



Net-Net® 4000 Maintenance and Troubleshooting Guide

Release Version S-C6.2.0

Acme Packet, Inc.
71 Third Avenue
Burlington, MA 01803 USA
t 781-328-4400
f 781-425-5077
www.acmepacket.com

Notices

©2002—2009 Acme Packet, Inc., Burlington, Massachusetts. All rights reserved. Acme Packet, Session Aware Networking, Net-Net, and related marks are trademarks of Acme Packet, Inc. All other brand names are trademarks, registered trademarks, or service marks of their respective companies or organizations.

Patents Pending, Acme Packet, Inc.

The Acme Packet Documentation Set and the Net-Net systems described therein are the property of Acme Packet, Inc. This documentation is provided for informational use only, and the information contained within the documentation is subject to change without notice.

Acme Packet, Inc. shall not be liable for any loss of profits, loss of use, loss of data, interruption of business, nor for indirect, special, incidental, consequential, or exemplary damages of any kind, arising in any way in connection with the Acme Packet software or hardware, third party software or hardware, or the documentation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusions may not apply. These limitations are independent from all other provisions and shall apply notwithstanding the failure of any remedy provided herein.

Copying or reproducing the information contained within this documentation without the express written permission of Acme Packet, Inc., 71 Third Avenue, Burlington, MA 01803, USA is prohibited. No part may be reproduced or retransmitted.

Acme Packet Net-Net products are protected by one or more of the following patents: United States: 7072303, 7028092, 7002973, 7133923, 7031311, 7142532, 7151781. France: 1342348, 1289225, 1280297, 1341345, 1347621. Germany: 1342348, 1289225, 1280297, 1341345, 1347621. United Kingdom: 1342348, 1289225, 1280297, 1341345, 1347621. Other patents are pending.

About this Guide

Introduction

The *Net-Net 4000 Maintenance and Troubleshooting Guide* provides the information you need for understanding and troubleshooting the operation of Acme Packet's Net-Net 4000 session border controller.

About Net-Net 4000 Software Releases

Release version S-C6.2.0 is supported on the Net-Net 4000 series platforms. This series contains two systems, the Net-Net 4250 and the Net-Net 4500. S-C6.2.0 also runs on the Net-Net 3000 series of systems. Net-Net 4250 images are titled S-C6.2.0, while Net-Net 3800 and Net-Nt 4500 System images are titled S-Cx6.2.0.

In addition, the Net-Net 3800 also runs the same software as the Net-Net 4500; it also runs an image called S-Cx6.2.0.

Who is Acme Packet?

Acme Packet enables service providers to deliver trusted, first class interactive communications-voice, video and multimedia sessions-across IP network borders. Our Net-Net family of session border controllers satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks. Our deployments support multiple applications-from VoIP trunking to hosted enterprise and residential services; multiple protocols-SIP, H.323, MGCP/NCS and H.248; and multiple border points-interconnect, access network and data center.

Established in August, 2000 by networking industry veterans, Acme Packet is a public company traded on the NASDAQ and headquartered in Burlington, MA.

Related Documentation

The following table lists related documents.

Document Name	Document Description
Net-Net 4250 Hardware Installation Guide (400-0003-00)	Contains information about the components and installation of the Net-Net 4250 SBC.
Net-Net 4500 System Hardware Installation Guide (400-0101-00)	Contains information about the components and installation of the Net-Net 4500 system.
Net-Net 3800 Hardware Installation Guide (400-0118-00)	Contains information about the components and installation of the Net-Net 4500 system.

Document Name	Document Description
Net-Net 4000 Storage Module Installation Guide (400-0133-00)	Contains information about how to install the storage expansion module in your Net-Net 3800 or 4500.
Net-Net 4000 Configuration Guide (400-0061-00)	Contains information about the administration and software configuration of the Net-Net SBC.
Net-Net 4000 ACLI Reference Guide (400-0062-00)	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Net-Net 4000 Maintenance and Troubleshooting Guide (400-0063-00)	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
Net-Net 4000 MIB Reference Guide (400-0010-00)	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Net-Net 4000 Accounting Guide (400-0015-00)	Contains information about the Net-Net SBC's accounting support, including details about RADIUS accounting.
Net-Net 4000 Administrative Security Essentials (400-0132-00)	Contains information about the Net-Net SBC's support for its Administrative Security license.
Net-Net 4000 Border Gateway Essentials (400-0087-00)	Contains the following information about the Net-Net Border Gateway (BG): conceptual, configuration, and monitoring

Technical Assistance

If you need technical assistance with Acme Packet products, you can obtain it on-line by going to <https://support.acmepacket.com>. With your customer identification number and password, you can access Acme Packet's on-line resources 24 hours a day. If you do not have the information required to access the site, send an email to tac@acmepacket.com requesting a login.

In the event that you are experiencing a critical service outage and require live assistance, you can contact the Acme Packet Technical Assistance Center emergency hotline:

- From the United States, Canada, and Mexico call: 1 866 226 3758
- From all other locations, call: +1 781 328 4400

Please note that a valid support/service contract with Acme Packet is required to obtain technical assistance.

Customer Questions, Comments, or Suggestions

Acme Packet is committed to providing our customers with reliable documentation. If you have any questions, comments, or suggestions regarding our documentation, please contact your Acme Packet customer support representative directly or email support@acmepacket.com.

Contact Us

Acme Packet
71 Third Avenue
Burlington, MA 01803 USA
t 781 328 4400
f 781 425 5077
www.acmepacket.com

Contents

About this Guide	iii
Introduction	iii
About Net-Net 4000 Software Releases	iii
Who is Acme Packet?	iii
Related Documentation	iii
Technical Assistance	iv
Customer Questions, Comments, or Suggestions	v
Contact Us	v
 1 Logs	 27
Introduction	27
About Logs	27
Logging Events	27
Event Categories	28
About Events	28
Types of Events	28
Process Log Events	28
System Log Events	29
Protocol Trace Events	29
Event Granularity	29
Event Severity	30
SNMP Traps	30
Alarms	30
Process Log Events	31
System Log Events	31
Traps	31
Alarms	31
Working with Logs	32
Writing to Logs	32
Manually Rotating Logs	32
Working with Logs Example	32

Displaying List of Log Files	33
Viewing Logs.	33
Viewing a Specific Logfile	34
Dynamically Changing Log Level	35
Requesting Log Level Data	36
ACLI show loglevel Command	36
ACP	37
Wildcarding Task Name and Log Type.	37
Specific Task with Wildcard Log Level	39
Specific Task and Log Level Type	40
Log Files	42
log.sysmand.	42
log.bootstrap	42
log.berpd	42
log.brokerd.	42
log.lemd	42
log.algd.	42
log.mbcd	42
miboco.log.	42
log.radd	43
log.h323d	43
log.sipd.	43
sipmsg.log	43
log.acli	43
log.acliConsole	43
log.acliTelnet0-4	43
log.SSH0-4.	43
log.tCliWorker.	43
syslog	43
Process Logs	44
HA Switchover Log	44
Log Message Graphical Display on Net-Net SBC.	44
2 Fault Management.	45
Overview	45
Accessing Fault Management Data.	45
About Traps.	45
Standard Traps	46
Enterprise Traps	46
About Alarms	48
Overview	48

Types of Alarms	48
About the Alarm Process	48
About Alarms and the Health Score	49
ACLI Instructions and Examples	49
Displaying Alarms	49
Clearing Alarms	50
About the Alarm Display on the Chassis	50
Alarm Severity Levels	50
Net-Net SBC Response to Alarms	51
Writing to syslog (acmelog)	51
Sending SNMP Traps	51
About Dry Contacts	51
Displaying Alarms to the Chassis	52
Hardware and Environmental Faults	52
Hardware Temperature Alarm	52
Fan Speed Alarm	53
Environmental Sensor Alarm	53
Media Link Alarms	54
Power Supply Alarms	54
Voltage Alarms	55
Physical Interface Card Alarms	55
Viewing PROM Statistics (Net-Net SBC 1 only)	56
Graphic Window Display	57
Fan Stopped Alarm	57
Temperature High Alarm	57
System Fault Statistics	58
System State	58
Viewing System Uptime	58
Viewing System State	58
System Resources	58
Viewing CPU Usage	58
CPU Utilization Alarm	59
Memory Usage	59
Viewing Memory Usage Statistics	59
Checking Remaining Boot Directory Space	60
Viewing Memory Buffer Statistics	60
Memory Utilization Alarm	61
License Capacity	61
Configuration Statistics	61
Specifying a Configuration Element	62
Viewing Current Configuration	63
Viewing Running Configuration	63

Viewing Realm-Specific Configuration	64
Configuration Save Failed Alarm.	67
HA Functionality	67
Viewing Health Information	67
Viewing Redundancy Information.	68
HA Alarms	69
Base Display Level	71
HA State Display Stats	71
Initial State Displays	71
Out Of Service State Displays	72
Becoming Standby State Displays	72
Standby State Displays	72
Active State Displays	72
ARP Functionality	72
Testing Address Resolution	72
Viewing Current Address Mappings	73
ARP Table Utilization Alarm	74
Local Policy	74
Viewing Running Configuration Local Policy	74
Viewing Current Configuration Local Policy	74
Viewing Runtime Protocol Tracing	75
Viewing Real-Time SIP Session Statistics	76
Media and Bandwidth Statistics	77
Viewing MBCD Task Errors	77
Viewing Steering Port and Bandwidth Usage	79
Viewing Real-Time Media Monitoring Statistics	79
Media Alarms	80
Task Statistics	81
Viewing Function Call Stack Traces	81
Viewing the Stack Trace	81
System Task Suspended Alarm	83
System Problem Statistics	83
Packet Tracing	83
Capturing and Viewing Packets.	83
System ACLs	86
Notes on Deleting System ACLs	86
Viewing System ACL Configurations	86
Viewing System ACL Statistics	86
Phy Link Redundancy	87
Viewing Redundancy Link Information	87
Wancom Port Speed and Duplex Mode Display	88
Application Faults	88
H.323 Statistics	88

