows information for only IP Telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

type x Type of station.

- movable x**
- list station movable always – shows extensions available for moves anytime
 - list station movable done – shows extensions that had the Automatic Moves field set to once, and have moved
 - list station movable error – shows extensions administered incorrectly and non-serialized extensions
 - list station movable no – shows extensions not available to be moved
 - list station movable once – shows extensions available to be moved once

actual x Lists the stations with actual set type.

count *n* Number of stations in the list.

schedule Specify a time to run the command.

release station

Use **release station** to remove specified administered voice terminal extensions from a maintenance busy state.

Syntax

```
release station x
```

x Extension number per dial-plan.

status station

Use **status station** to see the internal software state information for a specific station. Use the information for diagnosis and to help locate the facilities to which the station is communicating.

Syntax

```
status station x
```

x Extension number per dial plan.

status station field descriptions, page 1 — General Status

Field	Description
Active Coverage Option	Specifies the active coverage path.
Active call(s)	Displays the current status of the agent on an active call. • Yes: Agent is on an active call. • No: Agent is idle.
Administered Type	Administered station type.
Busied-out	Displays the service state of the station. • Yes: The station is out of service. • No: The station is in use.
Call Parked	Whether the station has a call parked (y/n)
CTI Monitoring Active	Displays the connection status of the CTI controller. • Active: An active CTI domain monitoring on the station (any type). • Not Active: The station has no active CTI domain monitoring.

Table continues...

Field	Description
Connected Ports	Port locations of the facilities to which the telephone/softphone is connected: cabinet-carrier-slot-circuit  Note: If a station is connected to a QSIG over SIP trunk, you can view the involved port of the SIP trunk. However, you cannot view the port of the QSIG trunk since the port is not involved in the media connection.
Connected Type	The type of telephone connected to this port.
Download Status	Status of soft key download.
EC500 Status	enabled — Extension to Cellular is enabled disabled — Extension to Cellular is disabled
Extension	Station or attendant extension.
Group Cntrl Restr	One or two of the following: • none • total • stat-stat • outward • terminate
Limit Incoming Calls	State of the Limit Number of Concurrent Call (LNNC).
Message Waiting	Whether there is a message waiting for the station. • AUDIX • PMS • blank if no messages are waiting
Network Region	The network region (NR) that determines whether Communication Manager triggers the IGAR or DPT feature: • For a DCP or analog station, this field displays the NR of the port network or media gateway to which the station is connected. • For a registered H.323 station, this field displays the NR to which the station is currently assigned. • For an unregistered H.323 station, this field displays the NR in which the station was registered recently. • For a SIP station, this field displays the NR associated with the IP address that Communication Manager received in the recent SIP INVITE or SIP response for that station.

Table continues...

Field	Description
Parameter Downlaod	Current status of downloading terminal parameter information. • complete — the information was successfully downloaded sometime in the past. • pending — the system is waiting to download the information. The download will complete through a background periodic test or demand test. • not applicable — this is not a programmable station.
Port	Port location of the endpoint.
Reachability Polling Active	• yes- If Communication Manager is actively polling the SIP station by the SIP Reachability feature. • no- If Communication Manager is not actively polling the SIP station. By default the field is set to <code>no</code>. Communication Manager will poll the station with SIP OPTIONS messages directly by the Reachability feature in either of the following cases and the Reachability Polling Active field on status station shall show <code>yes</code>: • The Enable SIP Agent Reachability? field is set to <code>yes</code>, and the SIP station has an ACD agent logged in. • The Enable Reachability for Domain Control SIP Stations? field is enabled and the station is monitored by CTI.
Reg Subscription Active	Displays the registration subscription state of the station on Session Manager. This field is active only when CTI is monitoring the station and SIP Reachability is disabled for the station or system-wide. • yes: Communication Manager is subscribed to registration events on Session Manager. • no: Communication Manager is not subscribed to registrations events on Session Manager.
Ring Cut Off Act	Whether ring cut-off is activated (y/n).
SAC Activated	Whether Send All Calls is activated on this extension (y/n).
Service Link Extension	Extension for the softphone off-premise destination on a telecommuter configuration.
Service Link Port	Shows the port used to establish a connection to the softphone off-premise destination on a telecommuter configuration.

Table continues...

Field	Description
Service State	State of the telephone endpoint: • in-service/on-hook (with no OPTIM calls, if applicable) • in-service/off-hook • in-service/disconnected (no OPTIM calls, if applicable) • in-service/idle (the station is AWOH or hardware is otherwise not present, with no OPTIM calls if applicable) • in-service/active (with OPTIM, has OPTIM calls and is not physically off-hook) • in-service/in-tsa (Terminal Self Administration) • out of service (the station is busied-out) For SIP stations, the following fields are available: • unknown — Communication Manager has no information about the service state of this station. • pending — Communication Manager is expected to have service state information soon after polling is done • out-of-service - Communication Manager has service state information and it shows the station is not operational. • in-service — Communication Manager has service state information and it shows the station is operational.
Shd TCP Signaling Status	Indicates whether a TCP signaling channel is established for the endpoint on a shared control connection. Displayed only for IP Telephones and Softphones. • connected — Endpoint is registered and TCP signaling link is established • connecting — Endpoint is registered and TCP signaling link is in the process of being connected • not connected — Endpoint is unregistered • on-demand — Endpoint is registered and TCP signaling link is not established. For IP endpoints with on-demand status, test station triggers TCP socket establishment. For all IP endpoints except soft IP endpoints such as IP Softphone and IP Agent, status station triggers TCP socket establishment.
Softphone Port	The port for the softphone controlling an IP telephone.

Table continues...

Field	Description
TCP Signal Status	Indicates whether a TCP signaling channel is established for the endpoint. Displayed only for IP Telephones and Softphones. • connected — Endpoint is registered and TCP signaling link is established • connecting — Endpoint is registered and TCP signaling link is in the process of being connected • not connected — Endpoint is unregistered • on-demand — Endpoint is registered and TCP signaling link is not established. For IP endpoints with on-demand status, test station triggers TCP socket establishment. For all IP endpoints except soft IP endpoints such as IP Softphone and IP Agent, status station triggers TCP socket establishment.
User Cntrl Restr	One or two of the following • none • total • stat-stat • outward • terminate

status station field descriptions, page 2 — Connected Station Information, Hospitality Status, and Enhanced Call Forwarding Destinations

Field	Description
General Status	
Connected Station Information	
Part ID Number	Part ID Number (comcode) of the telephone. If this field shows Unavailable, the software was unable to determine the Part ID Number.
Serial Number	Serial number of the telephone. • Unavailable — the software is unable to determine the Serial Number. • Errored — the serial number received is not in the correct format.
Station Lock Active	Indicates whether the station has been locked using Station Lock.
TOD Station Lock	Indicates whether the station is within a Time of Day lock interval.
Off-PBX Service State	• inservice/idle — there is no OPTIM call at the station • inservice/active — there is an OPTIM call at the station • out-of-service — the station is busied out.
Hospitality Status	

Table continues...

Field	Description
Awaken At	Time that Automatic Wakeup Call is scheduled. The time is based on the location of the station.
User DND	activated/not activated Status of Do Not Disturb
Group DND	activated/not activated Status of Do Not Disturb
Room Status	Whether a room is occupied or not • non-guest room • vacant • occupied
Languages	Communication Manager displays the language that you have downloaded on a 9404 or 9408 telephones. The default value of this field is blank.
Language File Version	Communication Manager displays the version of the language that you have downloaded on a 9404 or 9408 telephones. The default value of this field is blank.
CF Destination Ext	Call forwarding destination extension, if any. • blank when Extension to Cellular is enabled • is displayed for mapped extensions when Extension to Cellular is disabled
Enhanced Call Forwarding Destinations	Up to six Enhanced Call Forwarding destination numbers for Unconditional, Busy, or No Reply ECF types, and the internal or external destination for each.
Team Button Monitoring Stations	Shows all monitoring extensions that supervise the monitored station

status station field descriptions — Unicode Display Information, page 3

Field	Description
Native Name Scripts	N/A, or on a Unicode-enabled station, the script used for the native name of the station: 0x plus the hex value of the script tag, and up to 7 language acronyms.
Display Message Scripts	N/A, or on a Unicode-enabled station, the script used for the display language of the station: 0x plus the hex value of the script tag, and up to 7 language acronyms.
Station Supported Scripts	N/A, or on a Unicode-enabled station, the script supported by the telephone: 0x plus the hex value of the script tag based on the scripts supported by Unicode capable endpoints, and up to 7 language acronyms.

status station field descriptions — 3way IP Conference Call, pages 1–3

Field descriptions are the same as **status station**, pages 1 and 2 field descriptions.

status station field descriptions — Call Control Signaling, page 5

Field	Description
Call Control Signaling — Call Control Signaling fields display the information for both endpoints when an IP telephone and IP soft phone are in service on the same extension simultaneously (shared-control).	
Switch-End IP Signaling Loc	The procort serving the switch end of the IP signaling link. The port number is always 17 for the ethernet port of the procort. This field is blank for an unregistered H.323 station.
H.245 Port	The procort port serving the H.245 signaling link. The port number is 17 for the ethernet port. This field is blank for an unregistered H.323 station, a VPhone, or when H.245 tunneling in Q.931 is used.
Switch-end: IP Address and Port	Switch-end Q.931 (H.323 station) or CCMS (IP SoftPhone) IP signaling address and IP port. IP Port has a decimal value 0-65535. This field is blank for an unregistered H.323 station.
V4 Set-End: IP address and Port	Set-end IPv4 IP signaling address and IP port. IP port is a decimal value 0-65535.
V6 Set-End: IP address and Port	Set-end IPv6 IP signaling address and IP port. IP port is a decimal value 0-65535.
Node Name (for Call Control)	Label administered for an IP address.
Region (for Call Control)	A number given to a set of IP addresses to indicate they have a common set of characteristics.
H.245 Near	Switch-end H.245 IP signaling address and TCP/IP port. IP Port is 0-65535. This field is blank for IP SoftPhone endpoints, endpoints using Q.931 tunneling of H.245, and unregistered or inactive H.323 stations.
H.245 Set	Set-end H.245 IP signaling address and IP Port. IP Port is 0-65535. This field is blank for IP SoftPhone endpoints, endpoints using Q.931 tunneling of H.245, and unregistered or inactive H.323 stations.

status station field descriptions — Audio Channel, page 6

Audio Channel fields display the information for only the IP Telephone when an IP telephone and IP soft phone are in service on the same extension simultaneously. Product Information fields show the information for both endpoints for soft phone and Telephone Shared Control.

Field	Description
xxxxxxx Audio	The type of audio active for the station. xxxxxxxx is one of these values: G.711-MU, G711-A, G.729A, G.723.1-6.3, G.723.1-5.3, PCM, 711-MU, 711-A, 729, 729A, 729B, 729-AB, or 723.1-5.3/6.3. • PCM - the station is a telecommuter IP softphone configuration with call-back audio • blank - no audio path is present

Table continues...

Field	Description
Port/Shared Port	The physical port used to provide audio path for the endpoint. The port represents a media gateway or media server port for H.323 stations, or for stations using a H.323 endpoint for audio. An idle IP SoftPhone or H.323 station with an as-needed service link shows no audio port. Blank — stations with no established audio path, or for telecommuter stations.
Other-end IP Addr and Port	Other-end IP audio address and IP port. Port is a decimal value 0–65535. This field is blank for an idle station with no audio link, or for a telecommuter IP SoftPhone with circuit-switched audio link.
Set-end IP Addr and Port	Set-end IP audio address and IP port. Port is a decimal value 0–65535. This field is blank for an idle station with no audio link, or for a telecommuter IP SoftPhone with circuit-switched audio link.
Node Name	Label administered for an IP address.
Network Region	A number given to a set of IP addresses to indicate they have a common set of characteristics.
Audio Connection Type	Audio codec selected. • ip-tdm • ip hairpin • ip direct • ip-idle • blank — audio is carried directly to service link port
MAC Address	The Media Access Control (MAC) address received from the telephone when the telephone registers. This field is displayed in the second column of the screen when the Shared Port field is populated. • not available: the telephone registers but is unable to send a MAC address • blank: the telephone is not registered.

status station field descriptions — IP Endpoint Data, page 7

Field	Description
Product ID and Release	Identifier submitted by the endpoint during registration, and the release number of the endpoint that is provided to the gatekeeper upon registration. This field is displayed only for Avaya or Lucent products. This field is displayed in the second column of the screen when the Shared Port field is populated. Value is one of the 30 enabled product IDs administered on the system-parameters customer-options screen, including: • IP_Tel - IP Telephone • IP_Soft - IP Softphone • IP_eCons - An IP soft console • IP_Agent - An IP soft agent telephone • IP_ROMax - A remote office telephone
H.245 Tunneled in Q.931	y — H.245 is contained within Q.931, and H.245 fields are not displayed. Does not apply to IP SoftPhone endpoints. This field is displayed in the second column of the screen when the Shared Port field is populated.
Registration Status	Identifies the registration and authentication status of the IP endpoint. An unregistered IP SoftPhone cannot be identified as an IP endpoint. This field is displayed in the second column of the screen when the Shared Port field is populated. • unregistered (H.323 station only) — the endpoint is unregistered • registered-not-authenticated (H.323 station only) — the endpoint is registered, but has not been authenticated (the station is disallowed from making or receiving calls) • authenticated-not-registered (H.323 station only) — the endpoint has been authorized (by the associated IP SoftPhone), but is not yet registered • registered-authenticated — the endpoint is registered and authenticated (for example, an IP station that is able to make calls) • pending-unregistration — the endpoint is unregistered, but critical internal data structures have not yet been updated

Table continues...

Field	Description
MAC Address	The Media Access Control (MAC) address received from the telephone when the telephone registers. This field is displayed in the second column of the screen when the Shared Port field is populated. • not available - the telephone registers but is unable to send a MAC address • blank - the telephone is not registered.
Authentication Type	 Note: This field complies with the Unified Capabilities Requirements (UCR) 2008 Change 3 requirements and is approved by Joint Interoperability Test Command (JITC). This field is available only for the USA Department of Defense (DoD) and approved Federal government customers. When you register the stations with security profile H323TLS, status station shows Authentication Type as TLS.
Native NAT Address	Specifies the network address translation (NAT) IP address of the endpoint when a network device provides the network address translation function for the endpoint. The network device provides the NAT address of the endpoint at the time of registration. The field is blank if the NAT address is not known. This field is displayed in the second column of the screen when the Shared Port field is populated.
ALG-NAT WAN IP Address	This field is populated only when a special application turned on.
Media Encryption	aes indicates Advanced Encryption Standard encryption, the standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. aea indicates Avaya Encryption Algorithm. Not as secure as AES. none indicates an unencrypted media stream.

status station field descriptions — Alternate Gatekeeper List, page 8

Field	Description
Main	Main is the phone which did an ordinary H.323 registration. This phone did not register in shared control mode.
Shared Control Ports	Shared Control ports register more than one H.323 endpoint to the same Communication Manager extension number. Usually the endpoints are a desk phone and a softphone, but they can include an AES application.
Node Name	Node name is a label administered for an IP address.
Region	Region is a bunch of IP destinations that have a lot in common with each other.

status station field descriptions — ACD Status, page 9

Field	Description
Grp	Hunt Group number
Mod	ACD Work Mode
On ACD Call	Whether the agent is on an ACD call (y/n)
Occupancy	Occupancy of the agent logged in at the specified station

status station field descriptions — Network Status and Summary

Network Status fields show information for only the IP Telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

Field	Description
Average Jitter Last Ten Seconds # - more than 255 ms	The average jitter in received packets from the last ten one-second intervals. # — maximum (100%) packet loss per second during the one-second interval.
Packet Loss per Second Last Ten Seconds * - 100% loss	The 10 recent one-second samples of the lost packet information for the requested endpoint. * — maximum (100%) packet loss per second during the one-second interval. * is displayed when silence suppression is y on the ip-codec-set screen, or when packet loss = 100%.
Out of Order Count	A count of the number of out-of-order packets detected during the current connection.
SSRC Change for Call	The number of SSRC changes occurring during the current connection.
Last Rx Sequence No.	Last received data packet sequence number.
Last Tx Sequence No.	Last transmitted data packet sequence number.
Echo Return Loss	Loss of the echo signal, relative to the transmitted signal, due to the PSTN network including the hybrid.
Bulk Delay	Delay offset of the echo relative to the original signal.
ERL Enhancement	Loss introduced by the echo canceller. This is the measure of the effectiveness of the echo canceller.
Summary	
Worst Case this Call	Jitter: the worst-case, 1-second jitter (ms) experienced during the current connection. Packet Loss: the worst-case, 1-second packet loss experienced during the current connection.

Table continues...

Field	Description
Average this Call	Jitter: the average jitter for the current connection (the running average of all the 1-second intervals during the connection). Packet Loss: the average packet loss number for the current connection (running average of all the 1-second intervals experienced during the connection).
Current Buffer Size	The current jitter buffer size.

status station field descriptions — Connected Ports

Connected Ports fields show information for only the IP telephone when an IP telephone and IP Softphone are in service on the same extension simultaneously.

Field	Description
src port	The port address of the statused station.
MP	The physical port location of the media processing media module. The audio stream passes through a media processing media module (either a Medpro or a VoIP module on a gateway) when direct IP-IP audio connections are disabled or the connection cannot be direct for other reasons (for example, the call requires a codec conversion).
HP	Hairpinning. y is displayed when the audio stream is handled entirely on the media processing media module. The audio connection does not require more extensive processing (for example, some codec conversion), and does not use TDM bus resources.
ip-start	The IP address of one end of a direct connection.
ip-end	The IP address of the other end of a direct connection.
audio	Type of audio codec active for the connection. G.711-MU, G711-A, G.729A, G.723.1-6.3, G.723.1-5.3, PCM, 711-MU, 711-A, 729, 729A, 729B, 729-AB, or 723.1-5.3/6.3.
encryption	Type of media encryption as entered on the ip-codec-set screen. aes — Advanced Encryption Standard encryption, standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. aea — Avaya Encryption Algorithm. Not as secure as AES. none — An unencrypted media stream.
ss	on/off Indicates whether silence suppression is active on this audio stream.
pkt	Size of the packet carrying the audio.
dst port	The port address of one of the other parties to which the statused station has a connection on this call.

status station field descriptions — SRC Port to Dest Port Talkpath

Field	Description
src port	port number

status station field descriptions — Voice Statistics

Field	Description
TN Code	The media processor board code used for the call.
Board Loc	The carrier/slot location of the media processor for which data is being reported.
Codec	The codec used for the call.
Encryption	The type of media encryption used on the call (for example, AES, AEA, SRTP 1, and so on).
DSP Number	The number of the DSP on the media processor board used for the call.
Endpoint ID	The endpoint ID assigned for the call.
UDP Port	The UDP port used by the media gateway or media server for the call.
Called Number	The number of the endpoint which received the call (far end).
Dst Net Reg	The network region where the destination media gateway or media server is located.
Far-End IP Addr	IP address of the device on the far end of the call (called party).
Echo Canc	Indicates whether the echo cancellation is on/off for the call.
Echo Tail (ms)	The tail length of the echo canceller used for the call. 0 — implies that a different echo canceller was used than the one on the media processor.
Silence Suppression	Indicates whether Voice Activation Detection (VAD) is used for the call.
Comfort Noise Gen	Indicates whether CNG is being used for the call.
Data Call/Type	Indicates whether the call is a data call. If y (yes), include type of data call (for example, FAX, Modem, Clear Channel, TTY, Fax-PT (pass-thru), Mod-PT, TTY-PT). For example, Data Call/Type: y/T.38 FAX
Threshold Exceptions	A total number of thresholds that are exceeded for the call when the data was requested.
Packet Size (ms)	The size for each steam of data for the associated call, measured in milliseconds.
% Packet Loss	The amount of packet loss occurred for the call when the data was requested.
Peak Packet Loss (%)	The peak packet loss recorded for the call.

Table continues...

Field	Description
Jitter Buffer Size (ms)	The size of the jitter buffer used for the call, measured in milliseconds.
Jitter Buffer Overruns	A number of jitter buffer overruns occurred for the call. Overruns occur when too many packets arrive into the jitter buffer very quickly, causing the jitter buffer to fill up. When it happens, the jitter buffer is unable to handle additional traffic/packets. If the number of overruns exceeds 99, the value in this field is 99+ .
Jitter Buffer Underruns	A number of jitter buffer underruns occurred for the call. When the arrival time of packets goes beyond the size of the jitter buffer, the jitter buffer underrun occurs which results in silence until there are additional packets in the jitter buffer to process. If the number of underruns exceeds 99, the value in this field is 99+ .
Average Jitter (ms)	The average amount of jitter recorded for the call over a 10-second reporting interval, measured in milliseconds.
Peak Jitter (ms)	The peak amount of jitter recorded for the call, measured in milliseconds.
Avg RT Delay (ms)	The average round trip delay of packets, measured in milliseconds.
Peak RT Delay (ms)	The peak round trip delay recorded for the call, measured in milliseconds.

test station

Use **test station** to perform hardware diagnostic tests on an individual port circuit assigned to that extension. The technician must specify the extension and a translation is automatically done to the physical port location.