Viewing H.323 Statistics	88
H.323 Stack Initialization Failure Alarm	89
H.323 Monitoring Stack Alarm	89
MGCP Statistics	90
Viewing MGCP Errors	90
Viewing MGCP Processes	91
MGCP DNS Failure Alarm.	91
MGCP Congestion Control Information	91
MGCP Endpoint Inactivity.	92
SIP Statistics	92
Viewing SIP Errors	92
Viewing SIP Processes	93
Viewing IP Session Replication for Recording (SRR) Information	93
Viewing SIP Registration Cache Status	93
SIP NSEP Statistics	94
NSEP Statistics per R-Value Display.	94
Viewing NSEP Burst Statistics for SIP Session Agents	95
Resetting NSEP Statistics	95
Viewing SIP Method Throttling Mechanism Statistics	96
Viewing SIP IP CAC Statistics	97
Viewing SIP PUBLISH Statistics	97
RADIUS Statistics	97
Viewing RADIUS Statistics	97
RADIUS Connection Down Alarm	100
Security Breach Statistics	101
Viewing List of Denied ACL Entries	101
Viewing ACL List Entries	101
Viewing ACL List Entries by IP Address.	102
Viewing ACL Entry Space in the CAM.	103
Session Agent and Session Agent Group Faults	103
SIP Agent Statistics.	103
Viewing SIP Session Agent Statistics	103
Resetting Session Agent Statistics	104
Viewing SIP Session Agent Activity	104
SIP Session Agent Group Statistics.	105
Viewing Session Agent Group Statistics.	105
Viewing List of SIP Session Agents in a Group	106
Viewing Statistics for a SIP Session Agent	106
Session Agent and Session Router Constraint Statistics.	107
Notes on Statistics.	107
Example 1: Statistics from Transaction Mode.	107
Example 1: Statistics from Stateless Mode	108
H.323 Session Agent Statistics.	108

Viewing H.323 Session Agent List	108
Viewing Session Agent Configuration Statistics	108
Viewing H.323 Session Agent Statistics	110
H.323 Session Agent Group Statistics	110
Viewing List of H.323 Session Agent Groups	110
Viewing H.323 Session Agent Group Configuration Statistics.....	111
Viewing H.323 Session Agent Group Statistics	111
Realm Faults	112
Signaling	112
Viewing SIP Realm Statistics	112
Media Statistics	112
Viewing MBCD Steering Port and Bandwidth Usage for Realms	112
Viewing MBCD Statistics for a Specific Realm.....	113
Viewing MBCD Task Errors	114
Viewing Realm Configurations	115
Viewing Realm Configurations for a Specific Realm	116
Viewing Monthly Minutes for a Specific Realm.....	116
Media Alarms	116
Viewing Deny ACL List	116
Network Faults	117
NAT Statistics	117
Viewing Information from the NAT Table	117
Viewing NAT information By Index	118
Viewing NAT Information By Address	118
Viewing NAT Information In Tabular	119
Viewing General NAT Table Information.....	120
Viewing NAT Flow Information	120
NAT Table Utilization Alarm	123
ARP Statistics	123
Viewing Address Mappings	123
Gateway Unreachable Alarm.....	124
View Network Interfaces Statistics	125
Physical Interface Faults	128
Viewing Network Interface Statistics	128
Viewing Media Interface Statistics	129
Viewing Network Interface Statistics	130
Viewing Physical Interface Statistics	130
Viewing Front Interface Physical Level Statistics.....	130
Physical Interface Alarms.....	131
Verifying an IP Address	134
Specifying a Source Address for ICMP Pings.....	134

DNS Statistics	135
Viewing DNS Statistics for Specific Cache Entries	135
Clearing ENUM and DNS Statistics	135
System Support Information for Troubleshooting	136
Included Data	137
Using the ACLI show support-info command.	137
SIP Interface Constraints Monitoring	139
All SIP Interfaces.	139
Single SIP Interface.	139
Displaying and Clearing Registration Cache Entries	140
Working with the SIP Registration Cache	140
Displaying the SIP Registration Cache	140
Clearing the SIP Registration Cache	142
Auditing the SIP Registration Cache.	142
Working with the H.323 Registration Cache	143
Displaying the H.323 Registration Cache	143
Clearing the H.323 Registration Cache	144
Auditing the H.323 Registration Cache	144
Working with the MGCP Registration Cache	144
Displaying the MGCP Registration Cache	144
Clearing the MGCP Registration Cache	145
Auditing the MGCP Registration Cache.	146
Session Management for SIP, H.323, and IWF	146
Displaying Sessions	146
Example 1: Displaying All SIP Sessions	147
Example 2: Displaying All H.323 Sessions	147
Example 3: Displaying SIP Sessions for a Session Agent	148
Example 3: Displaying H.323 Sessions for a Session Agent	148
Example 4: Displaying SIP Sessions for a Call ID	149
Clearing Sessions	150
Example 1: Clearing All SIP Sessions	150
Example 2: Clearing an H.323 Session by User	151
 3 Performance Management	 153
Overview	153
Viewing System Information	153
ACLI Credit Information	153
User Privilege Mode	153
System Uptime	153
Current Date and Time	154

Software Release Current Version	154
Viewing System Resource Information	154
System Memory	154
Listing Memory Subcommands.	154
Application Object Allocation and Use.	155
Memory Buffer	156
Control and Maintenance Interfaces.	156
Viewing Active Processes	160
Accessing Process Subcommands	162
Viewing Statistics for all Processes	164
Viewing Totals for all Processes.	179
Viewing Current Statistics	180
Checking Remaining Space	180
Viewing Redundancy Statistics	181
Accessing Redundancy Subcommands.	181
Configuration Checkpoint Example	181
About High Availability Transactions	182
Viewing Border Element Redundancy Protocol Information	182
Viewing Redundancy Health.	183
HA States.	183
Command Examples.	184
Active	184
Standby	184
Viewing Routing Statistics	186
Viewing Routing Table Entries	186
.	186
Viewing Routing Stats	186
Testing Routing Policies.	186
Test Policy Subcommands	187
Testing Address Translations.	187
Viewing QoS Based Routing Statistics	187
Local Route Table Statistics and Management	189
Setting the Log Level	189
Updating the Local Cache	189
Testing a Lookup in the Local Cache	189
Displaying a Route Entry in the Local Cache.	189
Displaying Statistics for a Local Route Tables	190
Resetting ENUM Statistic Counters	190
Viewing SIP Protocol Performance Statistics	190
Accessing SIP Statistics	190
Example	191

Viewing SIP Status Information	191
Viewing SIP Performance Statistics	193
All	193
Example	196
About the Information	196
Viewing Statistics for Other SIP Methods	197
SIP Monitoring by Transaction Type	197
SIP Server Transactions	197
SIP Client Transactions	198
Viewing SIP Media Event Errors	198
Viewing SIP Session Agent Statistics	201
Viewing SIP Session Agent Group Statistics	202
Viewing Session and Dialog States	202
Sessions	203
Dialogs	203
Viewing SIP Endpoint	203
Viewing SIP Per User CAC Statistics	204
IP-Based CAC Information	204
AoR-Based CAC Information	204
Number of Calls Dropped because of Per User CAC Limits	205
Viewing Statistics for SIP Per User Subscribe Dialog Limit	205
Viewing IMS-AKA Statistics	205
STUN Server Statistics and Protocol Tracing	206
STUN Server Statistics	206
STUN Protocol Tracing	207
H.323 Protocol Performance	207
Viewing the H.323 Performance Statistics	207
About Status Statistics	208
About Stack Statistics	208
Viewing Current Configuration	208
Viewing Stack Information	209
Viewing a List of Stacks	209
Viewing Stack Details	209
Viewing Specific Stacks	210
Viewing Session Agent Stats	211
Viewing a List of Session Agents	211
Viewing Session Agent Stats	211
Viewing Specific Session Agent Statistics	212
Viewing Session Agent Configurations	213
Viewing Session Agent by Hostname	214
Viewing Session Agent Group Stats	216
Listing Session Agent Groups	216
Viewing Session Agent Group Stats	216

Viewing Session Agent Details	216
Viewing Specific Session Group Statistics	217
Viewing all Configurations.....	217
Viewing Specific Session Agent Group Statistics.....	217
Viewing Stats for Each Configured Stack	218
Viewing Statistics for Specific Stacks.....	218
Viewing H.323 Registrations	220
Viewing MGCP Performance Statistics	220
Listing the MGCP Performance Subcommands	220
Viewing MGCP Status Statistics	221
About State Statistics	221
About MGCP Transactions	222
All Available Information.....	222
Viewing MGCP Error Statistics	224
MGCP Message Monitoring	225
Other MGCP Stats	225
Viewing Accounting Data and Statistics	226
QoS Reporting	226
Viewing Network Management Control Statistics	227
Displaying Network Management Control Statistics	227
Resetting Network Management Control Statistics	227
Monitoring Your Net-Net System in Real-Time	228
Displaying the Statistics	228
Changing the Refresh Rate	228
Quitting the Display	228
Viewing Real-Time Media Statistics	228
Viewing Real-Time SIP Session Statistics.....	230
Viewing TLS Information	231
Clearing the Entire TLS Session Cache	231
Viewing TLS Session Cache State and Statistics	231
Viewing Certificates in PEM Form	231
Viewing Net-Net SSM Status	232
Viewing IPSec Statistics	232
Security Association Entries.....	232
Security Policy Entries	233
IPSec Statistics	233
Viewing Statistics for a Specific SA.....	233
Viewing Statistic for Traffic to/from the GMAC Interface and the Security Processor. .	233
Viewing IPSec Interface Status	233
Viewing SSH Security Information	234

Viewing SSH Statistics	234
Viewing a Brief SSH Statistics Output	234
Viewing a Detailed SSH Statistics Output	234
4 System Management.....	237
User Privilege Levels and Passwords: Without Data Storage Security.....	237
User and Superuser Modes	237
Setting Passwords.....	237
SSH Remote Connections	238
SSH RADIUS Authentication VSA Support.....	239
SSHv2 Public Key Authentication.....	239
ACLI Instructions and Examples: Viewing SSH Public Key Data	239
Importing a Public Key Record	240
Expanded Privileges	241
User Sessions	241
Concurrent Sessions.....	242
Data Storage Security	242
Considerations When Enabling Data Storage Security.....	242
About Net-Net SBC Password Features.....	242
Password Secure Mode	243
Protected Configuration Password for TLS, IPSec, and HDR.....	243
Configuration Migration.....	243
Password Requirements.....	243
Note on Backwards Compatibility.....	244
Password Reset and Recovery	244
Password Policy	244
Upgrade to ACP	244
SSH Password Considerations	245
ACLI Instructions and Examples.....	245
Enabling Password-Secure Mode for the First Time	245
Setting a Protected Configuration Password: Matching Configurations.....	246
Setting a Protected Configuration Password: Mismatched Configurations	247
Setting a Protected Configuration Password: Committing Changes	248
Changing Protected Configuration Password on a Standby System in an HA Node ..	249
Confirming Synchronous Protected Configuration Password and Configuration	250
Configuration Migration.....	250
Setting the Password Policy.....	251
System Time	251
Setting Time	251
Setting Timezone	252
Displaying the System Timezone	252

NTP Synchronization	252
Setting NTP Synchronization	253
Monitoring NTP from the ACLI	253
System Task Management	254
Viewing Tasks	254
Setting Task Log Levels	255
Stopping a Task.	256
Notifying Tasks	257
Tracing Sockets	257
Notify Subcommands.	257
Viewing Power Supply and RAMdrive Status	258
Rebooting the Net-Net SBC	259
reboot activate	259
reboot force	259
reboot force activate	259
Reboot Safeguards	260
Reboot Status File	260
Warning on Reboot	260
System Watchdog Timer.	260
Watchdog Timer Configuration.	261
Availability.	261
ACLI Example	261
Configuring the Front Panel Interface	261
admin-state	262
auto-negotiation	262
duplex-mode	262
speed	262
ARP Information.	262
show arp	263
arp-add.	263
arp-delete.	263
arp-check	263
NAT Information	264
show nat info.	264
show nat by-addr	264
show nat by-index.	266
show nat in-tabular.	266
SNMP Community and Trap Receiver Management.	268
SNMP Community Table.	268
show snmp-community-table	268

reset snmp-community-table	268
Trap Receiver.....	268
show trap-receiver	268
reset trap-receiver	269
Login Banner.....	269
ACLI Audit Trail.....	269
5 Inventory Management	271
Accessing Inventory Management Data.....	271
Hardware Inventory	271
Components	271
show prom-info mainboard.....	271
show prom-info CPU	272
show prom-info PHY0	272
show prom-info PHY1	272
Software Inventory.....	273
System image	273
Image Filename: Net-Net 4250 and Net-Net 4500	273
Location	273
show version image	273
bootparam	274
Version.....	274
show version	274
Configuration Information.....	275
Overview	275
Configuration Show Subcommands.....	275
Running configuration Commands.....	276
show running-config	277
show running-configuration media-manager	277
display-running-cfg-version	277
Configuration Commands	277
show configuration	278
show configuration media-manager	278
display-current-cfg-version	278
Realm Specific.....	278
realm-specifics <realm ID>	279
Running Configuration Example.....	280
Software License Inventory	296
About Licenses	296
Unlicensed Signaling Protocols.....	297

Viewing License Information.	298
show features.	298
license show	298
show sessions	299
6 Net-Net 4250 Upgrading.	301
Introduction.	301
Preparing for Upgrade	301
Transferring Files	301
Uploading SBC Software Image	301
Downloading Running Configuration	302
System Configuration Files Release Compatibility	302
Upgrade Paths and Release 2.2	302
ACLI Upgrade Preparation Command	303
ACLI Instructions and Examples.	303
Loading a New Image	303
When There is Insufficient Space for a New Image.	304
S-C6.1.0 to S-C6.2.0 Upgrade	305
Pre-Upgrade Checklist	305
Stand-alone Upgrade	305
Upgrade Procedure	305
HA Upgrade	306
Upgrade Overview	306
Upgrade Process	307
C6.0 to S-C6.1.0 Upgrade	309
Pre-Upgrade Checklist	309
Stand-alone Upgrade	309
Upgrade Procedure	309
HA Upgrade	310
Upgrade Overview	310
Upgrade Process	311
C5.1 to C6.0 Upgrade	313
Pre-Upgrade Checklist	313
Stand-alone Upgrade	313
Upgrade Procedure	313
HA Upgrade	314
Upgrade Overview	314
Upgrade Process	315
C5.0 to C5.1 Upgrade	317
Pre-Upgrade Checklist	317

Stand-alone Upgrade	317
Upgrade Procedure	317
HA Upgrade	318
Upgrade Overview	318
Upgrade Process	319
4.1 to C5.0 Upgrade	320
Pre-Upgrade Checklist	321
Standalone Upgrade	321
Upgrade Procedure	321
HA Upgrade	322
Upgrade Overview	322
Upgrade Process	322
4.0 to 4.1 Upgrade	324
Pre-Upgrade Checklist	325
Standalone Upgrade	325
Upgrade Procedure	325
HA Upgrade	326
Upgrade Overview	326
Upgrade Process	326
2.x to 4.0 Upgrade	328
Pre-Upgrade Checklist	329
Standalone Upgrade	329
Upgrade Procedure	329
HA Upgrade	330
Upgrade Overview	330
Upgrade Process	330
2.0/2.1 to 2.2 Upgrade	332
Pre-Upgrade Checklist	333
Standalone Upgrade	333
Upgrade Procedure	333
HA Upgrade	334
Upgrade Overview	334
Upgrade Process	334
2.0 to 2.1 Upgrade	336
Pre-Upgrade Checklist	337
Standalone Upgrade	337
Upgrade Procedure	337
HA Upgrade	338
Upgrade Overview	338
Upgrade Process	338
HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0.	341

HA Backout Procedure 1	341
HA Backout Procedure 2	342
HA Backout Procedures: Release S-C6.1.0 to Release C6.0	344
HA Backout Procedure 1	344
HA Backout Procedure 2	345
HA Backout Procedures: Release C5.1 to Release C5.0.....	346
HA Backout Procedure 1	346
HA Backout Procedure 2	347
HA Backout Procedures: Release C5.0 to Release 4.1	349
HA Backout Procedure 1	349
HA Backout Procedure 2	350
HA Backout Procedures: Release 4.1 to Release 4.0	351
HA Backout Procedure 1	351
HA Backout Procedure 2	352
HA Backout Procedures: Release 4.0 to Release 2.0/2.1	354
HA Backout Procedure 1	354
HA Backout Procedure 2	355
HA Backout Procedures: Release 2.2 to Release 2.0/2.1	356
HA Backout Procedure 1	356
HA Backout Procedure 2	357
HA Backout Procedures: Release 2.1 to Release 2.0	359
HA Backout Procedure 1	359
HA Backout Procedure 2	361
 7 Net-Net 4500 Upgrading.....	 363
Introduction.....	363
Notes on Boot Parameters	363
Net-Net 3800	363
Preparing for Upgrade	363
Password Secure Mode	363
Upgrading S-CX6.2.0 Software Images	363
Pre-Upgrade Checklist	363
Stand-alone Upgrade	364
Upgrade Procedure.....	364
HA Upgrade	365
Upgrade Process	365
HA Backout Procedure.....	367
Upgrading S-CX6.1.0 Software Images	368
Pre-Upgrade Checklist	368

Stand-alone Upgrade	369
Upgrade Procedure	369
HA Upgrade	369
Upgrade Process	370
HA Backout Procedure	372
Upgrading CX6.0.0 Software Images	373
Pre-Upgrade Checklist	373
Stand-alone Upgrade	373
Upgrade Procedure	374
HA Upgrade	374
Upgrade Process	374
HA Backout Procedure	377
Moving a Configuration	378
Backup Commands	378
Creating a Backup on Your Net-Net 4250	379
Listing Backups	379
Copying the Backup to Your Net-Net 4500	379
Restoring Backups	380
8 Working with Configurations	381
Configuration Overview	381
Configuration Process	381
Verifying & Regenerating Configurations	382
Verifying Address Duplication	383
Network-Interface	383
Steering-Pool	384
SIP-Interface	384
SIP-NAT	384
MGCP-Config	384
H323-Stack	385
Local-Policy>Local-Policy-Attributes	385
Session-Agent	385
Static-Flow	386
Capture-Receiver	386
Realm-Config	386
Verify-Config Errors and Warnings	386
Access-Control	386
Account-Config	387
Authentication	387
Call-Recording-Server	387
Capture-Receiver	388

Certificate-Record	388
Class-Policy	388
DNS-Config.	388
ENUM-Config.	389
Ext-Policy-Server	389
H323-Stack	389
Host-Route	389
IWF-Config	389
Local-Policy	390
Local-Routing-Config.	390
MGCP-Config	390
Network-Interface.	390
Phy-Interface	391
Public-Key	391
Realm-Config	391
Realm-Group.	392
Redundancy.	393
Security-Association	393
Security-Policy.	394
Session-Agent	395
Session-Group	395
Session-Translation	395
SIP-Config.	396
SIP-Interface	396
SIP-Manipulation	397
SIP-NAT	397
Static-Flow.	398
Steering-Pool.	398
Surrogate-Agent	398
System-Config.	398
TLS-Profile.	399
Viewing Configurations	400
Checking Configuration Versions	400
Deleting Configurations.	400
Configuration Checkpointing	401
Realm-Specific Delete Command.	401
Deleted Configurations	402
Deleted Parameter Values	403
ACLI Instructions and Examples.	403
System Prompt Indicator	404