Syntax

```
test station x [ short | long ][ repeat # | clear ]
```

x Extension number per dial plan.

short Execute the short nondestructive test sequence.

long Execute the long test sequence.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

Example

```
test station 81709 l
test station 85136 s r 2
test station 85036 l r 25
test station 84297 r 4
test station 81709 c
```

survivable-processor

list survivable-processor

Use `list survivable-processor` on the primary controller to see the status of Survivable Remote Server or Survivable Core Server administered on the Survivable Processors screen (`add survivable-processor`) or the system-parameters port-networks screen. Verify that the Survivable Remote Server or Survivable Core Server(s) register, and that translations are updated.

Syntax

```
list survivable-processor
```

list survivable-processor field descriptions

Field	Description
Name/IP Address	Name of the Survivable Remote Server or Survivable Core Server as administered on the Survivable Processors screen (<code>add survivable-processor</code>) or the System Parameters Port Networks screen. IP address of the node name as it is displayed in the IP Node Name screen and on the Survivable Processor Ethernet screen.
Type	Survivable Remote Server, Survivable Core Server Survivable processor type as listed on the Survivable Processor Ethernet screen (<code>add survivable-processor node-name</code>).
ID	Server ID number (cluster ID) of the Survivable Core Server or Survivable Remote Server.
Reg LSP Act	
Service State	in-service/idle — the Survivable Remote Server is registered out-of-service
Translations Updated	Time and date of the translation update to the Survivable Remote Server or Survivable Core Server.
Net Rgn	Network region in which the PE interface of the Survivable Remote Server or Survivable Core Server resides, as listed on the Survivable Processor Ethernet screen.

For more examples of the Survivable Processor screen, see 'Survivable Processor' in *Avaya Aura® Communication Manager Screen Reference*.

suspend-alm-orig

disable suspend-alm-orig

Use **disable suspend-alm-orig** to stop entries from the active Suspend Alarm Origination table. This command disables all board entries that match a specific physical board location.

 Note:

disable suspend-alm-orig does not disable port entries.

Syntax

```
disable suspend-alm-orig location
```

location Physical location of the board.

Example

```
disable suspend-alm-orig 1C03
disable suspend-alm-orig 1E07
```

enable suspend-alm-orig

Use **enable suspend-alm-orig** to suspend alarm origination for alarms generated by the specified board (location) or port (location) for a the specified amount of time (hrs).

enable suspend-alm-orig does not support media modules without a board location. Enter **enable suspend-alm-orig** multiple times to suspend alarms on different boards or ports. If a physical location is specified for which there is already a suspension in effect, the most recent suspension request replaces the previous request.

Use **enable suspend-alm-orig** to improve control over situations such as:

- Quieting a hyperactive port board during installation or troubleshooting.
- Improving control over customer requests. For example, use **enable suspend-alm-orig** to temporarily suspend off-board DS1 alarms for customers who periodically disconnect DS1 trunks for testing or other business purposes.
- Improving control over external (non-Avaya) problems. For example, use **enable suspend-alm-orig** to suspend off-board DS1 alarms before a customer resolves facility problems, such as working with the vendor of a T1 trunk that has developed an off-board condition.
- Improving control over internal (Avaya) problems that cannot be immediately resolved. For example, use **enable suspend-alm-orig** to suspend alarm origination for a bad media module detected late Friday night if personnel cannot be dispatched until Monday.

To see a list of active alarm origination suspensions, use **list suspend-alm-orig**. To disable a suspension, use **disable suspend-alm-orig**.

Syntax

```
enable suspend-alm-orig location [ off-board-only ] expires-in-hrs hrs
```

location Physical location of the hardware.

off-board-only (Optional) If not specified, both on-and off-board alarms suspended.

expires-in-hrs hrs Number of hours (1–72).

Example

```
enable suspend-alm-orig 1B03 expires-in-hrs 3
enable suspend-alm-orig 1B0701 expires-in-hrs 72
enable suspend-alm-orig 1B07 off-board-only expires-in-hrs 24
```

list suspend-alm-orig

Use **list suspend-alm-orig** to see active entries in the Suspend Alarm Origination table. Even though this command only lists active entries, an entry that expires during the list process is still displayed in the output. If the Suspend Alarm Origination table is empty, the output contain only the title and field headings.

Syntax

```
list suspend-alm-orig
```

synchronization

change synchronization

Use **change synchronization** to change the synchronization source for the system. After running change synchronization, clocks may momentarily lose synchronization.

Use **change synchronization** to administer primary and secondary references for the Stratum 4 option, or -Switch, indicating that the synchronization references are input directly to the switch.

Syntax

```
change synchronization [ media-gateway n | css | port-network n ]
```

media-gateway n Change the gateway number.

change synchronization feature interaction

DS1 interface, BRI trunk, or UDS1 board selected as either a primary or secondary sync source cannot be removed on the DS1 media module administration screen or the regular media module administration screen.

change synchronization field descriptions

Field	Description
Stratum	Enter 3 for stratum-3 clocking or 4 for stratum 4 clocking.
Primary	First choice system synchronization source. Blank means no synchronization. Enter 5-character board location on any system. Sync source must be in the cabinet being administered.
Secondary	Five-character board location for second choice system synchronization source. Blank means no synchronization. Sync source must be in the cabinet being administered.
Location	Media module location of all administered DS1 media module (media gateway).
Type	Type of media module.
Name	User-defined name for the DS1 media module.
Slip	y/n Slip alarm enabled on DS1 media module.

disable synchronization

Use **disable synchronization** to disable the automatic clock-switching capability of the Synchronization Maintenance subsystem. The synchronization subsystem (TDM bus clock, DS1 trunk board, and maintenance and administration software) provides error-free digital communication between the switch and other PBXs, COs, or customer equipment.

disable synchronization does not apply to -connected port networks.

Syntax

```
disable synchronization [ media-gateway n]
```

port-network # Disable the PN number entered.

media-gateway # Disable the media gateway number entered.

display synchronization

Use **display synchronization** to see a synchronization plan. On a duplicated server, specify the port network number.

Use **display synchronization** to display the synchronization screen with the administered synchronization stratum and reference sources.

Syntax

```
display synchronization [n| media-gateway n][ schedule ]
```

media-gateway n Display the gateway number entered.

schedule Specify a time to run the command.

display synchronization feature interaction

A DS1 interface or a UDS1 board that is selected as a primary or secondary synchronization source cannot be removed on the DS1 media module administration screen or the media module administration screen.

display synchronization field descriptions

Field	Description
Stratum	Specifies the synchronization stratum used.
Primary	Designates the first choice system synchronization source. Blank — no synchronization.
Secondary	Designates the second choice system synchronization source.
Location	The media module location (media gateway slot) of all media modules administered to serve as synchronization references.
Name	The user-defined name of the media module. If blank, no name was administered.
Slip	y If the media module has slip detection enabled.

enable synchronization

enable synchronization does not apply to -connected port networks.

Use **enable synchronization** to return control of the selection of the synchronization source to the Synchronization Maintenance subsystem after being previously turned off by **disable synchronization**.

list synchronization

Use **list synchronization media-gateway** to see all administered gateway reference boards and the existing reference sources.

Syntax

```
list synchronization [ media-gateway | port-network ] [ schedule ]
```

media-gateway List the gateway reference boards.

schedule Specify a time to run the command.

set synchronization

Use **set synchronization** to set a specific synchronization-capable media module as the reference source for system synchronization signals.

- DS1 Trunks
- BRI Trunks

Use **set synchronization** after automatic synchronization has been disabled with **disable synchronization**.

sys-link

list sys-link

Use **list sys-link** to see every system link. Each link's location, type and dlci number, state, current path status, faulted path status, and last recorded fault (if any) are displayed. See SYS-LINK (System Links) in *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers* for details.

See **status link** for more details on links.

Syntax

```
list sys-link [ schedule ]
```

schedule Specify a time to run the command.

list sys-link field descriptions

Field	Description
Location	The physical location of the far endpoint associated with the system link (cabinet-carrier-slot-circuit).
Type/dlci	The type of system-link and the dlci of the link (if there is one). System links include the following (see SYNC (Port Network Synchronization) in the <i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i>): • BFDL - Bearer Fault Detection Link • PRI - ISDN-PRI Signaling Link • TACL - Trunk Control Link
State	Whether the system link is up or down .
Current Path	This field specifies the status of the current path. This field displays none if the link is down or present if the current path is functional.

Table continues...

Field	Description
Faulted Path	This field shows whether the link has experienced a fault and been switched to another path. • Present indicates that the link has been faulted at least once. • None is displayed if the link has not gone down. • Default is displayed if the default faulted path is being used.
Last Fault Recorded	The date and time that the most recent fault on the link took place.

system

monitor system

Use **monitor system** to see a summary of the overall condition of the system, real-time status for time slots and buses, call rates, intervals, and so on. Press **CANCEL** to clear the command.

Syntax

```
monitor system view1 | view2 | conn [ conn pnn | conn pnn #
```

view1 Show attendant status, the maintenance status, the last hour's measurement of trunk groups, hunt groups, and the attendant group, and the time of day.

view2 Show the view1 screen except the last hour's hunt group measurements

conn Show the connection monitor output for key information

Use **monitor system view1** and **monitor system view2** to see the condition, or health, of the system.

- view1 shows attendant, maintenance, and traffic status. Attendant and maintenance status are updated every minute and traffic status is updated on an hourly basis. Pressing **CANCEL** forces a logout of the current login ID.
- view2 shows the view1 screen except the hunt group measurements

Use **monitor system connection** to see the status of connections, compiled by the connection manager. This on-line status report is automatically updated every minute or by pressing the **UPDATE** key. Pressing **CANCEL** forces a logout of the current login ID.

Examples

```
monitor system view1
monitor system view2
monitor system conn
```

monitor system view1 and view2 field descriptions

Field	Description
# of alarms for other resources	The number of existing minor and major alarms on every maintainable object in the system except trunks and stations.
First OSS number has been informed	Has every alarm been reported and acknowledged by the first OSS telephone number? If "Alarm Origination" is not enabled or there are no active alarms, this is n.
Measurement Hour	The starting time of the period for which the measurement was taken. For example, if the measurement hour is shown as 18, the traffic status data is for the time from 6 PM to 7 PM. The measurement is taken on an hourly basis).
Grp no	The trunk-group or hunt-group number.
Grp dir	Group direction: incoming, outgoing, or two way.
Calls qued	Total calls that arrived and were placed in the queue for trunk groups.
Calls aban	Total calls that were abandoned by the caller.
%Out blkg	The ratio of outgoing calls that are not carried, due to overload conditions, on a trunk group to the outgoing calls offered.
% Time ATB	The percentage of time within the polling interval that every trunk in the trunk group was unavailable for use.
Time of day	The current time of day acquired from the system.

monitor system conn field descriptions

Field	Description
Max_callrate	The maximum call rate hit during the time since the last hour has passed. For example, if monitor system conn is executed at 20 minutes past 12:00, this shows the maximum call rate obtained during the past 20 minutes.
Next_hour	0 or 1, depending upon if the measurements being taken are for this hour or the next. You can relate to the previous field in that the maximum call rate is reflected for this hour. When this flag is set, statistics begin to accumulate for the next hour. Thereafter, the maximum call rate becomes zero and new accumulations begin.
tot_ts_req	Number of time slots in use during the time elapsed since the top of the last hour. Data is collected every 100 seconds. When the timer fires and the data collection occurs, a check is made as to how many time slots are in use. One number is displayed for each PNN requested.
ts_total	Number of time slots requested since the top of the last hour.
fts_total	Number of fiber time slots requested since the top of the last hour.

reset system

Use **reset system** to reload Communication Manager software. All system resets are disruptive and terminate the SAT login.

Caution:

All system resets are service affecting, with higher levels being increasingly destructive. Some resets may take up to one-half hour to complete. Certain conditions may result in a higher reset level than the one requested. Unless you are experienced with resetting a system, follow normal escalation procedures.

Syntax

```
reset system level#
```

level# (1–5) Restart Level

Description

If you set the value of the Display Warning Prior to System Reset? field to **y** on the **system-parameters maintenance** screen and then use the reset system command, a warning message is displayed.

WARNING: All system resets are service affecting, with higher levels being increasingly destructive.

Press the SUBMIT or ENTER function key to continue or CANCEL to abort the command.

Note:

Connections are preserved on H.248 branch gateways on reset system 2 and reset system 4 conditions. To reset gateways from the SAT, use **reset media-gateway**.

reset system resets the system in the following manner:

- A mini-coredump is generated for non-interchange related restarts and placed in the directory: `/var/log/defty/dumps`.
- A change in translation administration is in progress.

System software does not escalate a demand system reset to a higher level. There are certain conditions that result in a higher level reset than that requested. These include:

- the restart is performed

Approximate Recovery Time for System Resets (min:sec)

System reset times differ between different configurations

Level	Recovery	2,400 lines	5,000 lines	15,000 lines
1	Warm Restart	:10	:10	:10
2	Cold-2	1:00	2:00	4:00
4	Reload	4:00	6:30	11:00

reset system feature interactions

reset system invokes system initialization like low-level maintenance. Software never escalates requested reset levels; technicians determine the levels.

Reset system cannot be canceled. The screen shows the results of various initialization tests. If reset system is successful, the user is logged off. Several conditions may prevent a requested reset.

Reset Level 1

Reset Level 1 (warm restart) duration, causes, and effects

Duration	Up to 10 seconds, typically 4 seconds
Causes	reset system 1 command from Communication Manager (SAT) command line Spontaneous server interchange (those caused by hardware faults) Software faults that are not service affecting Demand server interchange Software escalation
Effects	Stable calls are preserved; queued ACD calls, H.323 calls, and H.320 (multimedia) calls stay up. System links such as ISDN-PRI D-channel signaling links, CMS, AUDIX, DCS links over Procor are preserved. The CMS, DCS, and AUDIX links could lose buffered messages. Error and alarm logs are preserved, but every alarm is resolved except busyouts. Stable features are preserved. Transient calls (not yet connected) and some user stimuli are dropped. New calls are not processed during the reset. Encrypted system links may be dropped and reestablished. If the reset resulted from a spontaneous server interchange, memory shadowing is turned off, and the standby server will not be available for service until memory is refreshed (several minutes). Application links such as those to AUDIX and CDR are dropped and re-established in under 2½ minutes. Translation data is preserved in memory. If save translation is in progress, an SAT-requested warm restart would be aborted. A software-requested warm restart would result in an unsuccessful save translation and possibly corrupt translations.

Reset Level 2

Reset Level 2 (cold restart) duration, causes, and effects

Duration	Up to 3.75 minutes

Table continues...

Causes	<code>reset system 2</code> command from Communication Manager (SAT) command line Escalation from SAT's <code>reset level 1</code> An attempted SAT's <code>reset level 1</code> Spontaneous interchange into an unrefreshed standby server
Effects	Every system and application link is dropped. Gateways are not reset. Every call is dropped. Every administrative session is dropped. Every system link is dropped and re-established. Every application link is dropped and re-established. Non-translation feature data, such as Automatic Wakeup calls, are lost and must be re-entered. Translation data is preserved in memory. If <code>save translation</code> is in progress, a SAT-requested cold-2 restart would be aborted. A software-requested cold-2 restart would result in an unsuccessful <code>save translation</code> and possibly corrupt translations. Every login, including remote access and system port logins, is dropped. Initialization firmware runs diagnostics and displays results on the screen. Server memory shadowing is turned off, leaving the standby server unavailable for service for up to several minutes. Every hardware component is reset except: • DS1 clocks. Every busied-out MO is released and can be rebusied. Error and alarm logs are preserved, and every Communication Manager alarm is resolved.

Reset Level 4

Reset Level 4 (reload) duration, causes, and effects

Duration	Typically 11 to 14 minutes
Causes	<code>reset system 4</code> command from Communication Manager (SAT) command line Escalation from SAT's <code>reset level 2</code> Power up Recovery attempt from server-down mode

Table continues...

Effects	System software (boot image) is reloaded and every process is re-initialized. Communication Manager administration (translations) are reloaded from the hard disk. Before reboot, the system attempts to save the alarm and error logs. After reboot, error and alarm logs are restored. Some error and alarm information may be lost if the last save before the reboot save does not succeed. Other effects are the same as those in reset level 2, except that more extensive diagnostics are performed. A core dump is automatically enabled for this reset level and is saved to the /var/log/defty/dumps/ directory. The reboot is delayed until the core dump is finished.

System-parameters customer-options

display system-parameters customer-options

Syntax

display system-parameters customer-options

Use the **display system-parameters customer-options** command to view the parameters in the **Maximum Number of Avaya Media Server VoIP Channels** field.

Field	Description
IP PORT CAPACITIES	Indicate the license file provided by the Avaya Aura [®] Media Server (MS) VoIP channel license limit.
Used	Indicates the number of current active VoIP channels, which is the number of licenses currently used on active media connections.

```

display system-parameters customer-options                                Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 38
      Maximum Concurrently Registered IP Stations: 18000 4
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 0 0
      Max Concur Registered Unauthenticated H.323 Stations: 0 0
      Maximum Video Capable Stations: 41000 3
      Maximum Video Capable IP Softphones: 100 2
      Maximum Administered SIP Trunks: 24000 65
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0
      Maximum TN2501 VAL Boards: 128 1
      Maximum Media Gateway VAL Sources: 250 0
      Maximum TN2602 Boards with 80 VoIP Channels: 128 1

```

```
Maximum TN2602 Boards with 320 VoIP Channels: 128 0
Maximum Number of Expanded Meet-me Conference Ports: 0 0
Maximum Number of Avaya Media Server VoIP Channels: 12000 843
```

system-parameters ip-options

change system-parameters ip-options

Use **change system-parameters ip-options** to modify the IP-OPTIONS SYSTEM PARAMETERS screen. The RTCP Monitor Server Address fields support the IPv6 addresses.

Syntax

```
change system-parameters ip-options
```

For more information about changing system parameters ip-options, see *Avaya Aura® Communication Manager Screen Reference*.

display system-parameters ip-options

Use **display system-parameters ip-options** to display the IP-OPTIONS SYSTEM PARAMETERS screen. The description of the display system-parameters ip-options screen is the same as the change system-parameters ip-options screen. However, the fields in the display system-parameters ip-options screen are display-only.

Syntax

```
display system-parameters ip-options
```

See **change system-parameters ip-options** for more details.

system-parameters maintenance

change system-parameters maintenance

Use the **change system-parameters maintenance** command to specify and display scheduled maintenance operations and maintenance support functions. It also activates and deactivates INADS alarm origination during repairs. Fields on this screen may differ depending on the configuration of the system (duplicated or not).

Syntax

```
change system-parameters maintenance
```

change system-parameters maintenance field descriptions — page 1

Field	Description
Operations Support Parameters	
CPE Alarm Activation Level	Indicates the minimum level (Major, Minor or Warning) to activate Customer-Provided Equipment (CPE) alarm. If the level is none, the CPE does not activate for any alarm. When the switch goes into Emergency Transfer, the CPE alarm activates regardless of the CPE Alarm Activation Level setting.
Scheduled Maintenance	
Start Time	Hour and minute (24-hour notation) when daily scheduled maintenance starts.
Stop Time	The hour and minute when scheduled daily maintenance ceases. If any daily maintenance operations are not completed by this time, the system notes its stopped sequence location and includes those operations during the next scheduled daily maintenance.
Save Translation	Indicates days that translation data in memory automatically saves to the hard disk during scheduled maintenance. The operation saves to disk, then completes a backup to tape. Translation data saves to both servers. If you set the field value as <i>n</i> , the system does not save the translations automatically.
Update LSP and ESS Servers When Saving Translations	The values of this field are: <i>y</i> — update the LSP and ESS servers when saving translations <i>n</i> — do not update the LSP and ESS servers when saving translations Enable filesync to Survivable Remote Server and Survivable Core Servers during scheduled maintenance save translations.
Command Time-out (minutes)	Displays the time in which the command times out. The values of this field are in the range 10–360. Enter the number of inactive minutes after which an active SAT screen reverts to a Linux screen or the user is logged off of the system. Default is 120.
System Resets	
Display Warning Prior to System Reset?	The values of this field include: <i>y</i> — displays a warning prior to a system reset <i>n</i> — does not display any warning prior to a system reset

change system-parameters maintenance field descriptions — page 2

Field	Description
Minimum Maintenance Thresholds (Before Notification)	

Table continues...