9	Managing Backups and Archives	405
	Introduction	405
	Backup Commands	405
	Creating Backups	405
	Listing Backups	406
	Restoring Backups	406
	Deleting Backups	406
	Viewing Backup Configurations	406
	Archive Commands	407
	Creating Archives	407
	File Locations	407
	Log File Archives	407
	Listing Archives	407
	Deleting Archives	408
	Renaming Archives	408
	Viewing Free Space	408
	Appendix A	411
	Access-Control	411
	Account-Config	411
	Authentication	412
	Call-Recording-Server	412
	Capture-Receiver	412
	Certificate-Record	412
	Class-Policy	413
	DNS-Config	413
	ENUM-Config	413
	Ext-Policy-Server	413
	H323-Stack	414
	Host-Route	414
	IWF-Config	414
	Local-Policy	414
	Local-Routing-Config	415
	MGCP-Config	415
	Network-Interface	415
	Phy-Interface	415
	Public-Key	416
	Realm-Config	416
	Realm-Group	417
	Redundancy	417
	Security-Association	418

Security-Policy	419
Session-Agent	419
Session-Group	420
Session-Translation	420
SIP-Config	420
SIP-Interface	421
SIP-Manipulation	421
SIP-NAT	422
Static-Flow	422
Steering-Pool	422
Surrogate-Agent	423
System-Config	423
TLS-Profile	424

Introduction

This chapter describes the logs available with the Net-Net SBC and explains how to access and view them. It also explains the relationship between logs and system events.

About Logs

Logs are a critical component of system management and security. You can use the information in logs to assist real-time debugging and management, and to track potential security breaches or other nonstandard activities on the system. The Net-Net SBC supports the following three types of logs:

- `acmelog` (syslog): contains both generic messages (not task oriented) as well as system log messages
- process logs: contain process flow from tasks
- transaction logs: contain raw messages about protocol transactions sent and received by the Net-Net SBC.

The Net-Net SBC supports SYSLOG, a protocol that lets the Net-Net SBC log significant system information to a remote server.

Logging Events

The Net-Net SBC can log events that occur on different system components, such as those associated with a protocol transaction. If logging is enabled on the Net-Net system, monitored events are evaluated against the logging level set for the component that sent the event. Events that meet the logging level are written to a log file.

SNMP traps are sent when a Net-Net system generates a system log (`acmelog`) message and the following conditions are present:

- SNMP is enabled.
Set the system configuration's SNMP functionality to enabled. Using the ACLI, set the `snmp-enabled` field for `system-config` to `enabled`.
- Sending system log (`acmelog`) notifications to an NMS using SNMP is enabled.
Set the system configuration's log functionality to enabled. Using the ACLI, set the `enable-snmp-syslog-notify` field for `system-config` to `enabled`.
- Severity level that identifies at which severity level syslog notifications are sent is configured. For example:
Set the system configuration's log functionality to one of the possible severity levels. Using the ACLI, set the `snmp-syslog-level` field for `system-config` to `enabled`.

See the *Net-Net Configuration Guide* for details about configuring the Net-Net SBC and the *Net-Net ACLI Reference Guide* for details about using the ACLI.

Event Categories

This section describes the events and the different event categories the Net-Net SBC can generate.

About Events

Events are the circumstances that generate one or more of the following:

- alarm
- entry in a log file
- SNMP trap

The following table lists the three categories used to define these events.

Event Category	Description
Informational	Represents non-critical conditions. For example, a configuration element has changed.
Warning	Indicates pending failures or unexpected events. For example, you typed the wrong password at the console three consecutive times.
Error	Indicates that a serious condition has occurred. For example, an internal temperature reading exceeds the recommendation.

These broad categories generally consist of the facility that generated them, along with an indication of the severity of the message. This information helps filter the more important and time-sensitive notifications from the informative messages.

Types of Events

The Net-Net SBC can generate the following types of events.

- process log events
- system log events
- protocol trace elements

Process Log Events

Events are logged to the process log flow from tasks and are specific to a single process running on the Net-Net SBC. By default they are placed into individual files associated with each process with the following name format:

log. <taskname>

Note: Process logs serve as a debugging tool. When set to debug level, the quantity of events generated can become overwhelming for the Net-Net SBC. It should only be used by Acme Packet personnel, or with their assistance. It is not recommended for use on production systems.

When you configure the system, you set the default system-wide process log level and each task logs according to this setting. You can override this log level for specific tasks when configuring other elements. For example, when you configure the media manager you can set the ALGD and MBCD log levels to different severity levels.

System Log Events

System log events are a subset of the collection of all process log events. Every software process writes messages to a file called *acmelog*, if the severity of the event meets or exceeds the configured log level threshold. There is one system log for the whole Net-Net system (filename: *acmelog*).

System log events are also referred to as *acmelog* events and are analogous to a traditional *syslog* event. The *acmelog* file is typically viewed as an aggregation of notable alarms and errors from all software processes.

The Net-Net SBC supports logging using SYSLOG, which is an industry-standard protocol that lets a device send event notification messages across IP networks to event message collectors - also known as syslog servers. Messages are usually sent using UDP port 514.

The Net-Net SBC can send information to a remote SYSLOG server. You configure the server and globally set the severity level at which the Net-Net SBC logs events when you configure the system. See the *Net-Net Configuration Guide* for details.

Protocol Trace Events

Protocol trace events are the events associated with a protocol transaction. They are enabled on a per-process basis using the *notify* command, resulting in transactional events being placed into transaction logs, such as *sipmsg.log*.

These events are helpful for troubleshooting sessions, but they are also the highest volume events the Net-Net SBC produces and can only be enabled for short times.

Event Granularity

You can set the reporting level for events placed into the logs by using the following methods:

- Setting the system-wide severity level (at or above which events are logged) by configuring the system's process log level. This setting is persistent across boots.

You set the system-wide severity level by configuring the log severity level threshold when performing the system configuration. See the *Net-Net Configuration Guide* for more information.
- Configuring individual parameters for different elements that control specific process logs. For example, you can configure the *mbcd* log level for the media manager. These settings are persistent across boots.

For example, to configure the process log level for monitoring all H.323 activity on the Net-Net SBC, you configure the log level to INFO when configuring H.323 signaling. See the *Net-Net Configuration Guide* for more information.
- Using ACLI log-level command to dynamically specify the log level for a specific task (or all tasks using the keyword *all*). You can specify finer granularity by including specific subtypes within the process. These settings are not persistent across boots. See the *Net-Net ACLI Reference Guide* for more information.
- Using the ACLI or Acme Control Protocol (ACP) *notify* command. For example, *notify mbcd debug*. Such settings are not persistent across boots. See the *Net-Net ACLI Reference Guide* for more information about using the ACLI. See the *Net-Net ACP/XML Reference Guide* for more information about ACP.

Event Severity

There are eight severity levels ranging from lowest severity, Debug, to the highest, Emergency.

syslog Numerical Code	syslog Severity	Acme Packet Log Enumeration
0	Emergency (system is unusable)	EMERGENCY (0)
1	Alert (action must be taken immediately)	CRITICAL (1)
2	Critical (critical conditions)	MAJOR (2)
3	Error (error conditions)	MINOR (3)
4	Warning (warning conditions)	WARNING (4)
5	Notice (normal but significant condition)	NOTICE (5)
6	Informational (informational messages)	INFO (6)
7	Debug (debug level messages)	TRACE (7) DEBUG (8) DETAIL (9)

SNMP Traps

The Net-Net SBC supports several standard SNMP traps (cold start, link up/down) and proprietary traps used to notify SNMP managers of specific events:

- apSysMgmtGroupTrap – used for different events. The trap must be parsed by a management tool to extract the specific event details.
- specific uniquely identified traps – used for specific Net-Net SBC events. These traps correspond exactly to the events that show up in acmelog.

The unique traps are only generated if the following ACLI parameter is enabled:

```
System-confi g->enabl e-snm p-moni tor-traps
```

- apSysLogGeneratedTrap – used as a catch-all for system log (syslog) events.

See the *Net-Net MIB Reference Guide* for more details about traps.

Alarms

The most serious events noted by the Net-Net SBC are categorized as alarms. They appear in the alarm table, which is displayed in the ACLI using the command display-alarms. The ACLI also supports clearing alarms displayed in that table. Alarms are not sent off-box explicitly, however, at least one of the following mechanisms is usually triggered when an alarm occurs:

- A dry contact port on the back of the chassis that may be used to control a remote alarm panel.
- An SNMP trap may be generated
- A syslog event may be generated

See the *Net-Net MIB Reference Guide* for details about alarms.

Process Log Events

Process log events can be sent to a log server by configuring the system to include the destination server's IP address and port number. For example, using the ACLI you configure the following system parameters:

- **process-log-server**
- **process-log-port**

The process log port can be any port from 1025 to 65535. It is most commonly configured as port 2500.

The Net-Net SBC stops logging events to RAM memory and instead sends them to the configured remote server over UDP. Because of the added overhead of sending log messages using UDP datagrams versus writing to the RAM drive, message content decreases – even at the same configured log levels.

System Log Events

System log events can be sent to one or more syslog servers using the traditional UNIX syslog mechanism as described in RFC 3164. Users can configure one or more syslog servers to which the Net-Net SBC will send generated syslog events by setting the following syslog parameters in the system configuration:

- **address**
- **port**
- **facility**

If the port is left empty, the default value is UDP port 514 (the well-known syslog port).