Field	Description
MMIs	The minimum number of MMI ports needed for the Multimedia Call Handling (MMCH) feature to run efficiently. The MMCH feature must be enabled on the system-parameters customer-options screen before the MMIs field can be changed to a number greater than zero. If the number of in-service Multimedia Interface (MMI) ports falls below the minimum port capacity (valid entries between 0–128), a MMI-LEV error is logged. Each MMI media module contains a maximum of 32 ports. To alarm the first occurrence of an MMI being taken out of service, set this field to the total number of MMI ports. If this outage continues for 15 minutes, a major alarm is raised.
VCs	The minimum number of VC ports needed for the Multimedia Call Handling (MMCH) feature. The MMCH feature must be enabled on the system-parameters customer-options screen before the VCs field can be changed to a number greater than 0. Each VC media module contains 16 physical ports: eight ports are reserved for VC-DSPPT ports, and the remaining eight ports are designated as VC-SUMPT ports. The eight DSP ports are made up of four encoder and four decoder resources that encode and decode audio formats. Thus, one VC media module is required for every eight ports of MMCH port capacity. If the number of in-service VC ports falls below the MMCH port capacity (valid entries between 0 and 128), a VEC-LEV error is logged. To alarm the first occurrence of a VC port being taken out of service, set this field to the total number of VC ports. If this outage continues for 15 minutes a major alarm is raised.
Terminating Trunk Transmission Test (Extension)	
Test Type 100	Specifies extensions assigned to receive tie-trunk calls from other switches that have test line origination capability. The system responds by sending a sequence of test tones. Test Type 100 tests far-end to near-end loss and C-message by sending: • 5.5 seconds of 1004 Hz tone at 0 dB • Quiet until disconnect; disconnect is forced after the administered timer interval
Timer	When Test Type 100 is administered, you can change the default testing length for the test call in the Timer field. The field value range is 65–999 seconds. The default value is 65 seconds.  Note: When an extension is added for Test Type 100 that is meant for Central Office trunks configured on media module board in an H.248 media gateway, you must increase the timer to 300 seconds for complete test coverage.

Table continues...

Field	Description
Test Type 102	Test Type 102 tests far-end to near-end loss by sending: • 9 seconds of 1004 Hz tone at 0 dB • 1 second of quiet • This cycle is repeated until disconnect; disconnect is forced after 24 hours.
Test Type 105	Test Type 105 tests 2-way loss, gain slope, and C-message and C-notch noise by sending: • 9 seconds of 1004-Hz tone at -16 dB • 1 second of quiet • 9 seconds of 404-Hz tone at -16 dB • 1 second of quiet • 9 seconds of 2804-Hz tone at -16 dB • 30 seconds of quiet • ½ second of 2225-Hz test progress tone • approximately 5 seconds of quiet • forced disconnect
ISDN Maintenance	
ISDN-PRI Test Call Extension	Indicates the extension used by far-end ISDN nodes to place calls to the system, for testing ISDN-PRI trunks between the far end and the system.
ISDN-BRI Service SPID	Shows if the link associates with the Service SPID. If the link is associated with the Service SPID. This number is the test SPID (0–99999) (under BRI-SET MO). Otherwise, this field is blank. Service SPID is a feature used by the system technician to check building wiring between the switch and the BRI endpoint.
DS1 and MF Maintenance	
DS0 Loop-Around Test Call Extension	The extension used to set up a DS0 loop-around connection for testing non-PRI DS1 trunks. Use DS0 Loop-Around Test Call to test DS0 channels associated with non-PRI trunks. Activate the loop-around by dialing the test extension. Establish multiple DS0 loop-around connections by placing multiple calls to the loop-around extension. For more information, see the DS0 Loop-Around test section in <i>Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers</i>.

Table continues...

Field	Description
MF Test Call Extension	Enter the multifrequency test call extension. To allow COs in different locations to use different DID numbers to reach the MF test call extension, administer one number as the MF test call extension. Administer additional DID numbers as x-port stations, and call forward from the x-port stations to the MF test call extension.

change system-parameters maintenance field descriptions — page 3

Field	Description
Maintenance Save Translation Corruption Audit	
Enable Translation Audit	The values of this field include: • y — enables translation audit • n — disables translation audit Set to y to have a translation audit performed prior to every scheduled save translation operation. A translation audit detects corruption in the translation data. y applies when Save Translation on the first page of this screen is y.
Display Warning When Detected	The values of this field include: • y • n Display a warning on the SAT at login if translation corruption is detected by a translation audit. Write the event to the command history log. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.
Alarm When Detected	The values of this field include: • y • n Issue an alarm if translation corruption is detected by a translation audit. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.

Table continues...

Field	Description
Block Save Translation When Detected	The values of this field include: • y • n Block the save translation command if corruption is detected. The default field value is n. Set to y when translation corruption is actively being diagnosed. Displayed when Enable Translation Audit is set to y.

display system-parameters maintenance

Use **display system-parameters maintenance** to display translation data for maintenance-related system parameters.

Syntax

```
display system-parameters maintenance [ schedule ]
```

schedule Specify a time to run the command.

A series of maintenance tests and operations runs automatically every day according to the schedule and settings specified in the following fields.

See **change system-parameters maintenance** for field descriptions.

system-parameters ms-recovery-rule

change system-parameters ms-recovery-rule

Use **change system-parameters ms-recovery-rule** to set the rules for media server recovery.

Syntax

```
change system-parameters ms-recovery-rule
```

Field description

Field	Description
Failover Parameters	
Report Interval	Communication Manager sends a status message to each Avaya Aura[®] MS on the Communication Manager reporting list, which indicates whether Communication Manager is active or inactive for the specific media server. A short report interval increases network traffic and increases the CPU load of Communication Manager and Avaya Aura[®] MS.

Table continues...

Field	Description
Failover Parameters	
Report Expiration	Duration for Avaya Aura® MS to retain the status message. A short report expiration facilitates rapid failover, however increases the risk of unintended failover due to temporary conditions, such as a server reboot.
Fallback Parameters	
Auto Return	Controls the recovery or fallback to the main server. You can set the Auto Return field to any of the following: • yes: The Time Delay field is available. Time delay is the duration for the main server to be connected to Avaya Aura® MS before considering the network stable enough to start the fallback. The fallback to the main server takes a minute or two to fallback, subject to the specified time delay. • no: Starts the recovery manually according to your time of preference. You must type the command enable ms-return. • scheduled: The Day and Time fields are available. You can set the day and time for the recovery of the main server. The recovery occurs at the next occurrence of the specified day and time.

terminal

erase terminal

Use **erase terminal** to erase local data items from 2410 Release 2 and 2420 Release 4 DCP telephones. A system administrator can use erase terminal to reassign a telephone without having a technician erase the data manually. Erase terminal fails if the extension is busy on a call or on a local task.

erase terminal deletes:

- call logs
- speed dial lists
- button labels
- user option settings
- language

Syntax

```
erase terminal x [ log | customizations | all ]
```

x Extension number of the telephone.

log	Erase the call log.
customizations	Erase customizations: call log, button labels, speed dial list, user option settings.
all	Erase all data: call log, button labels, speed dial list, user option settings, language.

test-number

disable test-number

Use **disable test-number** to prohibit selected maintenance tests.

Use **enable test-number** to run a disabled test.

Syntax

```
disable test-number number
```

number Maintenance test number.

enable test-number

Use **enable test-number** to re-enable a specified test that was previously turned off with **disable test**. While disabled, a test cannot be run by background or demand maintenance. Before enabling a test, ascertain why it was disabled, and inform INADS that it has been turned back on.

Use **display disabled-tests** to list all disabled tests.

Syntax

```
enable test-number number
```

number Number of the test to be re-enabled.

Descriptions of each test are displayed under the relevant MO in *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*.

Example

```
enable test-number 102
```

test-schedule

display test-schedule

Use `display test-schedule` to see the test schedule for an S trunk.

Automatic Transmission Measurement System (S) provides advanced maintenance procedures for monitoring system trunk facilities. This system performs transmission tests on system trunks to determine whether trunks are performing satisfactorily.

Syntax

```
display test-schedule
```

display test-schedule field descriptions

Field	Description
Schedule	The current schedule number.
Schedule Time	The hour and minute that the test begins (24-hour time, with 00:00 being midnight). This time must be greater than the current time.
Schedule Date	Month (1 to 12), day (1 to 31), and year on which testing begins (default is the system date). This date must be equal to or greater than the current date.
Schedule Test Days	y next to the days of the week indicates which days of the week this test runs.
Interval	The length of this schedule in weeks. If 0 , the schedule runs on the specified days only once.
OTL Throttle	The number of trunk members (1–4) tested concurrently during a schedule. If this field is set to 1 , the OTL (originating test line) tests each trunk sequentially. If set from 2–4 , the specified number of trunks are tested in parallel.

Table continues...

Field	Description
Test Type	One of the following types of test to be performed on the trunk group/ members in this schedule: • full — runs the most comprehensive test and collects every associated measurement for each TTL type. • supv — performs a supervision test and only confirms the presence of the test set at the far end. No measurements are taken for this test. • no-st — runs the full test, but skips any self-test sequences. This saves about 20 seconds on the type 105 test and does not have any effect on type 100 or 102 tests. • no-rl — runs the full test, but skips any return-loss sequences. This saves about 20 seconds on the type 105 test and does not have any effect on type 100 or 102 tests. • no-st/rl — runs the full test, but skips every self-test and return-loss sequence. This saves about 40 seconds on the type 105 test and does not have any effect on type 100 or 102 tests.
Duration	The maximum number of hours (1 to 24) a schedule can remain active. Schedules continue to run until every trunk group/member for that particular schedule is tested or until the scheduled duration elapses. If the duration elapses before every trunk group/member can be tested, the schedule stops.
Trk Trp	The trunk-group numbers to be tested when this schedule runs. There is no limit to the number of times that a trunk group can be displayed on any particular schedule, or to the number of different schedules in which a trunk group can be displayed. Default is blank.
Bgn Mbr	The beginning member number of the trunk group to be tested; default is 1.
End Mbr	The ending member number of the trunk group to be tested. This value must be greater than or equal to the value of the beginning member field.

testcalls

list testcalls

Use `list testcalls` to generate an Automatic Transmission Measurement System (S) report. S allows the voice and data trunk facilities to be measured for satisfactory transmission performance. The performance of the trunks is evaluated according to measurements produced by a series of analog tests (`test analog-testcall`) and are compared against user-defined threshold values. The purpose of the report is to provide measurement data to help determine the

quality of trunk lines. The measurement report contains data on trunk signal loss, noise, singing return loss, and echo return loss.

The measurements are produced by a set of analog trunk tests (**test analog-testcall**). The tests are initiated by a maintenance demand test or by a set of scheduled tests. The largest portion of these measurements are generated through scheduled testing during system quiet hours (hours where the traffic volume is low). Each trunk test performed by the system stores the results in a database. The trunk measurements in this database reflect the state of each trunk at the time of its last test.

The test analog-testcall test aborts when attempting a test call on these trunk groups:

- ISDN-PRI: The S Summary Report (**list testcalls** command) shows a **0** in the in the Busied Out Trunks field when **test analog-testcall** is run on an ISDN-PRI trunk.
- SIP
- DID
- Any incoming trunk group (transmission tests can only be run on outgoing trunks).

Syntax

```
list testcalls [ detail | summary ][ grp # ][ to-grp # ][ mem # ][ to-mem # ][ port-  
location | result-identifier | not-result-identifier | count n ]
```

detail	Detailed measurement report displayed.
summary	Summary measurement report displayed.
grp #	Measurements for a specific trunk group displayed. When used with the to-grp option, this option is the starting trunk group in a range of user-specified trunk groups.
to-grp #	Measurements for all trunk groups from 1 to the specified to-grp trunk group are displayed. When used with the grp option, this option is the ending trunk group in a range of user-specified trunk groups.
mem #	Measurements for a specific trunk group member displayed. When used with the to-mem option, this option is the starting trunk group member in a range of user-specified trunk group members.
to-mem #	Measurements for all trunk group members from 1 to the specified to-mem trunk group member displayed. With mem, this option is the ending trunk group member in a range of user-specified trunk group members.
port-location	Measurements for a specific trunk circuit (port) displayed.
result-identifier	Filter out the measurement results that do not match the user-specified result. Only measurement results that match the specified result are displayed. Examples of results are pass, marg, fail.

not-result-identifier Filter out the measurement results that do match the user-specified result. Only measurement results that do not match the user specified result are displayed. Examples of results are pass, marg, fail.

count *n* Specify the number of records displayed.

list testcalls detail report field descriptions

Field	Description
Group	Trunk group number selected.
Type	Trunk group type.
Vendor	Vendor of this trunk group.
TTL Type	Kind of test line for this trunk group.
Threshold Values	The list of marginal and unacceptable threshold values defined on the trunk group form. The following fields display on the lower section of the form. Many of the column headings contain the abbreviations FE for far end and NE for near end. These abbreviations define which end took the measurements.
Trk Mem	The trunk member within the trunk group.
Test Date	The month and day this trunk was tested.
Test Time	The time of day this trunk was tested.
Tst Rslt	This field describes the results of the trunk transmission test.
1004Hz-loss Min	Far-to-near and near-to-far measurements of 1004-Hz loss from low-level tone.
1004Hz-loss Max	Far-to-near and near-to-far measurements of 1004-Hz loss at 0 dBm.
Loss dev at 404Hz	Transmission tests at low frequency. These tests measure a maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements.
Loss dev at 2804Hz	Transmission tests at high frequency. These tests measure a maximum positive and negative deviation of +9 and -9 dB from the 1004-Hz loss measurements.
C-msg Noise	Maximum noise interference (in dBrnC: decibels above reference noise, which is B(EQ)10 sup -12E(EQ) watts) terminating on a voice terminal within the voice-band frequency range (500 to 2500 Hz) between 15 and 55 dBrnC.
C-ntch Noise	Maximum signal-dependent noise interference on a line between 34 and 74 dBrnC.
SRL-LO	Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains and the sum of the circuit losses. SRL-LO occurs most often in the frequency range of 200 to 500 Hz.

Table continues...

Field	Description
SRL-HI	Singing return loss from 0 to 40 dB between the sum of the circuit (repeater) gains on a circuit and the sum of the circuit losses. SRL-HI occurs most often in the frequency range of 2500 to 3200 Hz.
ERL	Echo return loss from 0 to 40 dB between the level of signal strength transmitted and the level of signal strength reflected. ERL occurs most often in the frequency range of 500 to 2500 Hz.

list testcalls summary report field descriptions

Field	Description
Trk Grp Num	The trunk group number which is being summarized. Only outgoing or two-way analog trunks will be listed.
Num Of Trks	Total number of members per trunk group.
Last Test Date	Date of the oldest measurement in the trunk group.
Last Test Time	Time of the oldest measurement in the trunk group.
Trunks Passed Transm Test	Number of trunks that have passed the trunk transmission tests.
Trunks Failed Marginal Threshld	Number of trunks that failed a marginal threshold, but not an unacceptable threshold according to the threshold values defined on the trunk group form.
Trunks Failed Unaccept Threshld	Unacceptable threshold administered on the Trunk group form.
Trks In-Use	Number of trunks that were in-use at the time of testing.
Trks Not Test	Number of trunks that were not tested due to error conditions.
Busied Out Trunks	Number of trunks that were busied out at the time. This could be due to hardware problems, incorrect threshold values, etc.

tftp-server

change tftp-server

Use **change tftp-server** to copy a firmware image from the FTP file server into Communication Manager memory. The Local Node Name and TFTP Server Node Name fields support the v6 node names.

Syntax

```
change tftp-server
```

display tftp-server

Use **display tftp-server** to see the status of the TFTP Server, and to verify the status of a firmware image file download.

Syntax

```
display tftp-server
```

See `disable suspend-alm-orig`.

time

display time

Use `display time` to display the system date and time.

Syntax

```
display time [ schedule ]
```

schedule Specify a time to run the command.

display time field descriptions

Field	Description
Day of the Week	The day of the week that the system has stored.
Day of the Month	The numerical day of the month.
Month	The month of the year stored by the system.
Year	The current year stored by the system.
Hour	The hour of the current day.
Minute	The number of minutes into the hour.
Second	The number of seconds into the minute stored by the system.

set time

Use `set time` to show and edit the current day, date, month, year and time kept by the system clock. The second field is set to zero when the time on the clock is altered.

* Note:

When the system clock is upgraded from an earlier release, the daylight savings time rule on the set time screen defaults to 0 (no rule). When you change the daylight savings time rule, the system clock automatically adjusts during the next transition of the rule.

Syntax

```
set time
```

set time field descriptions

These are the fields on the set time input screen. The current time, or default time is displayed in the fields.

Field	Description
Day of the Week	Valid entries are Monday through Sunday.
Day of the Month	1–31 are valid entries. A check for leap year is also made.
Month	January through December.
Year	The year must be saved as translation data and passed to the kernel whenever kernel memory is corrupted (system reboot or cold I restart), or the data is changed.
Hour	0–23 are valid entries.
Minute	0–59 are valid entries.
Second	This field is reset automatically and cannot be altered.
Type	Daylight-savings — daylight savings time Standard — standard time
Daylight Savings Rule	The daylight savings time rule number (0 to 15). Rule 0 is no daylight savings time, and rule 1 defaults to U.S. daylight savings time rule.

trace

list trace media-gateway

Use **list trace media-gateway** to trace gateway registration messages and denial events. The **list trace media-gateway** command traces the following registration messages:

- ServiceChangeRequest
- ServiceChangeReply
- NotificationRequest (only Keep Alives)
- NotificationReply (only Keep Alives)

Syntax

```
list trace media-gateway ip-address ip-address | identifier n
```

ip-address ip-address The IPv4 or IPv6 address of the media gateway.

identifier n The number assigned to the media-gateway.

Example

```
list trace media-gateway ip-address 10.10.10.1
list trace media-gateway identifier 23
```

list trace ras

Use **list trace ras** to see the RAS (registration, admission, status) messages that Communication Manager is processing between:

- servers in a Survivable Core Server configuration
- servers in a Survivable Remote Server/Survivable Core Server configuration
- gatekeepers and endpoints

This can be limited to a single station or expanded to the whole system. It shows registration, keepalive, and unregistration requests.

This information is helpful when an endpoint fails to register. For example, use **list trace ras** for a particular endpoint, then register the endpoint. If no commands are displayed on the output screen, the gatekeeper is not receiving the message from the endpoint. Check for a network problem.

Syntax

```
list trace ras [ ip-address x | ip-stations x | forced_urqs ]
```

- ip-address x** Shows RAS messages between the entity owning the IP address and the recipients of its messages. To monitor registration requests from the Survivable Core Server, use **list trace ras ip-address** to display registration requests from the Survivable Core Server and the associated response from the Main server. The **list trace ras ip-address** command supports the IPv6 addresses.
- ip-stations x** Shows RAS messages between the gatekeeper and endpoints using the extensions specified in the command.
- forced_urqs** Shows some RAS unregistration request (URQ) messages sent by the gatekeeper to force unregister endpoints. Not all gatekeeper-originated URQ messages are captured here. See the denial event log (display events, category — denial) for a complete record.

list trace station

Use **list trace station** to trace the time and activity on a specific station.

Syntax

```
list trace station ext gw-diag n
```

- ext** Station extension.
- gw-diag n** Displays a full set of diagnostic information for V.150.1 calls. *n* is the debug level. If you set *n*=0, the system displays the default output. If you set *n*=1, the system displays a full set of diagnostic information for V.150.1 calls. *n*= 2 through 255 is reserved.

Use **list trace station** to check VPI.VCI data for a specific station. Add **/a** after the extension (**ext/a**) to request -specific trace data.

list trace tac

Use **list trace tac** to trace calls entering and leaving the server via a trunk group. To request additional trace data, follow **tac#** with a slash (/) and then one or more of the qualifiers.

Syntax

```
Enter tac[or tac[/a(all)c(calling #)l(log)m(MST)s(sip)|t(xfr)or[ Q(qsig only) ] ['gw-diag' (0-255) ]
```

a(all)	Captures all incoming and outgoing trunk call traffic tracing the call until the trunk is recorded then restarts to capture the next call. This command can be used in place of the 'c calling#' command to isolate incoming and outgoing call flow. list trace tac 1234/a
c(calling #)	Allows up to 13 digits or x's to match on to trigger the trace to start. To trace a call where the calling number has any digits followed by '538', followed by any digits, followed by the digit '4', followed by any digits execute the following command: list trace tac x538x4x/c
l(log)	to output list trace data to the ECS logs execute the following command: list trace tac1234/l
m(MST)	to clear and enable the MST trace when list trace starts tracing a call and disable the MST trace when exiting the command (must setup MST first) execute the following command: list trace tac1234/m
s(sip)	to output more SIP message detail (verbose mode) execute the following command: list trace tac1234/s
t(xfr)	to transfer trace control from the trunk to answering station execute the following command: list trace tac1234/t

list trace vdn

Use **list trace vdn** to trace vdn (Vector Directory Number) operations. Show the next call that enters the VDN, through all vectors, until the call leaves vector processing. **list trace vdn** command resembles list trace vector, except that **list trace vdn** follows the call through multiple vectors.