Traps

Traps are defined to be sent to a SNMP Manager using the following configuration parameters:

```
System-config->trap-receiver->ip-address
System-config->trap-receiver->filter-level
System-config->trap-receiver->community-name
```

Alarms

Alarms can be sent off the box using the dry contact port in the rear of the chassis.

Working with Logs

This section explains how to work with logs.

Writing to Logs

You need to configure the Net-Net SBC to indicate you want messages written to logs. See the *Net-Net Configuration Guide* and the *ACLI Reference Guide* for details.

The log files are written until they become 1 MB in size. The file is then closed and renamed with a .1 appended to the original file name. For example, sipmsg.log becomes sipmsg.log.1. New logs continued to be written to the original file, sipmsg.log, until once again they reach the 1 MB limit. Again the file is closed and renamed with a .1 appended to the original file name. The existing file with .1 appended is renamed to .2, for example sipmsg.log.2. This continues until you have 13 1 MB files associated with the log. When this limit is reached, the oldest file (the one with .12 appended to the name) is discarded.

Manually Rotating Logs

You can manually rotate (close) the log file by using the following command:

```
noti fy * rotate-l ogs
```

The * can be any of the following Net-Net SBC tasks:

- all
- sipd
- sysmand
- berpd
- lemd
- mbcd
- h323d
- algd
- radd

You can manually rotate the log files when you are trying to isolate a specific problem. Working with Acme Packet Technical Support, you could close all current log files (or just for a specific task) and then run a test of your problem. You can then easily identify the log files to review.

Working with Logs Example

For example, to troubleshoot issues you suspect are media-related using the ACLI, you can look at the logs for the middlebox control daemon (MBCD). To do this:

1. Instruct the Net-Net SBC to write all media management transactions to mbcd.log by entering the following command:

```
noti fy mbcd l og
```
2. Make some test calls.
3. Set message writing to the log off by entering the following command:

```
noti fy mbcd nol og
```
4. FTP the log off the Net-Net SBC to view it.

Note: Acme Packet recommends only setting the log level to DEBUG on non-production systems.

Displaying List of Log Files

You can display the list of log files by using the **display-logfiles** ACLI command. Every task writes to its own process log (log.taskname) and protocol trace logs (transaction logs) are enabled or disabled creating a task.log file. The log files are stored in the /ramdrv/logs directory on the Net-Net SBC.

For example:

```
ACMEPACKET# display-logfiles
```

Listing Directory /ramdrv/logs:

```
drwxrwxrwx 1 0 0 512 Jul 4 18:02 ./
drwxrwxrwx 1 0 0 512 Jul 6 09:50 ../
-rwxrwxrwx 1 0 0 820707 Jul 6 11:55 acmelog
-rwxrwxrwx 1 0 0 3447 Jul 2 17:40 log.sysmand
-rwxrwxrwx 1 0 0 3724 Jul 2 15:59 log.bootstrap
-rwxrwxrwx 1 0 0 132 Jul 2 17:40 log.brokerd
-rwxrwxrwx 1 0 0 740 Jul 2 17:40 log.npsoft
-rwxrwxrwx 1 0 0 369 Jul 2 15:59 log.berpd
-rwxrwxrwx 1 0 0 26660 Jul 6 11:46 log.clWorker
-rwxrwxrwx 1 0 0 3316 Jul 2 17:40 log.lcmd
-rwxrwxrwx 1 0 0 852 Jul 2 17:40 log.atcpd
-rwxrwxrwx 1 0 0 733 Jul 2 17:40 log.atcpApp
-rwxrwxrwx 1 0 0 2877 Jul 2 17:40 log.mbcd
-rwxrwxrwx 1 0 0 757 Jul 2 17:40 log.lid
-rwxrwxrwx 1 0 0 1151 Jul 2 17:40 log.algd
-rwxrwxrwx 1 0 0 741 Jul 2 17:40 log.radd
-rwxrwxrwx 1 0 0 728 Jul 2 17:40 log.pusher
-rwxrwxrwx 1 0 0 1448 Jul 2 17:40 log.ebmd
-rwxrwxrwx 1 0 0 671322 Jul 6 11:55 log.sipd
-rwxrwxrwx 1 0 0 681011 Jul 6 11:55 log.h323d
-rwxrwxrwx 1 0 0 1169 Jul 2 15:59 log.h248d
-rwxrwxrwx 1 0 0 18294 Jul 2 17:40 log.snmpd
-rwxrwxrwx 1 0 0 1078 Jul 2 17:40 snmpd.log
-rwxrwxrwx 1 0 0 190 Jul 2 15:59 log.acliSSH0
-rwxrwxrwx 1 0 0 191 Jul 2 15:59 log.acliSSH1
-rwxrwxrwx 1 0 0 192 Jul 2 15:59 log.acliSSH2
-rwxrwxrwx 1 0 0 192 Jul 2 15:59 log.acliSSH3
-rwxrwxrwx 1 0 0 192 Jul 2 15:59 log.acliSSH4
-rwxrwxrwx 1 0 0 3043 Jul 6 11:38 log.acliConsole
-rwxrwxrwx 1 0 0 2655 Jul 2 21:07 log.acliTelnet0
-rwxrwxrwx 1 0 0 195 Jul 2 15:59 log.acliTelnet1
-rwxrwxrwx 1 0 0 195 Jul 2 15:59 log.acliTelnet2
-rwxrwxrwx 1 0 0 195 Jul 2 15:59 log.acliTelnet3
-rwxrwxrwx 1 0 0 195 Jul 2 15:59 log.acliTelnet4
-rwxrwxrwx 1 0 0 1000005 Jul 4 18:01 acmelog.1
```

Viewing Logs

You can send the log off the Net-Net SBC through wancom0 or retrieve it using FTP in order to view it.

Note: The **view-log** command currently listed in the ACLI is not supported.

Viewing a Specific Logfile

You can view a specific logfile saved on the Net-Net SBC using the **show logfile** <filename> command. For example:

```
ACMEPACKET# show logfile acmelog
Jun 19 15:25:28.159 sysmand@ACMEPACKET: PROC[6] sysmand Started
[TaskId=0xf6c2d00 Process=0xf6ed390]
Jun 19 15:25:28.170 sysmand@ACMEPACKET: WARNING TLSEngine: Failed to
initialize UBSEC hardware accelerator
Jun 19 15:25:28.177 sysmand@ACMEPACKET: CONFIG[31] Populate Config
cver=16; rver=16
Jun 19 15:25:28.179 sysmand@ACMEPACKET: CONFIG[31] Finding
configurations for cver=16; rver=16
Jun 19 15:25:28.179 sysmand@ACMEPACKET: CONFIG[31] Load Configuration
Cache
Jun 19 15:25:28.180 sysmand@ACMEPACKET: CONFIG[31] Load DamCache
/ramdrv/running version=16
Jun 19 15:25:28.199 sysmand@ACMEPACKET: CONFIG[31] Load DamCache
/ramdrv/data version=16
Jun 19 15:25:28.215 sysmand@ACMEPACKET: CONFIG[31]
SRIInstance[ACMEPACKET]::load_config: ver=0 runver=16
Jun 19 15:25:28.216 sysmand@ACMEPACKET: CONFIG[31] Default to Session
Director (no config)
Jun 19 15:25:28.219 sysmand@ACMEPACKET: PROC[6] Start up tasks....
Jun 19 15:25:28.220 sysmand@ACMEPACKET: PROC[6] System Manager Running
Jun 19 15:25:28.223 bootstrap@ACMEPACKET: PROC[6] bootstrap Started
[TaskId=0xf7dbc50 Process=0xf809fd0]
Jun 19 15:25:28.223 bootstrap@ACMEPACKET: GENERAL[0] Bringing up box...
Jun 19 15:25:28.224 bootstrap@ACMEPACKET: GENERAL[0] Running Acme Net-
Net 4250 C6.0.0 Build A7
Jun 19 15:25:28.224 bootstrap@ACMEPACKET: GENERAL[0] Build
Date=05/27/08
Jun 19 15:25:28.224 bootstrap@ACMEPACKET: GENERAL[0] Build
View=/home/acme/cc/KYLE_integration
Jun 19 15:25:28.224 bootstrap@ACMEPACKET: GENERAL[0] User=acme@slider
Jun 19 15:25:28.228 brokerd@ACMEPACKET: PROC[6] brokerd Started
[TaskId=0xf7e2ab0 Process=0xf82b030]
Jun 19 15:25:58.431 bootstrap@ACMEPACKET: MINOR isWancom: No matching
i/f for 10.0.0.0
Jun 19 15:25:58.436 xntpd@ACMEPACKET: PROC[6] xntpd Started
[TaskId=0x1482e9f0 Process=0x14a85030]
Jun 19 15:25:58.445 berpd@ACMEPACKET: PROC[6] berpd Started
[TaskId=0x14aa02d0 Process=0x14ab8030]
Jun 19 15:25:58.445 berpd@ACMEPACKET: MINOR berpd: redundancy is
disabled
Jun 19 15:25:58.445 berpd@ACMEPACKET: PROC[6] berpd Exiting
[TaskId=0x14aa02d0 Process=0x14ab8030]
Jun 19 15:25:58.453 cliWorker@ACMEPACKET: PROC[6] cliWorker Started
[TaskId=0x14aa17d0 Process=0x14ab9030]
Jun 19 15:25:58.457 lemd@ACMEPACKET: PROC[6] lemd Started
[TaskId=0x14ad0ac0 Process=0x14aed020]
Jun 19 15:25:58.462 collect@ACMEPACKET: PROC[6] collect Started
[TaskId=0x14b13e70 Process=0x14b2c030]
Jun 19 15:25:58.466 atcpd@ACMEPACKET: PROC[6] atcpd Started
[TaskId=0x14b46fa0 Process=0x14b5f030]
Jun 19 15:25:58.503 atcpApp@ACMEPACKET: PROC[6] atcpApp Started
[TaskId=0x173c7110 Process=0x17483cc0]
Jun 19 15:25:58.510 mbcd@ACMEPACKET: PROC[6] mbcd Started
[TaskId=0x174f0fc0 Process=0x17509030]
Jun 19 15:25:58.836 lid@ACMEPACKET: PROC[6] lid Started
[TaskId=0x18010760 Process=0x180820e0]
Jun 19 15:25:58.842 algd@ACMEPACKET: PROC[6] algd Started
[TaskId=0x180848f0 Process=0x1882d030]
Jun 19 15:25:58.865 radd@ACMEPACKET: PROC[6] radd Started
[TaskId=0x188b0350 Process=0x189841f0]
```

```

Jun 19 15:25:58.876 pusher@ACMEPACKET: PROC[6] pusher Started
[TaskId=0x1899fd20 Process=0x189da000]
Jun 19 15:25:58.883 ebmd@ACMEPACKET: PROC[6] ebmd Started
[TaskId=0x18a46220 Process=0x18a5e030]
Jun 19 15:25:58.903 sipd@ACMEPACKET: PROC[6] sipd Started
[TaskId=0x18a8d3e0 Process=0x18afd080]
Jun 19 15:25:58.951 lrtid@ACMEPACKET: PROC[6] lrtid Started
[TaskId=0x18b2e520 Process=0x18be2b90]
Jun 19 15:25:58.959 h323d@ACMEPACKET: PROC[6] h323d Started
[TaskId=0x18c06ff0 Process=0x18c6f080]
Jun 19 15:25:58.973 h248d@ACMEPACKET: PROC[6] h248d Started
[TaskId=0x18cdf4d0 Process=0x18d5e9e0]
Jun 19 15:25:58.979 secured@ACMEPACKET: PROC[6] secured Started
[TaskId=0x18dc5cd0 Process=0x18ddd030]
Jun 19 15:25:59.011 snmpd@ACMEPACKET: PROC[6] snmpd Started
[TaskId=0x18e70900 Process=0x18f850e0]
Jun 19 15:25:59.105 brokerd@ACMEPACKET: MAJOR ALARM[00020014]
Task[0f7e2ab0] Slot 1 Port 0 DOWN
Jun 19 15:26:00.106 brokerd@ACMEPACKET: RAMDRV[47] <tStartup>
ramdrvCleanerInit: RamDrvParams:
Jun 19 15:26:00.106 brokerd@ACMEPACKET: RAMDRV[47] <tStartup>
ramdrv-log-min-free=30
Jun 19 15:26:00.106 brokerd@ACMEPACKET: RAMDRV[47] <tStartup>
ramdrv-log-max-usage=50
Jun 19 15:26:00.106 brokerd@ACMEPACKET: RAMDRV[47] <tStartup>
ramdrv-log-min-check=50

```

Dynamically Changing Log Level

You can dynamically change the log level by using the ACLI's **log-level** command, in the Superuser mode. The **log-level** command sets the log level for a specific task. The following table lists the three subcommands within the **log-level** command.

log-level subcommands	Description
task_name	Displays the log level according to the task/process name. (You do not have to enter @<system_name>.) To view all tasks, enter all. To list available task/process names, enter the show processes command.
log_level	Identifies the log level, either by name or by number.
log_type_list	Lets you list log types by number or by name in parentheses ().

To change the log level:

1. Access the ACLI in Superuser mode.
2. Type **log-level** followed by a <Space> and one of the log-level subcommands. You can change the log level for the following:
 - entire Net-Net system


```
log-level system <log level>
```

 For example:


```
log-level system DEBUG
```
 - log level at which a specific task/process sends to the acmelog file


```
log-level <task name> <log level>
```

 For example:


```
log-level sipd debug
```
3. Press <Enter>.

Requesting Log Level Data

You are able to view the current log level of processes/tasks that are running on the Net-Net SBC. You can do this through both the ACLI and ACP:

- ACLI—The **loglevel** subcommand has been added to the ACLI **show** command
- ACP—A new ACP method called GET_LOG_LEVEL has been added

ACLI show loglevel Command

The ACLI **show loglevel** command allows you to request log level data from the ACLI console. It takes one mandatory and two optional parameters. The mandatory parameter specifies the name of the Net-Net SBC task for which you are requesting information; one of the optional parameters specifies the type of log level for which you want information and the other allows you to select whether you want to view a verbose display of the task.

You can enter **all** as the value for either of these parameters to view information for all system tasks or all log levels. If you do not enter a parameter, the system returns an error message and provides a list of valid parameters. You can also wildcard these parameters by entering an asterisk (*), but entering partial wildcards does not work.

To view log level information for a single system task:

1. Type **show loglevel**, a <Space>, and then the name of the system task for which you want to see log level information. Then press <Enter>.

```
ACMEPACKET# show loglevel sipd
Log Levels for process sipd:
loglevel=DEBUG
```

To view log level information for a single system task with a specific log level:

1. Type **show loglevel**, a <Space>, the name of the system task for which you want to see log level information, and the name of the log. Then press <Enter>.

```
ACMEPACKET# show loglevel sipd GENERAL
Log Levels for process sipd:
GENERAL=NOTICE

ACMEPACKET# show loglevel sipd MINOR
Log Levels for process sipd:
MINOR=NOTICE

ACMEPACKET# show loglevel sipd DNS
Log Levels for process sipd:
DNS=NOTICE
```

To view verbose log level information for a single system task:

1. Type **show loglevel**, a <Space>, the name of the system task for which you want to see log level information, and **verbose**. Then press <Enter>.

```
ACMEPACKET# show loglevel sipd verbose
Log Levels for process sipd:
GENERAL=DEBUG
EMERGENCY=DEBUG
CRITICAL=DEBUG
MAJOR=DEBUG
MINOR=DEBUG
WARNING=DEBUG
PROC=DEBUG
IPC=DEBUG
SERVICE=DEBUG
EVENT=DEBUG
MESSAGE=DEBUG
TEST=DEBUG
```

```

TRIP=DEBUG
SIP=DEBUG
MBCP=DEBUG
FLOW=DEBUG
MEDIA=DEBUG
SESSION=DEBUG
TRANS=DEBUG
TIMER=DEBUG
ALG=DEBUG
MGCP=DEBUG
NPSOFT=DEBUG
ARP=DEBUG
SNMP=DEBUG
ANDD=DEBUG
XNTP=DEBUG
REDUNDANCY=DEBUG
SI PNAT=DEBUG
H323=DEBUG
ERROR=DEBUG
CONFIG=DEBUG
DNS=DEBUG
H248=DEBUG
BAND=DEBUG
ALI=DEBUG
SS8GI=DEBUG
COPS=DEBUG
ATCP=DEBUG
ATCPAPP=DEBUG
CLF=DEBUG

```

ACP

The new ACP command `GET_LOG_LEVEL` provides log level information. This ACP request requires authentication, and it must be sent to port 3000.

Because ACP message length is limited, obtaining log level information for multiple system tasks is a multi-step procedure. For a known, single task, the procedure does not require as many steps.

To obtain log level information, an ACP message with the `GET_LOG_LEVEL` method is sent, and its message body contains information about the log levels being requested. This message body takes the following format: `process: type`.

An asterisk (*) can be used instead of the process name or log type to wildcard that value. If the process name is replaced with a *, then the first message response is a list of processes; this allows the querying management software to query the level of each process directly.

Wildcarding Task Name and Log Type

When you want to wildcard the process name and log type, the ACP requests looks like this:

```

GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain
CSeq: 3 GET_LOG_LEVEL
Authorization: Digest
    username="user",
    realm="intern1",
    nonce=6eccad8d8a4d7473d3725bc54bdf4a59,
    uri="sysmand@acmesystem",
    response=5a700cf8c15a0902cb8e75a02cc99f33,
    algorithm="md5-sess",

```

```

cnonce=4c11d5,
qop="auth",
nc=00000002
Content-Length: 3

```

```

*. *

```

The response would return the actual list of system tasks running on the Net-Net SBC. Depending on what tasks are running, it would look like this:

```

ACME/1.0 200 Everything is OK
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 253

```

```

<ProcessList>
  <process
name='sysmand' />
  <process
name='acl i SSH0' />
  <process
name='brokerd' />
  <process
name='tcliWorker' />
  <process
name='lcmd' />
  <process
name='atcpd' />
  <process
name='atcpApp' />
  <process
name='mbcd' />
  <process
name='l i d' />
  <process
name='al gd' />
  <process
name='radd' />
  <process
name='pusher' />
  <process
name='ebmd' />
  <process
name='si pd' />
  <process
name='h248d' />
  <process
name='snmpd' />
  <process
name='acl i SSH1' />
  <process
name='acl i SSH2' />

```

```

    <process
name=' acl i SSH3' />
    <process
name=' acl i SSH4' />
    <process
name=' acl i Consol e' />
    <process
name=' acl i Tel net0' />
    <process
name=' acl i Tel net1' />
    <process
name=' acl i Tel net2' />
    <process
name=' acl i Tel net3' />
    <process
name=' acl i Tel net4' />
</ProcessLi st>

```

Specific Task with Wildcard Log Level

The NMS can use the list from the above example to query each task using additional GET_LOG_LEVEL messages by specifying the name of the tasks and the levels.