See *Avaya Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide* for more information.

Syntax

```
list trace vdn vdn#
```

vdn# Vector directory number.

list trace vector

Use **list trace vector** to trace vector operations. For a specific vector, see the next call that enters the vector, each vector step being executed, and data for steps associated with Best Service Routing until the call leaves the vector.

See *Avaya Call Center Release 4.01 Call Vectoring and Expert Agent Selection (EAS) Guide* for more information.

Syntax

```
list trace vector #
```

Vector number.

traffic

monitor traffic

Use **monitor traffic** to see the current load on specified trunk and hunt groups, the number of trunk group and hunt group calls waiting to be serviced, and the length of time that the oldest call in the group has been waiting.

Syntax

```
monitor traffic trunk-group [ starting-group # ]
monitor traffic hunt-group [ starting-group # ]
```

**trunk-group
starting-group
#**

Number of calls in the queue waiting to be serviced for each trunk group. The number of members in the group and the number of members active on calls are displayed for comparative analysis. Only administered trunk groups up to a maximum of 60 are displayed.

Use **#** to specify the starting trunk group. For example, enter 5 to see trunk groups from group 5 and up.

**hunt-group
starting-group
#**

Shows trunk-group report information plus how long the oldest call in each group's queue has been waiting. Updated every minute. Unadministered hunt groups are blank.

monitor traffic field descriptions

Field	Description
#	Group number for the trunk group or hunt group.

Table continues...

Field	Description
S	The number of members administered for each trunk or hunt group.
A	The number of members in a group that are active on a call. This does not include busied out members.
Q	The length of the queue administered for a group.
W	The number of calls waiting in the group queue to be serviced.
LCIQ	The time, in seconds, the oldest call in the hunt group queue has been waiting to be serviced.

translation

save translation

Use **save translation** to commit the active server translations (volatile) in memory to a file (non-volatile). It either completes or fails. For Linux platforms, the translation file is copied to the standby server by a filesync process.

 Note:

save translation can take up to 5 minutes to complete. Do not press **ENTER** key on the keyboard during this time, or result messages will be lost.

For Duplex server pair servers, the translation file is copied to the standby server by a filesync process. On Survivable Core Server, **save translation** changes only on the main server pair.

Syntax

```
save translation [ all | ess | lsp ]
```

- all** Save translations to all Survivable Core Server, Survivable Remote Server, and the main server pair.
- ess** From the Server, send changed translations to the active server and to the standby for Duplex server pair servers, and to the Survivable Core Server by a filesync process.
- lsp** From the Server, send changed translations to the active server and to the standby for Duplex server pair servers, and to the Survivable Remote Server by a filesync process.

All translation data is kept in volatile system memory or on the hard drive during normal operation. In the event of a power outage or certain system failures, data in memory is lost. **save translation** stores on disk the translation data currently in memory.

When a SAT user issues **save translation** on a duplicated system, translations are saved on both the active and standby servers. If an update of the standby server is already in progress, subsequent **save translation** commands fail with the message:

```
save translations has a command conflict.
```

save translation will not run and an error message is displayed when:

- translation data is being changed by an administration command
- translations are locked by use of the Communication Manager web interface Pre-Upgrade Step.

Run **save translation** as part of scheduled background maintenance or on demand. See **change system-parameters maintenance** for more information.

save translation field descriptions

Field	Description
Command Completion Status	Identifies the success or failure of the command.
Error Code	Identifier for any error that occurred during translation.

trunk

busyout trunk

Use **busyout trunk** to put an entire trunk group or a single trunk-group member in a maintenance busy state, whether it is installed or uninstalled. Entering only the group number busies out every member in the group.

Note:

You must not enter a group number and a slash (/) without a member number, because it busies-out the member with the lowest-numbered port location.

Syntax

```
busyout trunk group# [ /member# ]
```

group# Trunk group number.

member # Number of particular trunk in a group.

monitor trunk

Use **monitor trunk** to see same information as **status trunk**. **monitor trunk** updates the data automatically every minute, or manually with the **UPDATE** key. The terminal login is not dropped when you press **CANCEL** to cancel **monitor trunk**.

Syntax

```
monitor trunk trunk-group# [ hunt-group# ]
```

trunk-group# Trunk-group number.

hunt-group # Hunt group number.

monitor trunk field descriptions

Field	Description
Trunk Group/Member	Trunk group and group member number. (1–99/1–99).
Port	The port location (media gateway slot circuit) for trunks.
Signaling Group ID	If the trunk is ISDN, this field contains the number of the ISDN Signaling Group. Otherwise, this field is blank.
Connected Ports	Port locations (media gateway-slot-circuit) connected to the trunk.
Service State	In-service/active, in-service/idle, out-of-service, out-of-service-NE (Near End), out-of-service-FE (Far End), maint-NE/active, maint-FE/active, maint-NE/idle, maint-FE/idle, pending-in-service, pending-maint, or disconnected. NE (Near End) and FE (Far End) refer to the end of the trunk that has placed the facility in its current state.
Maintenance Busy	Identifies maintenance testing that occurs on the trunk.
CA-TSC State	The state of temporary signaling connections. (connection set up to pass call information over PRI signaling links).

release trunk

Use **release trunk** to remove specified trunk groups or trunk group members from a maintenance busy state. Specifying the group number releases a single group member and the member number; specifying the trunk group number releases members in a trunk group.

Syntax

```
release trunk group# [ /member# ]
```

group # Trunk group number

member # Trunk group member number

status trunk

Use **status trunk** to see information about the current status of a single trunk or of all members of a trunk group. You can also use status trunk to locate facilities with which the trunk is communicating.

* Note:

If you use status trunk for a trunk that uses a 1d interface, you receive different information with status trunk on the near end of the trunk from status trunk on the far end of the trunk.

- If you execute **status trunk** on the near end of the trunk, it correctly indicates whether or not the trunk is in a maintenance state.

- If you execute **status trunk** on the far end of the trunk, it never indicates that the trunk is in a maintenance state. This is because the near end is unable to inform the far end of its maintenance state status.

See **monitor trunk**, which shows the same information as **status trunk** and updates the screen automatically every minute or on demand.

Syntax

```
status trunk group# [ /member#]
```

group# Status all members of the trunk group.

/member # Status a specific member of a trunk group.

status trunk field descriptions — page 1

Field	Description
Trunk Group/Member	Group and member numbers of specified trunks.
Port	The location of the port associated with the trunk.
Signaling Group ID	For ISDN trunks, the number of the signaling group to which the trunk group belongs. For other trunk types, the field is blank.
Connected Ports	Locations of ports currently connected to the trunk.  Note: If a QSIG over SIP trunk call is active on a SIP trunk, the Connected Ports field displays the involved port of the reference trunk. If a QSIG over SIP trunk call is active on a QSIG trunk, the Connected Ports field does not display any ports.
Q-SIP Reference Port	This field works only with the status trunk QSIG-group-number/member-number, where QSIG-group-number is the QSIG trunk group number and member-number is the QSIG trunk group member number. If a QSIG over SIP trunk call is active on a trunk, the system displays the Q-SIP Reference Port field, irrespective of the service state. If the QSIG port is inactive, the Q-SIP Reference port field remains blank.  Note: If the trunk group is not Q-SIP enabled, the Q-SIP Reference Port field is not displayed.

Table continues...

Field	Description
Service State	One of the following states is displayed: in-service/active, in-service/idle, out-of-service, out-of-service-NE (Near End), out-of-service-FE (Far End), maint-NE/active, maint-FE/active, maint-NE/idle, maint-FE/idle, pending-in-service, pending-maint, or disconnected. NE (Near End) and FE (Far End) refer to which end of the trunk has placed the facility in its current state. Explanations of these service states for each type of trunk are displayed in the maintenance object descriptions in the <i>Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers</i> .
Maintenance Busy	Whether maintenance testing is currently being performed upon the trunk.
CA-TSC State	The status of the call-associated temporary signaling connection, if any. A TSC is a temporary connection set up to pass call information over ISDN-PRI signaling links.
Audio Connection Type	Shows ip-tdm, ip hairpin, ip direct, or ip idle.
Audio Switch Port	Shows a virtual port number (that is, one starting with T). If a trunk is in ip-idle state, the Audio Switch Port field is blank.
Media Encryption	Enter aes for Advanced Encryption Standard encryption, standard used by U.S. government to protect sensitive (unclassified) information. Reduces circuit-switched to IP call capacity by 25%. Enter aea for Avaya Encryption Algorithm. Not as secure as AES. Enter none for an unencrypted media stream.

Use **status trunk** to generate a snapshot jitter and packet loss report for a particular trunk-group member.

In this instance, jitter is the variability in the amount of time (in milliseconds) that packets are received over the network. When jitter increases, the user experiences a noisy connection, delays, and a general loss of quality, making speech unintelligible.

If you issue **status trunk** for a non-IP station or the connection is hairpinned or shuffled, then the packet loss and jitter size information (page 2) is not displayed. Refer to *Administering Network Connectivity on Avaya Aura® Communication Manager* for more information.

status trunk field descriptions — page 2

Field	Description
Average Jitter Last Ten Seconds # - more than 255 ms	The average jitter in received packets from the last ten one-second intervals. # — more than 255 ms
Packet Loss per Second Last Ten Seconds * - 100% loss	The ten most recent one-second samples of the lost packet information for the requested endpoint. * — maximum (100%) packet loss per second during the one-second interval. * is displayed when silence suppression is y on the ip-codec-set screen, or when packet loss is 100%.

Table continues...

Field	Description
Out of Order Counter	A count of the number of out-of-order packets detected during the current connection.
SSRC Change for Call	The number of SSRC changes occurring during the current connection.
Last Rx Sequence No.	Last received data packet sequence number.
Last Tx Sequence No.	Last transmitted data packet sequence number.
Worst Case this Call	Jitter — the worst-case, 1-second jitter (ms) experienced during the current connection. Packet Loss — the worst-case, 1-second packet loss experienced during the current connection.
Average this Call	Jitter — the average jitter for the current connection (the running average of all the 1-second intervals during the connection). Packet Loss — the average packet loss number for the current connection (running average of all the 1-second intervals experienced during the connection).
Current Buffer Size	The current jitter buffer size.

test trunk

Use **test trunk** to perform hardware diagnostic tests on an entire trunk group or an individual trunk-group member, depending on the options entered.

Syntax

```
test trunk group# [ /member# ] [ short | long ] [ repeat# | clear ] [ schedule ]
```

group # Administered group number.

member # Administered number identifying a particular trunk within a trunk group.

short Execute a series of nondestructive diagnostic tests.

long Execute a more comprehensive and longer version of the diagnostic tests. This may involve both destructive and nondestructive tests.

repeat # Number of times to repeat the test, between 1 and 100.

clear Repeat the test sequence until the alarm is cleared, or until a single test in the sequence fails.

schedule Specify a time to run the command.

trunk-group

list trunk-group

For information about `list trunk-group`, see 'Trunk Groups' in *Administering Avaya Aura® Communication Manager*.

list measurements trunk-group summary last-hour

Use `list measurements trunk-group summary last-hour` to see the trunk group summary report. Use this report to determine general traffic flow.

Syntax

```
list measurements trunk-group summary last-hour
```

tsc-administered

status tsc-administered

Use `status tsc-administered` to see the operational status of temporary signaling connections (TSCs) administered for a specified signaling group.

Syntax

```
status tsc-administered signaling-group # [ /tsc-index ]
```

signaling-group # Administered signaling group number.

/tsc-index TSC number in the signaling group.

Example

```
status tsc-administered 1 / 2
```

status tsc-administered field descriptions

Field	Description
TSC Index	The administered TSC index (1–759).
TSC State	inactive — the administered TSC is not functioning (D-channel out-of-service, disabled, etc.). active — the administered TSC is up and user information can be exchanged end-to-end. pending-inactive — the TSC is being released. pending-active — the TSC is about to come up.

Table continues...

Field	Description
Establish	This field pertains to the switch responsible for the origination of the administered TSC. as-needed — the TSC is established on an as needed basis. permanent — the TSC is permanently established.
Enabled	y — indicates that the administered TSCs have been enabled.
Congested	A congested state indicates that the network cannot handle the receipt of USER INFORMATION messages for the administered TSC. • y — the administered TSC is congested. • n — the administered TSC is not congested. • clear — the TSC was congested during its active period and the congestion has been cleared.

test tsc-administered

Use **test tsc-administered** to run diagnostic tests on any type of administered TSCs (Temporary Signaling Connections) on a signaling group. A switched services request to run the TSC heartbeat test is also performed.

Syntax

```
test tsc-administered signaling-group # [ /tsc-index ][ repeat # ][ schedule ]
```

- signaling-group #** Administered signaling group number.
- /tsc-index** TSC number in the signaling group.
- repeat #** Number of times to repeat the command, between 1 and 100.
- schedule** Specify a time to run the command.

test tsc-administered feature interaction

Additional data available after running the test. See **status tsc-administered** for how to access additional data.

tti

status tti

Use **status tti** to see the TTI/PSA status screen and see if the TTI background maintenance task is active. If the TTI background maintenance task is active, the screen shows whether TTI ports are being generated or removed, the number of TTI-supported boards that have processed,

and the number of TTI-supported boards that have not yet been processed. The screen also shows the elapsed time since the background maintenance task started.

To activate the TTI background maintenance task, enter `y` in the TTI field on the Feature-Related System-Parameters screen.

Use `status psa` to also see the TTI/PSA status screen. It shows that the status of PSA is dependent on the state of TTI.

Syntax

```
status tti
```

status tti field descriptions

Field	Description
TTI Background Task State	• generating TTI ports • removing TTI ports • suspended • not active • completed - all ports translated — The last background maintenance task completed normally • completed - some ports not translated — The last background maintenance task stopped when resources were exhausted, and some ports were not translated.
TTI State	off — TTI is disabled voice, data — the type of TTI ports that are being generated or removed
# of Boards Completed	Number of TTI-supported media gateway that were processed by the background maintenance task. The ports on a completed media gateway: • if unadministered, were translated as TTI ports • if administered, the administration was removed
# of Boards Left to Process	The number of TTI-supported media modules that were not processed by the background maintenance task.
Percent Complete	A ratio of the of number of media modules completed to the total number of media modules.
Elapsed Time Since Task Started	Elapsed time in hours:minutes:seconds since the TTI background task was started. This field is blank if the task is not active. If the task is completed or suspended, this field shows the elapsed time up to when the job finished or was suspended.

tti-ip-stations

list tti-ip-stations

Use **list tti-ip-stations** to see information on the stations administered as in TTI service.

Stations in TTI service do not show up on the list multimedia ip-unregistered screen.

Syntax

```
list tti-ip-stations
```

user-profile

change user-profile

Use **change user-profile** to change the access permissions of an existing SAT profile. Changes do not affect active SAT sessions, but become effective on new sessions.

The screen name is User Profile. Use **change user-profile-by-category**.

Syntax

```
change user-profile n
```

n Profile number (20–69).

See **add user-profile** for field descriptions.

display user-profile

Use **display user-profile** to display the permissions of an existing SAT profile.

The screen name is User Profile. Also use **display user-profile-by-category**.

Syntax

```
display user-profile n
```

n Profile number (20–69)

display user-profile field descriptions, page 1

Field	Description
User Profile Name	The user-defined profile name, up to 40 characters.

Table continues...

Field	Description
Shell Access	y/n y — users assigned this profile are able to execute <code>go shell</code> from the SAT. This does not affect the user's default login shell in Linux.
Facility Test Call Notification	y/n y — users assigned this profile receive notification at logoff if Facility Test if Notification is still administered. For security, set to y for all profiles.
Acknowledgement Required	y/n y — users assigned this profile must acknowledge that they want to logoff while Facility Test if Notification is still administered.
This profile is disabled	y/n n — the profile is active y — the profile is disabled If changed to y , an existing active login using this profile is unaffected, but any new attempted session using this profile fails. • A login via CLAN receives <code>access denied</code>. • A login via Linux receives an error return code with the message <code>access denied</code> displayed via stderr.
Grant un-owned Permissions	y/n y — If this profile has write access to the user-profile form, users with this profile can grant any permission allowed for profile 18 (customer super user) to other profiles even when this profile does not itself have those permissions. n — users may not grant permissions they themselves do not have.
Extended Profile	y/n , default is n y — extended profile is enabled. If y , the profile has additional access restrictions to the station and vector forms.
Name	Category name. Each category is associated with a unique set of SAT screens. A given object (SAT screen) displays in one category.
Cat	Category.

Table continues...

Field	Description
Enbl	y/n y — enable the category for this user-profile. Category displays y when any object in a category has permissions other than - -. n — disable the category for this user-profile. Category displays n only when all objects in the category have permissions - -. • If the field is changed from n to y, permissions for all objects assigned to the category are set to w--. • If the field is changed from y to n, permissions for all objects assigned to the category are set to --. This field also reflects the settings on pages 2 - x of this screen.

display user-profile field descriptions, page 2 – x

Field	Description
Set Permissions for Category _ to _	Set permissions for only the objects assigned to this specific category. 1. Enter a letter to specify the category to set. 2. Enter the permission. • Set permission entries as read/write for administration and yes/no for maintenance. • A blank character indicates no-change. For example, if the permissions field is set to blank -, all affected objects are set to deny maintenance access but the current access for administration for each object in this category remains unchanged. See the field description for Perm for more details.
Set All Permissions to	Set permissions for all objects in all categories.
Cat (category)	Display only. Letter that corresponds to the category, used for sorting alphabetically by category, as opposed to alphabetically by SAT form command object.

Table continues...

Field	Description
Perm (permissions)	Enter a two-character value, including blank. Set permission entries as deny, read/write for administration and deny, yes/no for maintenance. - The first character specifies access for administration. - (dash) — deny. No access. - r — view only. - w — add, change, remove in addition to view. - The second character specifies access for maintenance. - (dash) — deny. No access to maintenance commands. - m — access to maintenance commands. Setting this field to m requires at least read access for administration. - For example, r- — a user with this profile can use the commands read, display, export, status, and list for the object assigned the r- permission, and no others. wm — grants full access for all commands to the object assigned this permission A blank character indicates no-change. For example, if the permissions field is set to blank -(dash), all affected objects are set to deny maintenance access but the current access for administration for each object in this category remains unchanged. All permission fields on the User Profile pPage 2 – x accept the full range of values (r, w, d) or (w, m) Independent of whether all values apply to the field or not. Settings on these pages are reflected on the Enbl field on page 1 of this screen.
Name	Name of the SAT screen by command object. Display only.

duplicate user-profile

Use **duplicate user-profile** to duplicate an existing SAT profile. **duplicate user-profile x** copies the permissions from profile **x** to a new profile.

Syntax

```
duplicate user-profile x
```

x Number of an existing SAT profile greater than 17.

export user-profile

Use **export user-profile** to export SAT profile files for editing in a program such as Microsoft Excel.

When **export user-profile** is entered, SAT profiles in Communication Manager numbered 20–69 are written to `/var/home/ftp/pub/cmprofiles.txt`. If the file already exists, it is deleted and replaced.

Syntax

```
export user-profile
```

export user-profile file field descriptions

Field	Description
Fields from User Profile screen, page 1:	
first line	Current release
second line	Number of profiles being exported
next lines - x	Profile number and name of the profile, for as many profiles as exist
next line	Profile number and a list of existing SAT profile numbers in ascending order starting with the first existing number after profile 19.
Fields from User Profile screen, pages 2 - x:	
remaining lines	Two columns: - category and feature names as they display on the user-profile forms - object permissions for each profile number

export user-profile error messages

Error Message	Description
<code>/var/home/ftp/pub/cmprofiles.txt create error</code> (the actual file name from the <code>ecs.conf</code> variable <code>cm_profile_export_file</code>)	The file cannot be created.
<code>/var/home/ftp/pub/cmprofiles.txt write error</code> (the actual file name from the <code>ecs.conf</code> variable <code>cm_profile_export_file</code>)	The file cannot be written.

import user-profile

Use **import user-profile** to import SAT profiles numbered 20-69 from the `/var/home/ftp/pub/cmprofiles.txt` file to Communication Manager. You can edit SAT profile information in Microsoft Excel and import the information back into Communication Manager.

- If a profile in the file does not exist in Communication Manager, it is created.