The message would look like this:

```

GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain
CSeq: 3 GET_LOG_LEVEL
Authori zati on: Di gest
    username="user",
    real m="i ntern1",
    nonce=5dd735490c78a0146ca06d50f47c0a50,
    uri ="sysmand@acmesystem",
    response=129b882a3ee110db86565932819d017b,
    al gori thm="md5-sess",
    cnonce=859dcc,
    qop="auth",
    nc=00000002
Content-Length: 9

```

sysmand: *

To which the response would look like this:

```

ACME/1.0 200 Everything i s OK
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 544

```

<sysmand

```

GENERAL=DEBUG
EMERGENCY=DEBUG
CRITICAL=DEBUG
MAJOR=DEBUG
MINOR=DEBUG
WARNING=DEBUG
PROC=DEBUG
IPC=DEBUG
SERVICE=DEBUG
EVENT=DEBUG
MESSAGE=DEBUG
TEST=DEBUG
TRIP=DEBUG
SIP=DEBUG
MBCP=DEBUG
FLOW=DEBUG
MEDIA=DEBUG
SESSION=DEBUG
TRANS=DEBUG
TIMER=DEBUG
ALG=DEBUG
MGCP=DEBUG
NPSOFT=DEBUG
ARP=DEBUG
SNMP=DEBUG
ANDD=DEBUG
XNTP=DEBUG
REDUNDANCY=DEBUG
SIPNAT=DEBUG
H323=DEBUG
ERROR=DEBUG
CONFIG=DEBUG
DNS=DEBUG
H248=DEBUG
BAND=DEBUG
ALI=DEBUG
SS8GI=DEBUG
COPS=DEBUG
ATCP=DEBUG
ATCPAPP=DEBUG
CLF=DEBUG
/>

```

Specific Task and Log Level Type

To request a specific type of log level for a specific process, specify the process name and type specified in the body of the request:

```

GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain

```



```

CSeq: 3 GET_LOG_LEVEL
Authorization: Digest
    username="user",
    realm="intern1",
    nonce=d11774ac886bf2293217b1ed894444e3,
    uri="sysmand@acmesystem",
    response=b2eb7cae77e544685ce2883b90189e78,
    algorithm="md5-sess",
    cnonce=e0ad7,
    qop="auth",
    nc=00000002
Content-Length: 14

```

```
sysmand: CONFIG
```

The response to this request would look like this:

```

ACME/1.0 200 Everything is OK
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 26

<sysmand
    CONFIG=DEBUG
/>

```

Log Files

This section contains information about the log files and what each contains. The log files are stored in the /ramdrv/logs directory on the Net-Net SBC.

log.sysmand	This log contains information about the system manager task. This task is currently responsible for writing the system log (acmelog), dispatching commands to other application tasks, and starting the application-level code.
log.bootstrap	This log records information about the boot process as the Net-Net system becomes operational.
log.berpd	This log contains process logs for the berpd task or the redundancy health task. This file is primarily used for storing health messages and events and for determining whether a switchover is required.
log.brokerd	<p>This log contains information about platform-level tasks. For example, when the ARP manager wants to log information in a place other than the console, it sends a message to log-brokerd. This is also true of the various host tasks related to communicating with the network processors and/or the CAM.</p> <p>This log also contains messages from the IP fragmenter, which currently takes part in the SIP NAT process. brokerd forwards these messages through sysmand to the acmelog (the overall system log). Thus, log-brokerd contains a subset of the logs that acmelog contains.</p>
log.lemd	This log refers to the local element manager (or local database server) processes. Information in log.lemd pertains to remote retrievals of and writing of configuration data.
log.algd	This log contains information pertaining to MGCP processing. It occasionally contains information about the SIP NAT function.
log.mbcd	This log contains information pertaining to the application flow manager, such as the creation, updating, and removal of media NAT entries.
miboco.log	Tasks use MIBOCO protocol processing to communicate with the mbcd task. This log can be used to determine whether the mbcd has returned any error messages or other type of messages. It is possible that sipmsg.log and algd.log contain MIBOCO messages. However, the miboco.log is used infrequently because log.sipd and log.algd also report return codes from the mbcd.

log.radd	This log is used for the accounting daemon for RADIUS. It serves as a RADIUS client to the outside world. However, it also serves as a place to concentrate RADIUS records from various signaling protocol tasks running on the Net-Net SBC. Its logs reflect the latter function.
log.h323d	This log contains information pertaining to H.323 tasks.
log.sipd	This log contains information pertaining to the SIP processing task. The log contains information about how the Net-Net system's SIP proxy is processing messages.
sipmsg.log	This protocol trace log contains information about SIP messages that have been received, NAT'd, and sent by the SIP proxy. MIBOCO messages sent and received by the sipd process are also contained in this log.
log.acli	This log contains information pertaining to ACLI processing.
log.acliConsole	This log contains information about ACLI console functions.
log.acliTelnet0-4	This log contains information about ACLI Telnet sessions if your system access method is Telnet. You can have one log for each instance.
log.SSH0-4	This log contains information about SSH processes. You can have one log for each instance.
log.tCliWorker	This log contains information about tCliWorker processes.
syslog	<p>The term <i>syslog</i> refers to the protocol used for the network logging of system and network events. syslog facilitates the transmission of event notification messages across networks. Given that, the syslog protocol can be used to allow remote log access.</p> <p>The syslog message functionality lets you configure more than one syslog server, and set the facility marker value used in the messages sent to that syslog server independently. All syslog messages are sent to all configured syslog servers.</p> <p>Note: Acme Packet recommends configuring no more than eight syslog servers. As the number of configured syslog servers to which the Net-Net system sends logs increases, the Net-Net system performance might decrease.</p> <p>Configured syslog servers are keyed (identified uniquely) by IPv4 address and port combinations. The Net-Net SBC is able to send logs to multiple syslog servers on the same host.</p>

Process Logs

Each individual process running on the system has its own process log and a server where the Net-Net system sends those logs.

HA Switchover Log

The switchover log provides historical information about the role of an HA Net-Net SBC in an HA Net-Net SBC pair. This log lists the last 20 switchovers on an HA Net-Net SBC. The switchover log is not persistent across reboot(s). The switchover log message appears in the information provided by the `show health` command, and it also appears immediately on the terminal screen when a switchover takes place.

Log Message Graphical Display on Net-Net SBC

The switchover log message displayed on the HA Net-Net SBC that has moved from the Standby to the BecomingActive state (has assumed the active role) indicates the date and time that the switchover took place. It also indicates from which HA Net-Net SBC peer the active role was assumed and why. The HA Net-Net SBC peer displaying this message took the active role because a health score fell below a set threshold, because a timeout occurred, or because it was forced by a Net-Net system administrator via the ACLI.

Refer to the following example of a switchover log for an HA Net-Net SBC whose health score fell below a configured threshold.

```
ACMEPACKET# Mar 28 16:36:38.226: Standby to BecomingActive, active peer
ACMEPACKET2 has unacceptable health (50)
ACMEPACKET#
```

Refer to the following example of a switchover log for an HA Net-Net SBC that has timed out.

```
ACMEPACKET# Mar 29 13:42:12.124: Standby to BecomingActive, active peer
ACMEPACKET2 has timed out
ACMEPACKET#
```

The HA Net-Net SBC relinquishing the active role (becoming the standby system in the HA Net-Net SBC pair) also displays the date and time that the switchover took place. The HA Net-Net SBC also indicates that it has moved from the Active to the RelinquishingActive state.

Refer to the following example of a switchover log for an HA Net-Net SBC that is relinquishing its active role.

```
ACMEPACKET2# Mar 28 16:38:08.321: Active to RelinquishingActive
ACMEPACKET2#
```

Overview

This chapter explains how to access Net-Net SBC fault management statistics to locate faults, determine the cause, and make corrections. Fault management involves the following:

- Continuous monitoring of statistics
- Viewing alarms that warn of system problems

Accessing Fault Management Data

You can access fault management information using the following ACLI commands:

- `show` commands to view statistics
- `display-alarms` command to view alarms

You can access all show commands at the user level.

About Traps

This section defines the standard and proprietary traps supported by the Net-Net system. A trap is initiated by tasks (such as the `notify` task) to report that an event has happened on the Net-Net system. SNMP traps enable an SNMP agent to notify the NMS of significant events by way of an unsolicited SNMP message.

Acme Packet uses SNMPv2c. These notification definitions are used to send standard traps and Acme Packet's own enterprise traps.

Traps are sent according to the criteria established in the following:

- IETF RFC 1907 *Management Information Base for Version 2 of the Simple Network Management Protocol*
- IETF RFC 2233 *The Interfaces Group MIB using SMIv2*
- Or the appropriate enterprise MIB (for example the Acme Packet syslog MIB or the Acme Packet System Management MIB).

For additional information about the traps and MIBs supported by the Net-Net System, see the *Net-Net 4000 MIB Reference Guide*.

Standard Traps

The following table identifies the standard traps that the Net-Net system supports.

Trap Name	Description
linkUp	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.
linkDown	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state.
coldStart	The SNMPv2 agent is reinitializing itself and its configuration may have been altered. This trap is not associated with a Net-Net system alarm.
authenticationFailure	The SNMPv2 agent received a protocol message that was not properly authenticated. If the snmp-enabled and enable-snmp-auth-traps fields in the ACLI's system-config element are set to enabled a snmpEnableAuthenTraps object is generated. This trap is not associated with a Net-Net system alarm.

Enterprise Traps

The following table identifies the proprietary traps that Net-Net system supports.

Trap Name	Description
apSyslogMessageGenerated	Generated by a syslog event. For example, this trap is generated if a switchover alarm occurs (for High Availability (HA) Net-Net system peers only), or if an HA Net-Net system peer times out or goes out-of-service. You enable or disable the sending of syslog messages by using the ACLI.
apSysMgmtGroupTrap	Generated when a significant threshold for a Net-Net system resource use or health score is exceeded. For example, if Network Address Translation (NAT) table usage, Address Resolution Protocol (ARP) table usage, memory usage, or Central Processing Unit (CPU) usage reaches 90% or greater of its capacity, the apSysMgmtGroupTrap is generated. If the health score (for HA Net-Net peers only) falls below 60, the apSysMgmtGroupTrap is generated.
apLicenseApproachingCapacityNotification	Generated when the total number of active sessions on the system (across all protocols) is within 98 - 100% of the licensed capacity.
apLicenseNotApproachingCapacityNotification	Generated when the total number of active sessions on the system (across all protocols) has gone to or below 90% of its licensed capacity (but no sooner than 15 seconds after the original alarm was triggered).
apEnvMonI2CFailNotification	Generated when the Inter-IC bus (I2C) state changes from normal (1) to not functioning (7).
apEnvMonStatusChangeNotification	Generated when any entry of any environment monitor table changes in the state of a device being monitored. To receive this trap, you need to set the system config's enable-env-monitor-table value to enabled.
apSwCfgActivateNotification	Generated when an activate-config command is issued and the configuration has been changed at running time.