- If a profile in the file already exists in Communication Manager, the profile in Communication Manager is overwritten.
- If profiles exist in Communication Manager that do not exist in the file, they remain in Communication Manager unmodified.

Use **status logins** to see SAT profile assignments.

Syntax

```
import user-profile
```

import user-profile error messages

Error message	Description	Result
 Note: In the following text, the file <code>/var/home/ftp/pub/cmprofiles.txt</code> shall be replaced by the actual file name from the <code>ecs.conf</code> variable <code>cm_profile_export_file</code>.		
<i>/var/home/ftp/pub/cmprofiles.txt does not exist and the import aborted.</i>	The file does not exist.	The import is aborted.
<i>var/home/ftp/pub/cmprofiles.txt not readable</i>	The file is not readable.	The import is aborted.
<i>release mis-match</i>	The first line of the file does not contain a release number that exactly matches the release number of Communication Manager.	The user is prompted as to whether or not to continue. Additional checks will prevent corruption and cannot be overridden.
<i>invalid profile identifier in file var/home/ftp/pub/cmprofiles.txt</i>	The file contains a profile number lower than 20.	The import is aborted.
<i>invalid feature name at line xxx in var/home/ftp/pub/cmprofiles.txt</i> xxx — the file line number where the first error is found.	The feature names do not exactly match in spelling, order and number the existing profile forms in Communication Manager.	The import is aborted.
<i>invalid permissions at line xxx in var/home/ftp/pub/cmprofiles.txt</i>	The feature permissions characters are not valid.	The import is aborted.

list user-profiles

Use **list user-profiles** to see existing SAT profile numbers and profile names in numerical order.

Use **status logins** to see SAT profile assignments.

Syntax

```
list user-profiles
```

list user-profile field descriptions

Field	Description
Profile	Profile number
Extended Profile	y/n y — the Extended Profile field is y on the User Profile (add user-profile) screen.
User Profile Name	Avaya-defined name for Profile numbers 0–19. Customer-defined name for Profile numbers 20–69.

remove user-profile

Use **remove user-profile** to remove an existing SAT profile and its extended profile, if one exists.

When **remove user-profile n** is executed, the selected profile is displayed. Submit the form to remove the profile.

When a profile is removed, SAT sessions using the profile are automatically logged out.

Syntax

```
remove user-profile n
```

n Profile numbers 20–69.

user-profile-by-category**add user-profile-by-category**

Use **add user-profile-by-category** to add a new SAT profile and administer permissions, where **n** is the profile number 20-69.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile.

Set permission entries as read/write for administration and yes/no for maintenance. Also use **add user-profile**.

Syntax

```
add user-profile-by-category
```

For field descriptions, see **add user-profile**.

change user-profile-by-category

Use **change user-profile-by-category** to change the access permissions of an existing SAT profile. Changes do not affect active SAT sessions, but become effective on new sessions.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile. Also use **change user-profile**.

Syntax

```
change user-profile-by-category n
```

n Profile number (20–69).

See **add user-profile** for field descriptions.

display user-profile-by-category

Use **display user-profile-by-category** to display the permissions of an existing SAT profile.

Pages 2 - X contain a list of SAT forms in order by category and alphabetically within category, and the type of access granted to or denied this profile.

The screen name is User Profile. Also use **display user-profile**.

Syntax

```
display user-profile-by-category n
```

n Profile number 20–69.

See **add user-profile** for field descriptions.

video-bridge

status video-bridge

Use **status video-bridge** to view the status of the video bridge.

Syntax

```
status video-bridge number
```

number Video bridge number.

status video-bridge field descriptions

Field	Description
Name	The name configured on the video-bridge screen
Bridge Status	• in-service — the bridge is available • low-resources — the bridge is heavily loaded, but available • call-rejected — the last conference attempt failed • no-resources — the bridge has not reported any resources • trunks-busy — the configured trunks for this bridge are all full or busied out. Check trunk status • out-of-service — check signaling group status  Note: Typically, CM does not use the low-resources and call-rejected bridges. However, if the in-service bridge is unavailable, CM uses the low-resources or call-rejected bridge.
Ports Used	The number of call-legs administered on the video bridge form which CM uses.
Network Region	The network region used to assess the bandwidth requirements of the bridge.
PRIORITY CONFERENCE STATUS	The resources available for priority users (see Class Of Service settings)
Call Rate	The allowed bandwidth usage for the call-legs to a bridge. • Maximum — bandwidth up to the reported rate. • Exact — bandwidth of the reported rate.
Ports Available	The available ports reported by the bridge.  Note: The available ports are bridge dependent and may not match with the CM configuration or the number of endpoints in the conferences, especially if the bridge is supporting multiple CMs.
Conferences Available	The available conferences are reported by the bridge.  Note: The available conferences are bridge dependent and may not match with the CM configuration or the number of conferences underway, especially if the bridge is supporting multiple CMs.
Ports Rsvd per Conf	The number of ports on the bridge that a new conference takes up.

Table continues...

Field	Description
Conference Failure Rate	The number of conferences reverted to the audio-only mode.  Note: Typically, conferences are reverted to the audio-only mode if one or more call-legs to the video bridge are dropped.
Participant Failure Rate	The number of participants who are unable to dial in to the bridge.  Note: If a participant is unable to dial in to the bridge, the call-rejected status is displayed. This status continues to display till the participant is able to make a call successfully.

vector

list usage vector

Use `list usage vector` to see where each vector is used throughout the system.

Syntax

```
list usage vector n
```

n Number between 1 and 8000.

list vector

Use `list vector` to see a list of existing vectors.

Syntax

```
list vector starting number, [count (1-8000)], [schedule]
```

Chapter 3: Linux bash commands

Linux Commands

Introduction

Linux platform commands are executed from the bash shell. These commands provide server information and help troubleshoot problems in the switch and other components.

Linux commands can be found in **/opt/ecs/bin** and **/opt/ecs/sbin**. The user must be logged into the switch as **root** to execute certain bash commands.

Use **-?** to see a description of command options. For example, `fasttop -?` displays the options that can be entered for the `fasttop` command.

acpfindvers

Use **acpfindvers** to display the release string, date, and time for an object located in **/opt/ws** and in which software base the object was built. More than one file can be specified on the command line.

Syntax

```
acpfindvers [ -? ] [ -c ] file1 [file2] ...
```

-?	Display the command option descriptions.
-c	Display only the CDA vintage string for the file(s)
file1 [file2] ...	Display the information for the specified files..

Example

```
acpfindvers pcd
```

aideCheck

Syntax

```
aideCheck
```

Note:

You must enable Advanced Intrusion Detection Environment (AIDE) before running the **aideCheck** command. To enable AIDE, see [setCMAide](#) on page 381.

Description

Use **aideCheck** to perform a file integrity check manually against the AIDE database. After the command is executed, a report is generated on the terminal.

aideDBUpdate

Syntax

Run the following command as a super-user:

```
aideDBUpdate
```

* Note:

You must enable Advanced Intrusion Detection Environment (AIDE) before running the **aideDBUpdate** command. To enable AIDE, see [setCMAide](#) on page 381.

Description

Use **aideDBUpdate** to update the AIDE database when the following tasks are completed on your system:

- Patches are installed.
- Configurations are updated.

⚠ Warning:

If you do not run the **aideDBUpdate** command when the changes are made to your system, the AIDE reports will flag the files and directories as potential security breaches.

When **AIDE** is enabled, it is recommended to go through the following steps when making a change to the system:

- Using the **aideCheck** command, run an AIDE database check to make sure that no unexpected changes are currently present.
- Perform the upgrade or configuration change.
- Run the **aideDBUpdate** command to re-initialize the AIDE database to take into account the recent changes.

almcall

Use **almcall** to:

- set or display the telephone numbers to services
- enable or disable alarm abbreviation on those numbers
- set the interval between retries

Syntax

```
almcall [ -f first-number ] [ -a [y|n] ] [ -s second-number ] [ -b [y|n] ] [ -t timer ] [ -i interval ] [ -? ]
```

-f first-number Set the first dial-out number to **first-number**. The number can have up to 30 digits (0–9) and “,” for pause. Dashes are allowed but are ignored.

- a [y | n]** Set alarm abbreviation on (y) or off (n) for the first telephone number. The default is y.
- s second-number** Set the second dial-out number to **second-number**. The number can have up to 30 digits (0–9) and “,” for pause. Dashes are allowed but are ignored.
- b [y | n]** Set alarm abbreviation on (y) or off (n) for the second telephone number. The default is y.
- t timer** Set the alarm abbreviation timer to the **timer** value. Valid values are between 1 and 24 hours. The default value is 4.
- i interval** Set the interval between retries in minutes. The interval range is between 1 and 20 minutes. The default is 7 minutes. The value 0 is ignored.
- ?** Display the command usage.

Description

almcall with no arguments displays the dial-out numbers, alarm abbreviation, timer, and interval information.

almclear

Use **almclear** to clear specific server alarms, a list of server alarms, or all server alarms within a range. An alarm is referenced by a positive integer called the Alarm ID, which can be found using the **almdisplay** command. **almclear** does not clear Communication Manager alarms.

Syntax

```
almclear [ -a ] [ -n [id | id1, idsl,...idn | idn1-idn] ] [ -? ]
```

- a** Clear all outstanding server alarms.
- n id** Clear a single server alarm with Alarm ID *id*.
- n id1, id2, ... idn** Clear a set of server alarms with Alarm ID numbers *id1*, *id2*, ... *idn*.
almclear -n 1, 2, 3 is a valid command. **almclear -n 1 2 3** is not.
- n id1–idn** Clear a range of server alarms from ID number *id1* to ID number *idn*
- ?** Display the usage statement.

almdisplay

Use **almdisplay** to display the list of outstanding messaging, Communication Manager, and server alarms.

Syntax

```
almdisplay [ -v ] [ -? ]
```

-v Display the description contained in the original alarm string in addition to the outstanding alarms.

-? Display the usage statement.

Description

almdisplay with no options displays the outstanding alarms.

almdisplay field descriptions

Field	Description
ID	Lists the unique Alarm ID assigned to each alarm.
MO	Name of the Maintenance Object that was alarmed.
Source	Displays the abbreviated name of the source which generated the alarm.
On Bd	Display y if the problem is on-board, n if the problem is off-board.
EvtID	Displays the Event ID of the alarm. The Event ID identifies a particular event that occurred on a given source that generated the alarm.
Lvl	The severity level of the alarm: Warning (WRN), Minor (MIN), Major (MAJ).
Ack	Displays Y or N, indicating if the alarm has been acknowledged or not.
Date	The time stamp assigned when the alarm was created.

almenable

Use **almenable** to enable or disable dial-out and SNMP alarm origination.

Syntax

```
almenable [ -d [n] ] [ -s [y|n] ] [ -? ]
```

-d n Set the dial-out alarm origination to **neither** (default). Disable alarming dial-out. Alarm Origination does not occur, reports are not sent to either OSS number.

-s y|n Enable (y) or disable (n) alarming through SNMP. The default is y.

-? Display the usage statement.

almnotif

Use **almnotif** to set the alarming strategy for dial-out.

Syntax

```
almnotif [ -r [y|n] ] [ -c [y|n] ] [ -? ]
```

-r y|n Enable (y) or disable (n) restart notification.

-c y|n Enable (y) or disable (n) clear alarm notification.

-? Display the usage statement.

Description

almnotif with no options display the administration for restart notification and clear alarm notification.

almsnmpconf

Use **almsnmpconf** to administer or display administered information for SNMP alarming to a services organization.

Syntax

```
almsnmpconf [ -d IP ] [ -c community ] [ -b [y|n] ] [ -e [y|n] ] [ -add | -del |  
-mod ] [ -? ]
```

- d IP** Set the IP address *IP* to send SNMP traps.
- b y|n** Enable (y) or disable (n) alarm abbreviation for SNMP.
- e y|n** Enable (y) or disable (n) the trap destination.
- add** Add a new trap destination. A valid IP address is required.
- del** Remove the trap destination. A valid and existing IP address is required.
- mod** Modify an existing trap destination. To modify an IP address, the trap destination must first be deleted, then re-added with the modifications.
- ?** Display the usage statement.

almsummary

Use **almsummary** to display a summary of outstanding Major and Minor alarms against Communication Manager, Messaging, and servers.

Syntax

```
almsummary [ -? ]
```

- ?** Display the usage statement.

almsuppress

Use **almsuppress** to suppress/unsuppress alarm origination or to check the state of alarm suppression. Use this command to stop alarms during troubleshooting operations.

Syntax

```
almsuppress [ -s [y|n] ] [ -t minutes ] [ -? ]
```

- s y|n** Suppress (y) or unsuppress (n) alarm origination for 30 minutes. The default is y.

-t *minutes* Number of minutes to suppress alarm origination, where *minutes* is in the range of 30–120. The default is 30 minutes.

-? Display the usage statement.

authtype

Use **authtype** to verify if a login is authenticated with a password or Access Security Gateway (ASG).

Syntax

```
authtype [ -l ] [ -u login-name ] [ -h | -? ]
```

-l Return status of the ASG lock.

-u *login-name* The *login-name* to check.

-h | -? Display the usage statement.

autosat

Syntax

```
autosat
```

Use **autosat** to run a Communication Manager SAT (System Access Terminal) session.

ClamavUpdate

Syntax

Run the following command as a super-user:

```
sudo ClamavUpdate=<updatemethod>
```

Where <updatemethod> can be one of the following:

- **wget** — Initial configuration is done in this mode. When this mode is used, the probability of successful updates in your network are high.
- **freshclam** — Robust and best mode to use, as it has additional mirror logic.
- **manual** — Used to disable daily updates when there is no network connection.

Description

Use **ClamavUpdate** to identify which method is most suitable for automatic virus and malware definition updates, or to perform a definition update manually if Internet connection is not available in your network.

To identify which method is best suitable for automatic updates, do the following:

- Start by verifying that your DNS servers are setup correctly.
- Then, test the freshclam method. If this method works, use this as the automatic update method for your daily updates. This method is faster and more robust due to additional mirror logic in it.

- If the freshclam method does not work, use the wget method. This method may sometimes be slow, but it works in most networks as long as the DNS settings are correctly configured on your server.

clamscanDaily

Syntax

```
clamscanDaily
```

Description

Use **clamscanDaily** to manually run a virus and malware scan when:

- ClamAV is enabled.
- Any 7.1 SSP greater than RHEL7.2ssp001 is installed.

When you run the **clamscanDaily** command, a scan is initiated and the results appear after few minutes.

cmpasswd

Use **cmpasswd** to create or change a login password.

Syntax

```
cmpasswd username
```

username	The login to create or change.
-?	Display the usage statement.

cmuseradd

Use the **cmuseradd** command to add an administrator account.

Syntax

```
cmuseradd <type> [ -C profile ] [ -P key ] [ -p password ] [-S Limit] username
```

type	The type of account that you want to add: • super-user • nonsuper-user • cm-only • remote
-C profile	The profile for the account that you want to add. You must assign a profile to the account of type cm-only . However, do not assign a profile to the account of type remote .
-P [key]	An ASG-authenticated account. If you do not specify the key on the command line, the system generates the key. Do not use this parameter with -p .

- p [password]** A password-authenticated account. *password* is the encrypted password. Do not use this parameter with *-P*. The *-p* parameter requires an encrypted password. Therefore, you can use the **cmuseradd** command without the *-p* parameter, and then use **cmpasswd** to set the password.
- S Limit** The limit for the number of concurrent SAT sessions. You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

Examples

```
cmuseradd super-user username
cmuseradd cm-only -C 20 username
cmuseradd cm-only -C 20 -S 3 username
```

cmuserdel

Use the **cmuserdel** command to delete an administrator account. This command replaces the SAT command `remove login`.

Note:

If you delete an account, the system removes the restriction on the number of concurrent sessions for the account.

Syntax

```
cmuserdel username
```

username The account to delete.

cmusermod

Use the **cmusermod** command to modify an administrator account.

Syntax

```
cmusermod [ -C profile ] [ -P key ] [ -p password ] [ -S Limit ] [-L] [-U] ]-G
<group0>,...,<groupN>] username
```

- C profile** The profile for the account. You must assign a profile to the account of type **cm-only**. However, do not assign a profile to the account of type **remote**.
- P [key]** An ASG-authenticated account. If you do not specify the key on the command line, the system generates the key. Do not use this parameter with *-p*.
- p [password]** A password-authenticated account. *password* is the encrypted password. Do not use this parameter with *-P*. The *-p* parameter requires an encrypted password. Therefore, you can use the

cmuseradd command without the **-p** parameter, and then use **cmpasswd** to set the password.

- L** Lock the account. You must not use this parameter with **-U**.
- U** Unlock the account. You must not use this parameter with **-L**.
- G <group0>,...,<groupN>** A secondary group list. The system accepts the group names on the **profN** screen as Communication Manager profile groups.
- S [Limit]** You can assign up to five concurrent sessions or retain the default value none. If you retain the default value, the restriction on the number of concurrent sessions does not apply to the login. However, the restriction applies to the system.

corevector

Syntax

```
corevector [-l] [-s [-f]] [-c arg] [-?]
```

- l** List the current settings.
- s [-f]** Set [**f** = force] the core dump vector using the arguments noted for the **-c** option.
- c** Clear the core dump vector using the following options:
 - **all** - coredump files on all Communication Manager restarts.
 - **warm** - coredump on warm restart request.
 - **cold2** - coredump on cold2 restart request.
 - **reload** - coredump on reload (reboot) restart request.
 - **insane** - coredump on system insane condition.
 - **single** - coredump on single process restart and killing of **TERMINAL** processes.
 - **trap** - coredump of process that trapped.
- ?** Display the usage statement.

Description

corevector is used to request or clear coredump requests. The core dump files are generated prior to the execution of the restart requested. After the core files are taken, a reload of Communication Manager processes is executed. Specifying a single process restart will also create a core file for terminal processes, e.g., **map**.

When the core files are to be taken, the state of health is lowered to force a server interchange. The system then waits to allow the interchange to occur (all processes are stopped), checks to ensure the standby server is now active, and generates the core files. The core files are only taken on the **ACTIVE** server unless the **-f** (force) option is specified.

In a simplex server configuration, the *-f* option is necessary.

corevector accepts multiple arguments, for example, **corevector-s warm cold2**

custalmopt

Syntax

```
custalmopt [ -d ] [ -m ] [ -a ] [ -h | -? ]
```

- d** Display the current settings.
- m** Report Major/Minor alarms only.
- a** Report all alarms.
- h | -?** Display the usage statement.

Description

custalmopt sets or displays the current customer alarm option report option. This command runs on the active server only, and Communication Manager must be running.

defsat

Syntax

```
defsat
```

Description

Use **defsat** to invoke a Communication Manager SAT session if the incoming TCP port is 5022 or 5023.

dhelph

Syntax

```
dhelph [ command ] [ -? ]
```

- command** Name of the shell command or first character(s) of command.
- ?** Display the command option descriptions.

Description

Enter **dhelph** to display the list of valid Linux commands.

Enter **dhelph command** to display the command options and descriptions for a particular command, such as **dhelph server**.

disp_dup_log

Syntax

```
disp_dup_log [ --hour | -h ] [ --day | -d ] [ --help | -? ] [ #_of_entries ]
```

--hour -h	Display the hourly duplication measurements.
--day -d	Display the daily duplication measurements.
--help -?	Display the usage statement.
#_of_entries	Number of entries to display.

Description

Display logs from the duplicate server.

displaydenialevents

Syntax

```
displaydenialevents [-?]
```

-? Display the usage statement.

Description

Display the denial events in Communication Manager log files, including the event description.

dkill

Syntax

```
dkill [-def] [-a] [-h] [ <proc1> [<proc2>...]]
```

-def	All Communication Manager (defty) processes.
-a	All processes.
-h	Display the usage statement.
<proc1> [<proc2>]	Kill only this process or list of processes.

Description

Use **dkill** to send a kill signal to processes in Communication Manager. This command is generally used with the **-a** option (all) when a system is caught in a state where the **stop all** command failed.

dsat

Syntax

```
dsat [ -h | -? ] [path]
```

-h -?	Display the usage statement.
path	Path to a directory containing a SAT executable.

Description

Use **dsat** to run a Communication Manager SAT session. Use **sat path** to use an alternate SAT executable, where *path* is the path to the directory containing the SAT executable.

EASGManage

Use **EASGManage** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

--enableEASG	Enables Enhanced Access Security Gateway (EASG) authentication.
--disableEASG	Disables EASG authentication.
--enable	Enables EASG authentication only for the Avaya Services logins specified in the <i>user</i> variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft.
--disable	Disables EASG authentication only for the Avaya Services logins specified in the <i>user</i> variable.
--userStatus	Displays the EASG status of the user specified in the <i>user</i> variable.
--listUsers	Lists the available EASG users.
--f	Forces the enable or disable action to run without prompts.
--printDisableWarning	Displays the warning message for disabling EASG on the system.
--printEnableWarning	Displays the warning message for enabling EASG on the system.

EASGProductCert

Use **EASGProductCert** to determine whether the EASG product certificate expires within the specified days and to check the information about the EASG product certificate.

Syntax

```
EASGProductCert [--lessThanDays number_of_days] [--certInfo]
```

--lessThanDays	Determines whether the certificate expires within the number of days indicated by <i>number_of_days</i> .
--certInfo	Displays information about the Enhanced Access Security Gateway (EASG) product certificate.

EASGSiteCertManage

Use **EASGSiteCertManage** to manage the Enhanced Access Security Gateway (EASG) site certificate.

Syntax

```
EASGSiteCertManage [--add pkcs7_file_path] [--saf SAF_string] [--list] [--show installed_pkcs7_name] [--delete installed_pkcs7_name | all]
```

- add** Adds the specified file to the site certificate repository. If you do not use the **--saf** option, the system prompts you to confirm the certificate details and enter a site authentication factor.
- saf** Provides the site authentication factor in the **--add** option, which enables the system to run the command in a noninteractive mode.
- list** Lists all the site certificates that are installed on the system.
- show** Displays information about the specified site certificate.
- delete** Deletes the specified site certificate from the system. You can use the **all** option to remove all site certificates.

EASGStatus

Use the **EASGStatus** command to check the status of the Enhanced Access Security Gateway (EASG) feature.

Syntax

```
EASGStatus
```

encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

Syntax

```
encryptionLocalKey [enable | disable]
```

- enable** Enables the local key store.
- disable** Disables the local key store.

Considerations

You must deploy the application with data encryption.

encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

Syntax

```
encryptionPassphrase [add | change | remove | list]
```

- add** Displays the prompts to add the encryption passphrase.
- change** Displays the prompts to change the encryption passphrase.
- remove** Removes the encryption passphrase.
- list** Displays the encryption passphrase and slot assignment.

Considerations

You must deploy the application with data encryption.

encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

Syntax

```
encryptionRemoteKey [add | remove | list]
```

- add** Displays the prompts to add the remote key server.
- remove** Removes the remote key server.
- list** Displays the remote key server and slot assignment.

Considerations

You must deploy the application with data encryption.

encryptionStatus

encryptionStatus displays information about encryption on the system.

Syntax

```
encryptionStatus
```

Considerations

You must deploy the application with data encryption.

environment

Syntax

```
environment [ -v ] [ -? ]
```

- v** Turn on verbose mode.
- ?** Display the usage statement.

Description

Use **environment** to display reports for environmental sensors such as temperature, fan speed, and voltage.

fasttop

Syntax

```
fasttop [-D] [-L] [-M] [-h | -?] [-o filename] [-d delay] [-c #] [-n lines]
```

- D** Query the HMM overload information.
- L** Do not track threads.
- h | -?** Display the usage statement.
- o filename** Put the output in the specified filename.
- d delay** Display the results every *delay* seconds. The default is 5.
- c #** Number of ticks between looking at /proc.
- n lines** Display the number of lines specified by *lines*.

Description

Use **fasttop** to see occupancy results for Communication Manager processes running on the server. The default screen refresh is 5 seconds.

To exit the command, enter **quit**.

fileserver

Use **fileserver** to enable downloading IP phones software and configuration files from an Avaya Solutions Platform S8300 server. By default, the file server is disabled.

The HTTP/HTTPS file server is available on the Avaya Solutions Platform S8300 server to allow IP phones download of software and configuration files. A system administrator in the “susers” group can use the **fileserver** command to enable or disable the file server. After the command is executed, any administrator in the “susers” group can read, write, or update the files in the `/var/web/fileserver/html` directory.

The file server on Avaya Solutions Platform S8300 supports the following IP phones:

- 46xx H.323
- 96x0 SIP and H.323
- 96x1 SIP and H.323
- 16xx H.323
- J1xx SIP and H.323
- K1xx (Vantage) SIP

 Note:

- If a pre-8.1.1 backup is restored after enabling the file server, then the current settings are not overwritten.
- If the R8.1.1 service pack is removed after the file server is enabled, then the file server will be disabled as the **fileserver** command is no longer available.

Syntax

```
fileserver [-h] [-e [http|https|both]] [-d [http|https|both]] [-q] [-t v1.0|v1.1|v1.2>] [-f] [-l] [-a [SW package]] [-r [SW package]] [-v <SW package>] [-u <file>] [-c <file>] [-i]
```

-h	Print this help message.
-e [http https both]	Enable the HTTP or HTTPS file server or both HTTP and HTTPS file server which is the default if no argument is given.
-d [http https both]	Disable the HTTP or HTTPS file server or both HTTP and HTTPS file server which is the default if no argument is given.
-t v1.0 v1.1 v1.2	Set the minimum TLS version allowed for the HTTPS connections to the file server. By default, file server uses v1.2.
-f	Display all the files available for download.
-l	List the IP phones software packages with status.
-a [package]	Add or activate an IP phones software package to the file server document root directory. Without a parameter, the available packages are displayed for selection.
-r [package]	Remove or deactivate a package from the file server document root directory if active or from the download location, if packed. Without a parameter, the available packages are displayed for selection.
-v [package]	View information about an activated or packed IP phones software package.
-u file	Update or copy a given file to the file server document root. If a path is not given, the default download location <code>~ftp/pub</code> is used.
-c file	Clean up or remove a given file from the file server document root.
-q	Query or print the status of the web file server and its disk usage.

Example

```
fileserver -h
```

Description

This command performs various administrative operations for the HTTP, HTTPS file server available on the Avaya Solutions Platform S8300 server only.

The file server can be used to download new software or configuration files or both to Avaya IP phones.

The HTTP server is available on port 81 and the HTTPS server is available on port 411. Use the HTTPPORT DHCP variable, or manually administer using IP-Address:port to configure the non-standard ports.

It is possible to simply check the current status of the server and the disk space used by the file server using the -q option.

IP phones software packages downloaded using the SMI to the `~ftp/pub` directory can be installed using the -a option and later removed using the -r option. IP phones packages can be listed with the -l option.

IP phone packages must use the standard naming convention: series-IPT-protocol-release-date.zip where protocol is SIP or H323. Release starts with 'R' and series is the IP phone series. For example: 96x1-IPT-SIP-R7_1_5_0-040219.zip

This command can only be executed by 'root' or system administrators in the 'susers' group.

Files

File server root directory: `/var/web/fileserver/html/`

HTTPS certificates directory: `/etc/opt/ecs/certs/web411/`

File server log files: `/var/log/httpd/fileserv_*`

Directory containing downloaded IP phones software packages: `/var/home/ftp/pub/`

filesync

Syntax

```
filesync [-w] [-s | -f | -t | -i | -d | -e | -v] [-Q <TYPE> [NUM]] [-r <TYPE>] [-a <TYPE> <ipaddr>] [-q | -H <TYPE>] [filegroup]
```

Description

Use **filesync** to request synchronization of files from active to standby server(s). You can:

- Specify all files or sets of files.
- Define the type of synchronization.
- Enable, disable, or temporarily inhibit file synchronization.
- Report synchronization status and history.

File synchronization sends translations to a duplicate server, a standby server, or a survivable remote server. File synchronization may take place because of survivable remote server registration or with the following commands:

- **filesync trans** (sends translations to the standby server or the survivable remote servers)

- **loaddisplang** (sends unicode files to the standby server and the survivable remote servers)
- **loadlicense** (sends the license file to the standby server).
- **loadpwd** (in this instance, sends the password files to the standby server and the survivable remote servers).
- **save_trans** (sends translations to the standby server).
- **save_trans lsp** (sends translations to the standby server and the survivable remote servers).
- **server -i** (sends all synchronized files to the standby server before the interchange).

filesync command options

Option	Option description
-w filegroup	Wait for results. Specify <i>filegroup</i> , or <i>all</i> for all groups.
-s filegroup	Run the file synchronization silently. The exit status is the only indication of success or failure. Specify <i>filegroup</i> , or <i>all</i> for all groups.
-t filegroup	Timestamp-based synchronization for the specified filegroup to the duplicate server. Verify the timestamps on all files in the specified sets, and synchronize the file/remote server when: • the file's timestamp is more recent than the last synchronization. • the last synchronization attempt for the set failed. <i>-t</i> is more efficient on the active server. It ensures that if the file is changed locally, it will be synchronized to the other server(s). filesync -t will not correct a corrupted file on the other server. Specify <i>filegroup</i> , or <i>all</i> for all groups.
-i	Inhibit file synchronization temporarily. This command will not exit if given this option, so it should be run in the background as follows: <pre>filesync -i& fs=\$! ***other processing *** kill-HUP \$fs</pre>
-d	Disable file synchronization. No files will be synchronized to or from this server until an enable is given. The disable state persists across Communication Manager restarts and Linux reloads.
-e	Enable or re-enable file synchronization.
-v	Turn on verbose mode. Use with -Q queries.
-q filegroup	Query the status and receive a summary of the most recent synchronization, and synchronize the requested filegroup. Implies -w , wait for a response before returning. Specify <i>filegroup</i> , or <i>all</i> for all groups.
-a <TYPE> <ipaddr> filegroup	Send files to a server of <TYPE> ESS or LSP at the specified IP address. Specify <i>filegroup</i> , or <i>all</i> for all groups.

Table continues...

<code>-Q <TYPE> [NUM]</code>	Query the status of the translation synchronization number [NUM] to the specified servers of type <TYPE>. Display the status for save trans, filesync trans, or nightly maintenance. The default synchronization number is the most recent synchronization. Server <TYPE> may be <code>dup</code> , <code>ess</code> , <code>lsp</code> , or <code>all</code> .
<code>-H <TYPE></code>	Show the history of the last 25 translation synchronizations to specified server types. Displays the history for save trans, filesync trans, or nightly maintenance. Server <TYPE> may be <code>dup</code> , <code>ess</code> , <code>lsp</code> , or <code>all</code> .
<code>-r <TYPE></code>	Send files to the duplicate server and remote servers of a specified type. Server <TYPE> may be <code>dup</code> , <code>ess</code> , <code>lsp</code> , or <code>all</code> .

filesync exit codes

If an error occurs, an explanation of the error is sent to stdout. If the command is successfully sent and any response is received, a description of the status is displayed.

Exit Code	Explanation
0	Successful
2	Synchronization is in progress.
3	Synchronization is currently inhibited or disabled.
4	Pre-script execution returned non-zero status.
5	Post-script execution returned non-zero status.
6	Request was invalid (such as an invalid set name).
7	File error in file set.
8	Duplex server is out of service.
9	An error occurred during file synchronization.
10	A local error occurred.

ftpserv

Syntax

```
ftpserv [-? | -h] [-l] [-o] [-a] [-q] -s ftp [on | off]
```

<code>-l</code>	Lists the services supported by this command.
<code>-o</code>	Display only the services name, not the description.
<code>-a</code>	Display the “active” state of the service.
<code>-q</code>	Query for the state of the service.
<code>-s ftp [on off]</code>	Enable (on) or disable (off) ftp service.
<code>-? -h</code>	Display the usage statement.

Description

Use **ftpserv** to configure ftp access and service. This command works when the user is logged in as root or with **sudo** (i.e., **sudo ftpserv**).

fwdlreason

Syntax

```
fwdlreason [ -a ] [ -c code ] [ -? ]
```

- a** Display the list of all reason codes
- c code** Display the reason for a specific *code*.
- ?** Display command option descriptions.

Description

Use **fwdlreason** to see reason codes for firmware download failures.

hardware_info

Syntax

```
hardware_info [ -D <delimiter> ] [ -W <keyword> ] [-l] [-v] [-w] [-h] [-?]
```

- D <delimiter>** User-defined delimiter for the -w option.
- W <keyword>** Get a particular value.
- l** List the valid keywords for the -W option.
- v** Turn on verbose mode and display all system hardware information.
- h | -?** Display the usage statement.

Description

The **hardware_info** command display the hardware configuration for a server or virtual machine.

Example

```
hardware_info -w [ -D <delimiter> ] [ -v ]
hardware_info -W <keyword> [ -v ]
hardware_info -w [ -v ]
hardware_info -l
```

kernel_opts

Syntax

Run the following command as a super-user:

```
kernel_opts {status | enable | disable}
```

Description

Use **kernel_opts** to change the kernel option flags associated with the Spectre and Meltdown kernel changes. By default, Communication Manager comes up with all the supported option flags enabled. By disabling the flags, you can reduce the performance impact caused by these changes.

You can use the following parameters:

- **status** — Displays the current status of the kernel options.
- **enable** — Enables all flags to provide maximum protection.
- **disable** — Disables all flags to provide maximum performance.

listhistory

Syntax

```
listhistory [-l] [-f filename] [-?]
```

- l** Lists the names of the existing command history log files.
- f filename** Specifies which command history log file.
- ?** Display the command usage.

Description

Use **listhistory** to list the Communication Manager shell commands which alter system administration or environment. **listhistory** displays the most recent command history log file.

loaddisplang

Syntax

```
loaddisplang [-? | -h]
loaddisplang [-q] [-c] [-C] [-s] [-S] [-d] [-f] [filename]
loaddisplang -i[c|s] [d]] [filename]
```

- c** Operate on all custom non-installed telephone message files.
- C** Operate on all custom installed telephone message files.
- s** Operate on all standard non-installed telephone message files.
- S** Operate on all standard installed telephone message files.
- d** Indicates the file in question is user-defined (omission implies default of unicode file).
- f** Indicates the file in question is non-installed telephone message files.
- i** Install a unicode or user-defined file. With no file specifiers, will install all valid unicode files in the ftp directory.

- q** Perform a query of the language tag.
 - With no file specifiers, will query among the installed set of unicode files.
 - With the **-d** option, will query among the installed set of user-defined files.
 - With the **-T** option with filename, will query on the filename for time and date it was installed.

In all of the above cases, precedence is given to the custom file.

-v Display the version.

-? Display the usage statement.

Description

Use **loaddisplang** to query (-q) or install (-i) Unicode/user-defined telephone message files. There is no uninstall option for this command. If the installed files are not satisfactory, the user is expected to either overwrite them by re-running **loaddisplang** or to manually delete the installed files across all servers on which they reside. On Linux platforms, the ftp directory is `/var/home/ftp/pub`. The installation directory is `/etc/opt/defty/i18n/`

loadpwd

Syntax

```
loadpwd [-c directory] [-o file] [-l file] [-i] [-f] [-t] [-L lacfile] [-?]
```

- c directory** The path to the directory that contains the `passwd.conf` and `group.conf` files. These files have the same format as `/etc/group` and `/etc/passwd`. They describe the attributes the logins added by this command will have (uid, home directory, etc.). The default is `/etc/asg`.
- o file** Path to the output file. Default is `/etc/asg/asgfile`.
- l file** Path to the authentication file to be loaded. The default is the newest file in `/var/home/ftp/pub`.
- i** Ignore the config file if the login already exists. By default, logins in the authentication file that already exist on the system are changed so they match what is in the `passwd.conf` and `group.conf` files. This option overrides this behavior.
- f** Force the new authentication file to load even if product ID's don't match.
- t** Test if the authentication file is valid; do not install.
- L lacfile** Only valid with **-t** option. Use this file for the overwrite legality test instead of the installed `lacfile`.
- ?** Display the usage statement.

Description

Use `loadpwd` to run a command-line version of the utility to load the Avaya authentication file (password file) onto the:

- host server
- standby server
- Survivable Remote server

locktrans

Syntax

```
locktrans
```

Description

Use `locktrans` to lock translations so that no save translations can be performed until you use the `unlocktrans` command.

Caution:

This command does not have any options. Entering `locktrans -?` causes the command to lock translations.

logclear

Syntax

```
logclear
```

Description

Use `logclear` to remove logmanager output files from the `/var/log/ecs` directory.

logecho

Syntax

```
logecho -p procname -s[c|h|m|l] -l level | -t type -|message logecho -x procname
logecho -?
```

- p procname** The process name the user wants to display in the log.
- s severity** Severity: c = critical, h = high, m = medium, l = low
- l level** The level mask. The level can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- t type** The type mask. The type can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- Log each stdin line.
- message** The message to log.

- x** Do a `gstTrace_exit` for this process.
- ?** Display command option descriptions.

Description

Use **logecho** to make an entry in the logmanager log. Only the first non-option argument is placed in the log as the message body. Shell quoting can be used to put messages which contain white space. If the argument value is "-", then the standard input is read, and each line becomes an entry in the log.

logfilter

Syntax

```
logfilter [-o] [-a] [-d] [-s] [-l level] [-t type] processname | all
logfilter [-h] [-?]
```

- o** OR in the mask for which levels and types of messages will be logged. The mask can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- a** AND in the mask for which levels and types of messages will be logged. The mask can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- d** Reset the debugging level and type to the original default.
- s** Display a summary of the debugging level and type.
- l level** Sets the mask for which levels of messages will be logged. The mask can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- t type** Sets the mask for which types of messages will be logged. The mask can be entered in decimal, octal (preceded by '0'), or hex (preceded by '0x').
- ? | -h** Display the usage statement.

Description

Use **logfilter** to selectively turn on or off the logging-specific types of messages as well as specific levels of messages for a specific process or all processes. If either the level or type mask is not specified, then its value is left the same. If neither are specified, then the current value of each for each specified process is displayed.

loginreport

Syntax

```
loginreport [ -afhrsvw ] [ -n # ] [ -l { login | all } ] [ -b {begin_time} ] [ -e {end_time} ] [-?]
```

- a** Report only active sessions. Only valid with the **-s** or **-y** options.

- b begin_time** Include sessions starting after this time. *Double quotes are required.* This parameter is optional. If not provided, events from the beginning of the file(s) to the stop time are included. The format is "**mm/dd hh:mm**"
- e end_time** Include activity in the report starting at or before this time. *Double quotes are required.* This parameter is optional. If not provided, all events from the begin time to the current time are included. The format is "**mm/dd hh:mm**"
- f** Produce a report of failed logins.
- n N** Limit the output to N lines.
- n N** Limit the output to N lines.
- r** Display the report with the most recent events listed first (reverse order).
- s** Produce a report of successful logins.
- v** Produce a detailed report of user activity.
- l login | all** Enter a specific user name or `all`. If a specific user name is entered, activity for that single user is included in the report. The default is `all`.
- w** Format the report for the web.
- ? | -h** Display the usage statement.

Description

Use `loginreport` to search for a specific set of log events. This command is intended to display normal user activity and is a starting point only for debugging analysis. At least one report type `[-sfv]` must be specified.

logv logc logw

Syntax

```
logv [OPTIONS]...[LOGS...] [-t time]...[[-a]FILTERS]...[-?]
logc [OPTIONS]...[LOGS...] [-t time]...[[-a]FILTERS]... [-?]
logw [OPTIONS]...[LOGS] [[-a]FILTERS]...[-?]
```

- b** Remove blank lines.
- c** Display the contents of the log. Automatically set if called with `logc`.
- d** Augment timestamps with time delta between entries displayed.
- desp [N]** Output a separator line when the delta between entries is greater than N seconds. The default is one second.
- ls** List the names and sizes of the log files.

-r	Reverse the order to display the latest entry first.
-s	Strip off the timestamp and header of each line.
-st	Leave the timestamp and strip off the rest of the header on each line.
-sd	Format the timestamp as yyyy/mm/dd HH:MM:SS and strip off the rest of the header on each line.
-w	Watch the log (automatically set if called with logw).
-v	Display the version of the command.
-l	Search only the latest file in the log. The default is all files.
-lf file	Assume that file is a log file and read input from it. Multiple -lf arguments may be entered.
-ld dir	Look for log files in the directory dir instead of the default directory.
-clear	Clear the log files (only logmanager files).
-t pattern	Filter events for a particular day/time pattern with the format of yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]
-t range	Filter events for a particular day/time pattern with the format of yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]-yyyy[mm[dd:[HH[MM[SS[mmm]]]]]]
-t today	Display today's log.
-t yesterday	Display yesterday's log.
app-pat	Filter events for a specific application or process (i.e., capro). Multiple application patterns may be specified.
-a	Application patterns following the -a are applied to the output of those preceding the -a . Application patterns following the -a are known to be grep patterns.
-g	Assume application filters are grep patterns instead of application names.
-l	Assume application pattern filters are grep patterns and ignore the case of letters.
--view VIEWNAME	Display the log using the log types and grep patterns associated with the view VIEWNAME . The built-in views are: • ipevt - List IP events (interfaces up/down, telephone/ endpoint registration/ deregistration). • bashhist - Platform command history log.

- **mst** - If enabled via a SAT command, entries to the Communication Manager's message sequence trace (MST) log can be echoed into the debug trace log as well.
- **hwerr** - The events that go into the Communication Manager's hardware error and alarm logs. This needs special deciphering by an external tool.
- **sat** - The System Administration and Maintenance activities performed on Communication Manager's System Access Terminal (SAT).
- **swerr** - The events that go into the Communication Manager's software error log. This needs special deciphering by an external tool.
- **kernel** - Linux kernel debug messages.
- **cron** - Linux scheduled task log.

-? Display command option descriptions.

Description

Use **logv** to merge and edit (vi) the various log files in the system.

Use **logc** to merge and output (cat) various log files to standard output.

Use **logw** to watch the requested log file for changes applying the specified filters. Multiple logs can be specified. The logs are merged and sorted by time. Multiple time patterns and time ranges can also be specified.

Log file name

The log file names are:

Log file name	Description
all	Display all possible logs.
lm	logmanager debug trace log (default).
lxboot	Linux boot message.
lxsy	Linux syslog.
lxsec	Linux access security log.
lxwtm	Linux login/logout/reboot log.
lxxfer	Linux file transfer log.
wd	Watchdog logs.
cmds	Platform command history log.
httperr	HTTP/web server error log.
httpssl	HTTP/web secure sockets layer (SSL) request log.
httpaccess	HTTP/web access log.
cmresetart	Communication Manager restart log (last 16 restarts).
filesync	Communication Manager file synchronization log.
update	System updates/patches

Table continues...

ccsppm	PPM log
siptrace	SIP trace log
ccsmasw	Core Router trace log.

modserv

Syntax

```
modserv [-T] [-v] [ -stat | -off | -once | -respawn | -? ]
```

- T** Turn on verbose mode.
- stat** Return the access status:
 - 0 = access off
 - 1= access on for one call
 - 2= access on for multiple calls
- v** Display current status if -stat option is set.
- off** Turn modem access off.
- once** Turn modem access on for one call.
- respawn** Turn modem access on for multiple calls.
- ?** Display command option descriptions.

Description

Use **modserv** to turn modem access on or off for one or more calls.

setCMHardening

Syntax

Run the following command as a super-user:

```
setCMHardening [-w] <enabled>
```

- [-w]** Add the Web Profiles associated with useradmin, switchadmin, maintenance, and auditor. These can be added later if desired by running this command again.
After the command is enabled, the command cannot be undone.

Description

Use **setCMHardening** to configure a number of system parameters into a hardened state. When you run this command, the system will undergo the following changes:

- Remove console.perms and console.perms.d
- Only allow console access in `/etc/securetty`

- Disable the kdump service for kernel crash monitoring
- Configure password strength and expiration policy
- Configure failed login account locking
- Change ownership of ppp-login shell to root:root
- Restrict audit tool permissions to privileged users
- Restrict crontab permissions to root user
- Remove the unused rasaccess user
- Configure session timeouts to 600 seconds for command line and SMI web interfaces
- Change default lock time for expired accounts to immediate
- Set the maximum polling time for ntp to 1024 seconds
- Start ntpd and verify that it is enabled to start at next boot
- Constrain modules and options used in web server directories

mv_lastlog

Syntax

```
mv_lastlog
```

Description

Use `mv_lastlog` to run the Communication Manager modified version of the Linux lastlog utility.

mv_status

Syntax

```
mv_status
```

Description

Use `mv_status` to generate a report on Communication Manager run status.

ping

Syntax

```
ping <ipaddr> [numpackets]
```

Description

Gets the target host IP address from the user at the command line. The user may elect to send from 1 to 255 data packets to the specified host by indicating the number of packets at the command line. Verifies that a remote host is reachable by sending ICMP echo request packets and waiting for replies. If the number of packets to send is not indicated on the command line, this command will send five data packets to the target host.

pingall

Syntax

```
pingall [ [-s [ServerID]] [-i [cab#][carrier]] [-c count] [-v] [-?]
```

- a** Ping all network entities on the remote sides, including servers, routers, and Procr media modules.
- s ServerID** Ping a specific customer LAN.
- i cab# [carrier]** Ping a specific Procr.
- c count** The number of test messages for each network entity
- v** Turn on verbose mode.
- ?** Display a description of command options

Description

Use **pingall** to verify basic connectivity. **pingall** will ping all Procr media modules.

productid

Syntax

```
productid [ -p ] [ -m ] [ productID ] [ -? ]
```

- p productID** Set this server's Communication Manager productid. The productID is a 10–digit number that starts with **1**.
- m productID** Set this server's Messaging productid. The productID is a 10–digit number that starts with **2**.
- ?** Display the command option descriptions.

Description

Use **productid** to view or set the Product ID for Communication Manager and , Messaging.

If no arguments are entered, **productid** displays the server's product IDs.

raid_status

Use **raid_status** to display the server RAID (Redundant Array of Independent Disks) controller status.

Syntax

```
raid_status -c
raid_status -h
raid_status [-s | -v]
raid_status [-s | -v] -p
raid_status [-s | -v] -n
```

- c** Check for a possible HDD failure and log the failure in syslog.
- h** Display the help message..

- v** Verbose output, display all RAID Controller Data.
- n** Display the number of disk drives.
- s** (Default). Display physical disk drive data, short version.
- p** Display physical disk drive data. Use with -v or -s.
- p -s** (Default). Display short physical disk drive data.
- p -v** Display verbose physical disk drive data.
- n -s** (Default). Display short drive data 1, 2, or -1 (not sure).
- n -v** Display verbose (slot number) number drive data
- ?** Display the help statement.

Description

raid_status -n displays the number of HDD's detected. The return values are:

- **-1 - raid_status -n** will return -1 when it is not clear if both hard drives are plugged in. If this occurs, enter **raid_status -n -v** or **raid_status -p** which displays if both hard drives are present or if one is marked as Failed.
- **Failed** - If a hard drive is shown as Failed, the amber LED on the associated failed hard drive will either be flashing on a regular basis or solidly on. A hard drive may also be marked as Failed if it was pulled live.
- **Interim Recovery Mode** - It is possible that a disk is bad or the server only has one HDD plugged into the server. To determine the server HDD state, enter **raid_status -p -v** or **raid_status -n -v**.

If **raid_status -c** is executed and a disk failure exists, the output will indicate the failed disk

Specifying the following options together is INVALID:

- **raid_status -v -s**
- **raid_status -p -n**

Note:

An unplugged HDD appears as a failed HDD to the RAID controller.

restartcause

Syntax

```
restartcause
```

Description

Use **restartcause** to see a list of Communication Manager restarts, their causes, and whether or not each restart escalated into a higher initialization. Use **restartcause** to help determine when an interchange or reload took place. Restarts are listed in ascending order of time.

Also see `display initcauses`.

Field	Description
Cause	The reason for the restart. • Initialized — System initialization. Internal request = Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. Software request = Typically, software detected an error and automatically requested a restart. • Craft request — A user logged in as craft requested the restart and selected the level through an administration session on the server. • Interchange — A State of Health change caused the arbiter process to initiate the restart. • Interchange-Craft — An administrative session (session -i command, on-demand interchange) caused the arbiter process to initiate the restart. • Internal request — Software requested the restart, usually in response to a server interchange. Internal request restarts are not initiated in direct response to an error and are non-escalating. • Software request — Typically, software detected an error and automatically requested a restart.
Action	The level of the restart. • 1 (Warm) — Communication Manager is restarted. Active calls remain up. • 2 (Cold) — Communication Manager is restarted, translations are preserved, and all calls are dropped. • 4 (Reload) — Communication Manager software is completely reloaded. All calls are dropped, the translations are reloaded, and the hardware is re-initialized.
Escalated	Escalated indicates whether the current restart has been escalated (increased in level) from a previous level. Restarts can be automatically or manually escalated to a higher level. For example, if the software detected an error and could not resolve the error by doing a level 1 restart, it would automatically initiate a level 2 restart.
Mode	State of the server immediately after the interchange, at the time of the restart. Look for a change of mode to help determine when an interchange occurred. • Active — Mode of a simplex server and for a duplex server that is the active server. • Standby — Mode of a standby server in a duplex configuration. • Busout — Mode of a standby server that has been placed out-of-service with a <code>busyout</code> command.
Time	The date and time the restart occurred. The restarts are displayed in descending order.

Error messages

Error Message	Description
invalid argument: <argument>	More than one argument was entered on the command line.
No initfile at ./initcause.log or /var/log/defty/initcause.log	The data file is either missing or unreadable (for example, there is no read permission).
restartcause: Error reading initcausefile, error — <error>	The command encountered a problem reading the data file. The file is either ./initcause.log or /var/log/defty/initcause.log.

rm_download_files

Syntax

```
rm_download_files [ file-to-delete ]
sudo rm_download_files [ file-to-delete ]
```

Description

Use **rm_download_files** to add remove files from the /var/home/ftp/pub directory.

rm_download_files *file-to-delete* attempts to delete the specified file from /var/home/ftp/pub. The file must be present in the directory (or a subdirectory) and must also be a regular file. The file must also be owned by the ftp user to prevent others from deleting files saved by other logins.

The susers group logins must use sudo to have access to this command since the command requires root permission to run.

rtrenice

Syntax

```
rtrenice
```

Description

Use **rtrenice** to change the current login's priority. Useful, but dangerous on a high occupancy customer switch.

Example

```
rtrenice -r 99 $$ (as root)
```

sat

Syntax

```
sat [-? | h] [path]
```

path Use an alternate SAT executable, where path is the path to the directory containing the SAT executable.

-? Display the help message.

-h Display the help message.

Description

Use **sat** to run a Communication Manager SAT (system access terminal) session. Also use **autosat** and **dsat**.

save_trans

Syntax

```
save_trans
```

Description

Use **save_trans** to save translations to the active and standby servers. Equivalent to **save translations** on the SAT. This command has no options.

server

Syntax

```
server [ -i | -if | -c | -b | -r | -q | -o | -? ]
```

- i** Perform an interchange between the active and standby servers.
- if** Perform an inerchange immediately with a forced health-override (potentially dangerous).
- c** Continuously display status updates at 1–second intervals.
- b** Busyout this server if it is in standby mode.
- r** Release this server if it is busied-out.
- u** Pre-update/upgrade step, if active.
- U** Undo the pre-update/upgrade step, if active.
- ?** Display command options descriptions.

Description

Use **server** to display or change server status on a server and to see the status and health of each server, including information regarding:

- duplication
- connectivity status
- shadowing
- status of outstanding major and minor alarms
- how long the servers have been up since the last restart
- state of health (hardware health, process health, control network health)

Use **server** with no options to display the status of the active and standby servers.

setCMAuditd

Syntax

```
setCMAuditd [ -f ] <enabled|disabled>
```

-f Sets the state accordingly without showing information about system performance or SELinux.

Description

Use **setCMAuditd** to enable or disable the operating system level auditing on the Communication Manager server.

Warning:

Using this command will have some impact on system performance. Run this command when the system's performance is not fully utilized.

setCMSelinux

Syntax

```
setCMSelinux [ -f ] <disabled|permissive|enforcing>
```

-f Sets the state accordingly without showing information about system performance.

Description

Use **setCMSelinux** to change the state of Security Enhanced Linux (SELinux) on the Communication Manager server.

Warning:

Using this command will have some impact on system performance. Run this command when the system's performance is not fully utilized.

Note:

1. Turning **selinux** on will automatically enable **auditd** even if **auditd** is not explicitly enabled with the **setCMAuditd** command.
2. When **selinux** is enabled, you must move **selinux** from disabled to permissive before moving to enforcing.

setnic

Syntax

```
setnic -h
setnic [-d] -B <interface>
setnic [-d] -m <10H|10F|100H|100F|1000H|1000F|AUTO> <interface>
setnic [-d] -q <interface>
```

-h Display the help message

-B Boot mode. Invoked from network scripts like ifup

- d** Turn on debug mode
- m** Set < interface > to specified speed/duplex
- q** Query the configured and current speed/duplex setting for < interface >
- w** Web option (only update speed settings in config file)

Description

Use **setnic** to configure Ethernet interface speed, duplex, and auto-negotiation settings on the NIC of a specific server running Communication Manager.

Caution:

If you use **setnic** to query/set the interface Speed/Duplex settings of an interface, that interface will be reset. Be careful about doing this on an active server.

sip-attendant

Syntax

```
list sip-attendant
```

Description

Displays all the SIP stations for which the Attendant field is enabled.

start

Syntax

```
start [ -a ] [ -c ] [ -s app ] [ -? ]
```

- a** Start all applications.
- c** Continually display application status until all applications are fully running.
- s app** Start a specific application.
- ?** Display the command option descriptions and a list of valid applications.

Description

Use **start** to start server applications. A single application or several applications can be specified.

The most common use is **start -ac**.

statapp

Syntax

```
statapp [-c# [-D | -U]] [-d] [-l [#]] [-p] [-w] [-b] [-s app1 [,app2,...]] [-v] [-?]
```

- c#** Continuous update of output every # (1-9) seconds.
- D** Exit continuous update when all processes are DOWN.
- U** Exit continuous update when all processes are UP.
- d** List only applications that are down but expected to be up.
- l** List all possible names of applications and services.
- l#** List the status of all possible applications and services. Show applications at level # (0-9) and below. The default is 0.
- p** List the names and status of processes associated with applications.
- w** Also list applications with status WATCHED by watchdog.
- b** Brief output status - application name and UP/DOWN/OFF status
- s app** List the status of the named applications.
- v** Display the command version.
- ?** Display the command options descriptions.

Description

Use **statapp** to see the status of the server applications.

statuslicense

Syntax

```
statuslicense [-a application] [-e] [-f [ # | field] ] [-v] [-h | -?]
```

- a application** Display the license information for the specified application. application may be:
 - 'CommunicaMgr' — display the license information for Communication Manager. This is the default.
 - 'Messaging' — display the license information for Communication Manager Messaging.
- e** Display Allocation License Status and Expiration Date if Enterprise Wide Licensing is enabled.
- f [# | field name]** Display whether the feature is on or off in the license for a feature field number or feature keyword.
- v** Turn on verbose mode to display more information.

-h | -? Display the command option descriptions and a list of valid applications.

Description

Use **statuslicense** to display license information.

stop

Syntax

```
stop [ -a | -b | -c | -f | -h | -i | -n | -r | -S | -s app | -? ]
```

- a** Stop all applications.
- b** Tell CMO to stop monitoring this virtual computer. Only applicable for vm_blade.
- c** Continually display system status until all applications are DOWN.
- f** Override any warnings or errors encountered with the -a, -h, -r and -s options.
- h** Stop all applications and execute a processor halt.
- i** Immediately stop all applications without allowing them to clean up.
- n** Do not prompt before executing this command.
- r** Stop all applications and execute a processor reboot.
- S** Wait until all applications are stopped. Normally, the stop command returns when the stop request has been received by the system.
- s app** Stop a specific application. Use stop -? for a full list.
- ?** Display a description of command options.

Description

Use **stop** to stop applications. The most common use is **stop -acfn**.

sudo

Syntax

```
sudo
```

Description

Use **sudo**, from a login that is not root, to temporarily run some commands as root.

swversion

Syntax

```
swversion [ -r [root-dir] [-v | -l | -R | -a ]] [-?]
```

- r** Use root2 as the base path.
- r root_dir** Use the specified directory as the base path.
- v** Display the Communication Manager software version string only.
- l** Display the Communication Manager load string only.
- a** Display all fields with the addition of the Application Directory information.
- R** Display the Communication Manager release string only.
- ?** Display the command option descriptions.

Description

Use **swversion** to display the current software version of Communication Manager running on the server, including patches and the last time translations were saved.

systat

Syntax

```
systat [ -b ] [-c# [ -D | -U ] ] [-d ] [ -l#] [-p ] [-w][ -s app1 [,app2, ... ] ] [-v] [-?]
```

- b** Display only the list of application names and their status.
- c#** Continuous update of output every # (1-9) seconds.
- D** Exit continuous update when all processes are DOWN.
- U** Exit continuous update when all processes are UP.
- d** List only applications that are down but expected to be up.
- l** List all possible names of applications and services.
- l#** List the status of all possible applications and services. Show applications at level # (0-9) and below. The default is 0.
- p** List the names and status of processes associated with applications.
- w** Also list applications with status WATCHED by watchdog.
- s app** List the status of the named applications.
- v** Display the command version.
- ?** Display the command options descriptions.

Description

Use **sysstat** to see an update of the processes that are running on Communication Manager.

testcustalm**Syntax**

```
testcustalm
```

Description

Use **testcustalm** to generate a customer-alarms test SNMP trap. No arguments are required. This command tests the health of alarm processing between the system and the receiver.

testinads**Syntax**

```
testinads
```

Description

Use **testinads** to test the connectivity between the system and INADS. **testinads** generates a test alarm, sends it to INADS, and waits for a response. No command options are required.

To run **testinads** directly on the remote maintenance board, enter `sudo /opt/alarms/bin/testinads`

testinadsport**Syntax**

```
testinadsport [ -p [1024-65535]] | [-?]
```

-p -p with no assigned value sets the internal tcp port to a default value of 21111.

-p with a valid value sets the internal tcp port to that value. The valid tcp port values are 1024-65535.

If you enter an invalid port value for -p, the system displays an error message. For example, if you enter an invalid port value such as 65536, the system displays the following error message: Invalid port number 1024-65535.

-? Display the tcp port value usage.

Description

Use **testinadsport** to view, add, or change the tcp port number in the ecs.conf file. **testinadsport** will display the current value of the internal tcp port that is used between the GMM and the testinads command.

testled**Syntax**

```
testled [ -a | -d | -s | -? ]
```

- a** Test the LEDs on the server and the duplication memory card.
- d** Test the Trans LED on the duplication memory card.
- s** Test the LEDs on the server.
- ?** Display command option descriptions.

Description

Use `testled` to test the LEDs in the server.

tlscertmanage

Syntax

```
tlscertmanage [ -l ] [ -r # ] [ -i file ] [ -h ] [ -q ]
```

- l** List all CA (Certificate Authority) certificates on the server.
- r #** Remove a CA (specify # 1–8) along with its corresponding file and hash link from the `/etc/opt/ecs/certs/CA` directory.



Caution:

Applications that depend on certificates will not operate properly if the certificates are removed.

- i file** Install a Certificate Authority into Communication Manager's trusted certificate repository on disk. This command:
 1. Copies the certificate file from the allowed location in the `/etc/opt/ecs/certs/CA` directory.
 2. Concatenates the data in the certificate file into the `all-ca.crt` file.
 3. Creates a link to the newly-copied certificate filename with the certificate's hash.

The full path to the file must be specified, e.g. `tlscertmanage -i /var/home/ftp/pub/newCA.crt`

- q** Quiet mode — limit logging and return codes.
- h | -?** Display the descriptions of the command options.

Description

The `tlscertmanage` (transport layer security certificate management) command facilitates loading a third-party trusted certificate into the Communication Manager repository for use the next time Communication Manager restarts.

CA certificates are now installed from the file system rather than being embedded into the telephony application. When Communication Manager is upgraded from an earlier release, the original Avaya CA certificates are installed. The administrator may then choose to modify the list

of trusted CA certificates used by the Communication Manager telephony application to support third-party identity certificates.

To change the Communication Manager telephony application's CA certificates:

1. Use **tlscertmanage** to modify the list using the options described above.
2. Restart the Communication Manager application (stop -afc, start -ac from the root-level command line).

To identify the latest CA certificates installed in the telephony application, review the Communication Manager log and locate the last section of messages containing the phrase "gip/tls: Loaded trusted CA cert". Each CA certificate installed into the application is recorded in the Communication Manager log, which is viewable using the command **vi log**.

If the application fails to install any or all specified CA certificates, the Communication Manager log will contain one or more of the following error messages (where x is the Communication Manager release number):

- CMx_proc_err: pro=7204, err=201, seq=22145,da1=<n>,da2=<max>. This indicates that the number of CA certificates specified exceeds the number supported by the telephony application. <n> is the overlimit value and <max> is the maximum number of certificates supported. To resolve, use **tlscertmanage** to edit the list, then restart the application.
- CMx_proc_err: pro=7204, err=201, seq=22146,da1=<n>,da2=0. This indicates that a failure occurred when attempting to install the n'th CA certificate into the application. <n> is the index of the CA certificate list item that failed to install. To resolve, use **tlscertmanage** to remove, then re-add the certificate. Once re-added, restart the application.
- CMx_proc_err: pro=7204, err=201, seq=22147,da1=0,da2=0. This indicates that the CA certificate list file, /etc/opt/ecs/certs/CA/all-ca.crt, cannot be opened. This may be due to a user privilege issue or a missing/corrupted file. Use **tlscertmanage** to reconstruct the CA certificate list, then restart the application.

tlscertmanage informs the administrator upon successfully displaying, adding, or removing CA certificate list entries, and notes that a restart of the application is required if the list has changed. It prompts for confirmation before deleting a CA entry and associated CA files from the file system. It returns a warning message if the CA certificate list is empty.

topsting

Syntax

```
topsting [ -e ] [ -C procname ] [-p pid] [-d directory] filename
```

- e** Generate abbreviated core files for all processes.
- C procname** Generate abbreviated core files for a specific procname. This option can be repeated for multiple processes.
- P pid** Generate abbreviated core files for process id (PID). This option can be repeated for multiple processes.
- d directory** The directory where abbreviated core files are to be placed. The default is the current directory.

- p path** path contains a colon-separated list of directory paths used to locate the `exec_file` and any shared libraries. An example would be `-p $MYPJ/_mipslx.O:$BASEPJ/_mipslx.O`
- filename** Name of the mini-core dump file.
- ?** Display the command option descriptions.

Description

Use `topsting` to pull information from a specific mini-core dump, based on the mini-core dump filename. Mini-core dump files are located in `/var/log/defty/dumps`, and are created after traps or buffer exhaustion in the system.

uname

Syntax

```
uname [ -a ] [ --help ]
```

Description

Use `uname -a` display all system information, including the kernel and the node name.

Use `uname --help` to display the list of valid options.

unlocktrans

Syntax

```
unlocktrans
```

Description

Use `unlocktrans` to unlock the “locked” translations and allow successful translation saves.

unused_login_audit

Syntax

```
unused_login_audit
```

Description

Use `unused_login_audit` to lock logins after a period of non-use.

update_activate

Syntax

```
update_activate [ -h ]
```

- h** Display the command options.

Description

Use `update_activate` to activate a previously unpacked update on the server. Updates cannot be activated when a kernel update is in a pending state.

update_deactivate

Syntax

```
update_deactivate [ -h ]
```

-h Display the command options.

Description

Use **update_deactivate** to deactivate a previously activated update on the server. Updates cannot be deactivated when a kernel update is in a pending state.

update_info

Syntax

```
update_info [ -h ]
```

-h Display the command options.

Description

Use **update_info** to see information about a specified software update that is already installed.

update_remove

Syntax

```
update_remove [-a | <update_id> ] [-h | -?]
```

Description

Permanently remove an unpacked (deactivated) update from the server.

Use **update_remove -a** to remove all unpacked updates.

Use **update_remove update_id** to remove a specific unpacked update.

Use **update_remove -h** or **update_remove -?** to display the command option descriptions.

Note:

Communication Manager must be stopped for **update_remove** to complete successfully.

update_show

Syntax

```
update_show [-a] [-c] [-k ] [-u] [-d] [-L] [--everything] [--updateidonly] [-?|-h|--help]
```

-a Display activated updates.

-c Display pending kernel updates.

-k Display all kernel updates.

-u	Display all unpacked updates.
-p	Display packed updates.
-L	Display load-specific updates only.
--everything	Display all updates.
--updateidonly	Display only the updated ID names.
-? -h --help	Display the command option descriptions.

Description

Use `update_show` to display information about a specified software or kernel update.

update_unpack

Syntax

```
update_unpack [-L or <update-name.tar.gz>]
```

Description

This command unpacks the specified packed update or lets you select from a list of packed updates. Updates can only be unpacked if they are packed.

Use `update_unpack -L` to list only load-specific updates.

Use `update_unpack update-name.tar.gz` to unpack a specific update.

setCMAide

Syntax

Run the following commands as a super-user:

```
setCMAide <enabled|disabled>
```

Description

Enable the `setCMAide` to configure the Advanced Intrusion Detection Environment (AIDE) to generate a report every night for any modified system files. When the `setCMAide` is enabled, a cron job is set up that will run every night to check the system state. Additionally, the initial AIDE database is also created to provide a base to compare against for the system state check. When the `setCMAide` is disabled, AIDE is turned off. Results are sent to `/var/log/messages`.

setCMClamav

Syntax

Run the following commands as a super-user:

```
setCMClamav [-u <freshclam|wget|manual>] <enabled|disabled>
```

-u Allows you to specify the database update type.

- **freshclam**: Uses mirrors to download the updates most efficiently, but does not work in every network
- **wget**: If DNS settings on the server are setup correctly and internet access is available, this method will usually work. However, it does not always use the most efficient mirror, and as a result it can be slow sometimes.

The "wget" method is enabled by default.

- **manual**: Does not put any update cron job in place. Use this method if your server does not have internet access.

In 7.1.x release, you must install a service pack with the ClamAV RPMs before ClamAV starts working. After the SSP is installed with RPMs, the system is configured automatically to start the scan every night. Use **ClamavUpdate** to change the method used for automatical virus/malware definition updates, or to perform a manual definition update if there is no Internet connectivity in your network.

Description

Use **setCMClamav** to scan the system every night for viruses and malware. Results are sent to `/var/log/messages`.

userlock

Syntax

```
userlock [-t tries] [-o lockout] [enable] [disable] [settings] [[-u login] unlock] [[-u login] status] [-?] | [-h]
```

- t tries** The number of sequential failed login attempts when the account becomes locked out. The default is 5.
- o lockout** The number of seconds to lock out an account. The default is 600 seconds.
- enable** Enable the security software that locks out accounts.
- disable** Disable the security software that locks out accounts. The current settings of `tries` and `lockout` are preserved upon the next `enable`.
- settings** Display if the feature is enabled or not, the value for the number of unsuccessful login attempts, and for how long a login should be locked out.
- unlock** Unlock all locked-out accounts, or just the specified login if `-u login` is used.
- status** Display the lockout status of all accounts, or just the specified login if `-u login` is used.
- u login** Unlock or display status on this login only.
- ?|-h** Display the help message.

Description

Use **userlock** to configure the security software used to lock out login accounts where too many unsuccessful login attempts have occurred. This command also unlocks accounts that have been locked out by the security software.

vilog

Syntax

```
vilog [ -q ]
```

-? Display the usage statement.

Description

Use **vilog** to run the vi editor and to open current Communication Manager log files.

Use **vilog-?** to display the usage of a command.

wlog

Syntax

```
wlog -?
```

-? Display the usage statement.

Description

Use **wlog** to run the vi editor and to open current Communication Manager log files.

xlnrecovery

Syntax

```
xlnrecovery [-d] [-i ] [-?]
```

-d Set the translation recovery strategy to deferred.

-i Set the translation recovery strategy to immediate.

-? Display the usage statement.

Description

xlnrecovery provides the ability to display or set the translation recovery strategy stored in the system configuration files. There are currently two supported translation recovery strategies: immediate and deferred. The recovery strategy is applied during a system restart when Communication Manager detects that the restart has interrupted a translation transaction and has left the translation corrupted.

The **immediate** recovery strategy escalates the current system restart to a higher restart level that forces translation to be read from the disk to eliminate the corruption. This is the default strategy.

The **deferred** strategy just sets the translation corruption flag and continues execution of the current restart level. Setting the corruption flag prevents the corrupted translation from being saved to the disk file. At some later time, a system restart can be executed to force translation to be read from the disk to eliminate the corruption. This strategy allows the user to select a convenient time for the system restart.

Chapter 4: Related Media Gateway CLI Commands

set mgc list

The mgc stands for Media Gateway Controller. Use command `set mgc list` to check if there is an entry that starts as “sbc@xxxx”. This sets the value of the parameter of gateway mode into **Edge Mode** which then disables the Ephemeral Cached VoIP connections.

Syntax

```
set mgc list
```

Chapter 5: Resources

Communication Manager documentation

The following table lists the documents related to Communication Manager. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Design		
<i>Avaya Aura® Communication Manager Overview and Specification</i>	Provides an overview of the features of Communication Manager.	Sales Engineers, Solution Architects
<i>Avaya Aura® Communication Manager Security Design</i>	Describes security-related issues and security features of Communication Manager.	Sales Engineers, Solution Architects
<i>Avaya Aura® Communication Manager System Capacities Table</i>	Describes the system capacities for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
<i>LED Descriptions for Avaya Aura® Communication Manager Hardware Components</i>	Describes the LED for hardware components of Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
<i>Avaya Aura® Communication Manager Hardware Description and Reference</i>	Describes the hardware requirements for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
<i>Avaya Aura® Communication Manager Survivability Options</i>	Describes the system survivability options for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects
<i>Avaya Aura® Core Solution Description</i>	Provides a high level description for the solution.	Sales Engineers, Solution Architects
Maintenance and Troubleshooting		
<i>Avaya Aura® Communication Manager Reports</i>	Describes the reports for Avaya Aura® Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
<i>Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers</i>	Provides procedures to maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel

Table continues...

Title	Description	Audience
<i>Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers</i>	Provides commands to monitor, test, and maintain Avaya servers and gateways.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
<i>Avaya Aura® Communication Manager Alarms, Events, and Logs Reference</i>	Provides procedures to monitor, test, and maintain Avaya servers and describes the denial events listed on the Events Report form.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Administration		
<i>Administering Avaya Aura® Communication Manager</i>	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
<i>Administering Network Connectivity on Avaya Aura® Communication Manager</i>	Describes the network connectivity for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
<i>Avaya Aura® Communication Manager SNMP Administration and Reference</i>	Describes SNMP administration for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
<i>Administering Avaya Aura® Communication Manager Server Options</i>	Describes server options for Communication Manager.	Sales Engineers, Implementation Engineers, Support Personnel
<i>Avaya Aura® Communication Manager Data Privacy Guidelines</i>	Describes how to administer Communication Manager to fulfill Data Privacy requirements.	Sales Engineers, Implementation Engineers, Support Personnel
Implementation and Upgrading		
<i>Deploying Avaya Aura® Communication Manager in Virtualized Environment</i>	Describes the implementation instructions while deploying Communication Manager on VMware.	Implementation Engineers, Support Personnel, Solution Architects
<i>Deploying Avaya Aura® Communication Manager in Software-Only and Infrastructure as a Service Environments</i>	Describes the implementation instructions while deploying Communication Manager on a software-only environment and Amazon Web Service, Microsoft Azure, and Google Cloud Platform.	Implementation Engineers, Support Personnel, Solution Architects

Table continues...

Title	Description	Audience
<i>Upgrading Avaya Aura® Communication Manager</i>	Describes instructions while upgrading Communication Manager.	Implementation Engineers, Support Personnel, Solution Architects
Understanding		
<i>Avaya Aura® Communication Manager Feature Description and Implementation</i>	Describes the features that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
<i>Avaya Aura® Communication Manager Screen Reference</i>	Describes the screens that you can administer using Communication Manager.	Sales Engineers, Solution Architects, Support Personnel
<i>Avaya Aura® Communication Manager Special Application Features</i>	Describes the special features that specific customers request for their specific requirement.	Sales Engineers, Solution Architects, Avaya Business Partners, Support Personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support > Documents**.
4. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
5. From the **Select Content Type** list, select one or both of the following options:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click > to search for the course.

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A

PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at <https://support.avaya.com> and log in.
2. On the top of the page, in **Search Product**, type the product name.
The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.

For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new service packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to <https://support.avaya.com> and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

For detailed information, see the **Subscribe to E-Notifications** procedure.

Index

A

aca	
list measurements	179
accessing port matrix	388
acpfindvers	337
add	
media-gateway	196
remote-office	254
station	272
user-profile-by-category	333
add announcement	40
add media-server X	
Communication Manager	207
aideCheck	337
aideDBUpdate	338
alarm categories	20
almcall	338
almclear	339
almdisplay	339
almenable	340
almnotif	340
almsnmpconf	341
almsummary	341
almsuppress	341
audits	
clear audits	46
status audits	46
authtype	342
autosat	342
Avaya Aura® application	
supported gateways	17
Avaya InSite Knowledge Base	391
Avaya Media Server	209 , 211
Avaya support website	391

B

busyout	
access-endpoint	27
board	52
campon-busyout	63
cdr-link	74
cti-link	113
data-module	118
ds1-facility	122
journal-printer	168
link	171
mis	217
pms-link	240
port	243
pri-endpoint	245
sp-link	271

busyout (<i>continued</i>)	
station	272
trunk	319
busyout command	20

C

cancel	
hardware-group	140
change	
communication-interface links	77
communication-interface processor-channels	78
cti-link	114
extended-user-profile	136
extension	273
integ-annc-brd-loc	150
ip-codec-set	151
ip-interface	158
ip-network-region	158
logging-levels	175
media-gateway	200
mst	220
public-unknown-numbering	249
remote-office	254
synchronization	290
system-parameters maintenance	300
tftp-server	312
user-profile	327
user-profile-by-category	334
change history	16
change media-server X	208
change system parameters	
system-parameters ip-options	300
changes to platform support	17
ClamavUpdate	342
clamscanDaily	343
clear	
amw all	39
errors	125
isdnpri-testcall	164
mst	220
port	243
cmdHistoryLogConfig	
history	147
cmpasswd	343
cmuseradd	343
cmuserdel	344
cmusermod	344
collection	
delete	389
edit	389
generating PDF	389
sharing content	389

command syntax	18
common error codes	23
common output fields	22
common parameters	21
Communication Manager	209 , 211
content	
publishing PDF output	389
searching	389
sharing	389
sort by last updated	389
watching for updates	389
contention	19
corevector	345
craft2	
disable craft2	113
enable craft2	113
custalmopt	346

D

defsat	346
dhelp	346
disable	
administered-connection	30
announcement-board	42
ess	129
mst	221
nr-registration	226
suspend-alm-orig	289
synchronization	291
test-number	307
disp_dup_log	346
display	
alarms	34
bulletin-board	61
capacity	64
communication-interface links	78
communication-interface processor-channels	80
disabled-tests	121
errors	125
events	135
extended-user-profile	137
failed-ip-network-region	138
hunt-group	148
initcauses	148
logging-levels	176
media-gateway	200
mst	221
node-names	226
port	243
profile-base	248
public-unknown-numbering	250
remote-office	255
signaling-group	259
synchronization	291
system-parameters ip-options	300
system-parameters maintenance	305

display (<i>continued</i>)	
test-schedule	308
tftp-server	312
time	313
user-profile	327
user-profile-by-category	334
display announcement	40
display media-server X	209
display system-parameters customer-options	299
displaydenialevents	347
displaying	
busied-out maintenance object	20
dkill	347
documentation	
Communication Manager	386
documentation center	389
finding content	389
navigation	389
documentation portal	389
ds1	
list measurements	179
dsat	347
duplicate	
ip-network-region	160
user-profile	330

E

EASG	348 , 349
EASGManage	348
EASGProductCert	348
EASGSiteCertManage	349
EASGStatus	349
enable	
administered-connection	30
announcement-board	42
ess	130
filexfer	139
mg-return	216
nr-registration	227
suspend-alm-orig	289
synchronization	292
test-number	307
encryptionLocalKey	349
encryptionPassphrase	349
encryptionRemoteKey	350
encryptionStatus	350
Enhanced Access Security Gateway	348 , 349
environment command	350
erase	
announcement	40
terminal	306
error categories	20
error codes	
common	23
error messages	23
export	

export (<i>continued</i>)	
user-profile	331

F

fasttop	351
fileserv	351
filesync	353
finding content on documentation center	389
finding port matrix	388
ftpserv	355
fwdreason	356

G

get	
ethernet-options	133
go	
shell	258

H

hardware_info	356
history	
notify	147

I

import	
user-profile	331
ip codec	
list measurements	181
ip dsp-resource	
list measurements	183
ip signaling-groups	
list measurements	195

K

KB	
Support site	391
kernel_opts	356

L

Linux commands overview	337
list	
aar route-chosen	26
announcement	41
ars route-chosen	43
audio-group	45
calltype route-chosen	62
coverage path	112
cti-link	115
directory	120
disabled-mos	121

list (<i>continued</i>)	
ethernet-options	134
extension-type	137
history	144
hunt-group	148
ip-network-region	158
isdnpri-testcall	164
location-parameters	174
locations	174
marked-ports	177
mct-history	178
measurements trunk-group summary last-hour	324
media-gateway	201
media-gateway configuration list	111
moh-analog-group	219
monitored-station	220
mst	221
multimedia	223
night-service attendant	224
night-service hunt-group	225
night-service trunk-group	225
off-pbx-telephone station-mapping	234
pms-down	239
public-unknown-numbering	250
registered-ip-stations	252
remote-office	255
set-data	258
signaling-group	261
skill-status	268
station	273
survivable-processor	288
suspend-alm-orig	290
synchronization	292
sys-link	293
testcalls	309
trace media-gateway	314
trace ras	315
trace station	315
trace tac	316
trace vdn	316
trace vector	317
tti-ip-stations	327
usage digit-string	120
usage vector	336
user-profile	332
vector	336
list aar analysis	
aar analysis	25
list ars analysis	
ars analysis	42
list ars route-chosen fields	
common	44
list configuration	
software-versions	111
list directory source	120
list int-annc-sources	41
list media-server	205

list members network-region-group	224
list network-region-group	224
list usage	
audio-group	46
cti-link	116
integ-ann-c-board	150
listhistory	357
loaddisplang	357
loadpwd	358
locktrans	359
logc	361
logclear	359
logecho	359
logfilter	360
loginreport	360
logv	361
logw	361

M

mark	
port	244
media gateway controller list	385
modserv	364
monitor	
bcms	48
health	143
security-violations	256
socket-usage	269
system	294
traffic	317
trunk	319
mv_lastlog	365
mv_status	365

O

output fields	
common	22
overview	16 , 19
overview, Linux commands	337
overview, maintenance commands	16

P

parameters, common	21
PCN notification	393
pin	
change pin	236
reset pin	237
ping	365
ping	237
pingall	365
port matrix	388
productid	366
PSN notification	393

R

raid_status	366
recovery rules	
auto return	305
Avaya Aura Media Server	305
Communication Manager	305
report expiration	305
report interval	305
release	
access-endpoint	27
board	53
cdr-link	74
cti-link	116
data-module	118
journal-printer	168
mis	217
modem-pool	218
pms-link	241
port	244
pri-endpoint	246
sp-link	271
station	274
trunk	320
release command	20
remove	
file	139
remote-office	255
user-profile	333
remove media-server X	
Communication Manager	210
remove signaling-group	263
reset	
aesvcs link	31
board	53
ip-stations	160
login-id	176
media-gateway	202
meet-me-vdn	215
system	296
restartcause	367
resume	
hardware-group	141
rm_download_files	369
rtrenice	369

S

safety labels	18
sat	369
save	
translation	318
save_trans	370
searching for content	389
security alert label	18
server command	370
set	

set (continued)			
ethernet-options	134	status (continued)	
signaling-group	265	sp-link	271
synchronization	293	station	274
time	313	trunk	320
set mgc list	385	tsc-administered	324
set options		tti	325
options	230	status media-server	211
setCMAide	381	statuslicense	373
setCMAuditd	371	stop	374
setCMClamav	381	sudo	374
setCMHardening	364	support	391
setCMSelinux	371	supported gateways	
setnic	371	Avaya Aura® application	17
sharing content	389	swversion	374
signaling-group		syntax	18
list usage signaling-group	262	systat	375
signing up			
PCNs and PSNs	394	T	
simultaneous commands	19	test	
sip-attendant	372	access-endpoint	29
sort documents	389	aesvcs-server	33
start	372	alarms	36
statapp	372	analog-testcall	39
status	334	board	53
access-endpoint	28	cdr-link	76
administered-connection	30	cti-link	116
aesvcs cti-link	31	customer-alarm	117
aesvcs interface	32	data-module	119
aesvcs link	33	ds1-facility	122
attendant	44	ds1-loop	123
bri-port	54	eda-external-device-alm	124
cdr-link	75	failed-ip-network-region	138
cleared-alarm-notif	77	isdnpri-testcall	166
conference	80	journal-printer	169
data-module	118	led	170
ess clusters	131	license	170
hardware-group	141	link	173
health	143	media-gateway	204
ip-network-region	159	modem-pool	218
ip-synchronization	162	pms-link	242
isdnpri-testcall	165	port	245
journal-link	167	pri-endpoint	247
link	171	signaling-group	267
logins	177	sp-link	272
media-gateway	203	station	287
mg-announcements	215	trunk	323
nr-registration	228	tsc-administered	325
off-pbx-telephone station	233	testcustalm	376
periodic-scheduled	235	testinads	376
pms-link	241	testinadsport	376
pri-endpoint	246	testled	376
psa	248	tlscertmanage	377
remote-access	253	topsting	378
remote-office	255	training	390
signaling-group	265		
socket-usage	270		

U

uname	379
unlocktrans	379
unused_login_audit	379
update_activate	379
update_deactivate	380
update_info	380
update_remove	380
update_show	380
update_unpack	381
userlock	382

V

videos	391
viewing	
PCNs	393
PSNs	393
vilog	383

W

watchlist	389
wlog	383

X

xlnrecovery	383