Trap Name	Description
apSysMgmtPowerTrap	Generated if a power supply is powered down, powered up, inserted/present or removed/not present.
apSysMgmtTempTrap	Generated if the temperature falls below the monitoring level.
apSysMgmtFanTrap	Generated if a fan unit speed falls below the monitoring level.
apSysMgmtTaskSuspendTrap	Generated if a critical task running on the system enters a suspended state.
apSysMgmtRedundancyTrap	Generated if a state change occurs on either the primary or secondary system in a redundant (HA) pair.
apSysMgmtMediaPortsTrap	Generated if port allocation fails at a percentage higher or equal to the system's default threshold rate. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
apSysMgmtMediaBandwidthTrap	Generated if bandwidth allocation fails at a percentage higher or equal to the system's default threshold rate. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
apSysMgmtMediaOutofMemory	Generated if the media process cannot allocate memory.
apSysMgmtMediaUnknownRealm	Generated if the media process cannot find an associated realm for the media flow.
apSysMgmtRadiusDownTrap	Generated if all or some configured RADIUS accounting servers have timed out from a RADIUS server.
apSysMgmtGatewayUnreachableTrap	Generated if the gateway specified becomes unreachable by the system.
apSysMgmtH323InitFailTrap	Generated if the H.323 stack has failed to initialize properly and has been terminated.
apSysMgmtHardwareErrorTrap	Provides a text string indicating the type of hardware error that has occurred. If the message text exceeds 255 bytes, the message is truncated to 255 bytes.
apSysMgmtDOSTrap	Generated when the IP address and the realm ID is denied of service.
apSysMgmtCfgSaveFailTrap	Generated if an error occurs while the system is trying to save the configuration to memory.
apSysMgmtSystemStateTrap	Generated when the Net-Net SBC is instructed to change the system-state or the transition from becoming offline to online occurs. This trap contains one field called APSysMgmtSystemState, and that field has three values: <ul style="list-style-type: none"> • online(0) • becoming-offline(1) • offline(2)
apSysMgmtAuthenticationFailedTrap	Generated when an attempt to login to the Net-Net SBC through Telnet or by using the console fails for any reason. The trap sent to all configured trap receivers includes the following information: <ul style="list-style-type: none"> • administration and access level (SSH, user, enable) • connection type (Telnet or console)

About Alarms

This section describes the alarms generated by the Net-Net system. Alarms play a significant role in determining overall health of the system. For additional information about the generated by the Net-Net System, see the *Acme Packet MIB Reference Guide*.

Overview

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. This alarm contains an alarm code, a severity level, a textual description of the event, the time the even occurred, and for high severity alarms, trap information.

The Net-Net system's alarm handler processes alarms by locating the Alarm ID for a particular alarm condition and then looking up that condition in an alarm table. The alarm table is a database that contains all of the actions required for following up on the alarm.

Types of Alarms

The Net-Net system can generate the following types of alarms:

- hardware alarms: generated when a problem with the Net-Net system chassis occurs.
- system alarms: accounts for system resource and redundancy issues. For example, CPU utilization is over threshold, memory utilization is high, the health score is under threshold, or a task is suspended. They also include low-level system calls (for example, there is not enough memory available).
- network alarms: can occur when the software is unable to communicate with the hardware.
- application alarms: account for application issues (for example, problems that involve protocols). These protocols include:
 - SIP
 - MGCP
 - RADIUS

Application alarms also include security breaches, session failures, and problems related to accounting.

About the Alarm Process

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. This alarm contains the following elements:

- **Alarm ID:** a unique 32-bit integer that contains a 16-bit category name or number and a 16-bit unique identifier for the error or failure within that category.
- **Severity:** how severe the condition or failure is to the system.
- **Character string:** a textual description of the event or condition.
- **Trap information:** is not contained within every alarm, but is only sent for events of greater severity. See the *Acme Packet MIB Reference Guide* for more information.

About Alarms and the Health Score

The Net-Net SBC health score is used to determine the active/standby roles of the Net-Net SBCs participating in an HA Net-Net pair architecture. The healthiest Net-Net SBC peer (peer with the highest health score) is the active Net-Net SBC peer. The Net-Net SBC peer with the lower health score is the standby Net-Net SBC peer.

The health score is based on a 100-point scoring system. When all system components are functioning properly, the health score of the system is 100.

Alarms play a significant role in determining the health score of an HA Net-Net SBC. Some alarm conditions have a corresponding health value, which is subtracted from the health score of the Net-Net system when that alarm occurs. When that alarm is cleared or removed, the corresponding health value is added back to the Net-Net system's health score.

If a key system task (for example, a process or daemon) fails, the health score of that HA Net-Net SBC might be decremented by 75 points, depending on how the system configuration was configured. These situations, however, do not have a corresponding system alarm.

When an alarm condition is cleared or removed, this action has a positive impact on the health score of a system.

ACLI Instructions and Examples

You display and clear alarms using the following ACLI commands:

- **display-alarms**
- **clear-alarm**

The clear-alarm command is only available in Superuser mode. You must have that level of privilege to clear alarms.

Displaying Alarms

To display Net-Net system alarms:

1. Enter the **display-alarms** command.

A list of the current alarms for the system will be displayed. For example:

```
ACMEPACKET# di spl ay-al arms
3 al arms to show
ID      Task      Severi ty      First Occurred      Last Occurred
262147  35615744      4      2005-02-10 13: 59: 05      2005-02-10 13: 59: 05
Count   Descri ption
1       ingress realm 'test_client_real m' not found

131075  36786224      3      2005-02-10 13: 59: 05      2005-02-10 13: 59: 05
Count   Descri ption
1       SI ot 0 Port 0 DOWN

131101  36786224      3      2005-02-10 13: 59: 10      2005-02-10 13: 59: 10
Count   Descri ption
1       heal th score is under threshol d 50%

done
ACMEPACKET#
```

Clearing Alarms

If an alarm situation is corrected, the corresponding alarm is cleared in the Net-Net system's alarm table and health is restored. You can also issue an ACLI command to clear a specific alarm:

To clear a specific Net-Net system alarm:

1. Ensure you are in Superuser Mode by entering the **show privilege** command. at the topmost ACLI level. For example:

```
ACMEPACKET# show privilege
console user - privilege level 1
```

- privilege level 0 refers Level 0:User Mode
 - privilege level 1 refers to Level 1: Superuser Mode.
2. Enter **display-alarms** to list the current alarms. Note the alarm ID (ID column) and task ID (Task column) of the alarm you want to clear. You will need this reference information in order to clear the alarm.
 3. Enter **clear-alarm** followed by a <Space>, the alarm ID, another <Space>, and the task ID of the task that generated the alarm.
 4. Press <Enter>.

With regard to redundant architectures, if you clear an alarm using the **clear-alarm** command without actually fixing the true cause of the alarm, it might have an adverse effect on the health score of the system and might, in turn, prevent future failover functionality.

About the Alarm Display on the Chassis

The alarm display appears in a two-line front panel display mode. During an alarm condition, the alarm display replaces the standard display on the chassis.

The first line of the graphic display shows the number of hardware-related alarms, if any. The second line of the graphic display shows the number of link-related alarms, if any. For example:

```
1 HW ALARM
2 LINK ALARMS
```

If the graphic display window indicates an alarm condition, the Net-Net system administrator must determine the nature of the condition by using the **display-alarms** ACLI command. Executing this command allows Net-Net system administrators to view specific details about the alarm.

When an alarm condition is cleared, the standard display replaces the alarm display.

Alarm Severity Levels

Five levels of alarm severity have been established for the Net-Net system. These levels have been designated so that the system can take action that is appropriate to the situation.

Alarm Severity	Description
Emergency	Requires immediate attention. If you do not attend to this condition immediately, there will be physical, permanent, and irreparable damage to your Net-Net system.
Critical	Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your Net-Net system.

Alarm Severity	Description
Major	Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net system will suffer no physical harm, but it will cease to function.
Minor	Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. There will be no physical harm to your Net-Net system. However, you should attend to this type of alarm as soon as possible in order to keep your Net-Net system operating properly.
Warning	Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your Net-Net system operating properly. For example, this type of alarm might indicate the Net-Net system is running low on bandwidth and you may need to contact your Acme Packet customer support representative to arrange for an upgrade.

Net-Net SBC Response to Alarms

The Net-Net system is capable of taking any of a range of actions when an alarm event occurs. It can present the alarms in the VED graphic display window on the front panel of the Net-Net chassis, use the `acmelog` (`syslog`) to log the events off the system, create an SNMP trap with an event notification, or use three dry contacts for external alarming.

Within the system, a database holds all information related to what actions to take given an event of a specific category and severity. This section sets out and defines these actions.

Writing to syslog (acmelog)

The term *syslog* refers to the protocol used for the network logging of system and network events. Because syslog facilitates the transmission of event notification messages across networks, the syslog protocol can be used to allow remote log access.

Sending SNMP Traps

An SNMP trap is essentially an event notification that can be initiated by tasks (such as the `notify` task), by Net-Net log messages, or by alarm reporting. When an event occurs, the Net-Net SBC sends a trap to the management station.

Although there is no direct correlation between Net-Net system alarms and the generation of SNMP traps, there is a correlation between Net-Net system alarms and the MIBs that support SNMP traps. For a list of the SNMP-related alarms and their associated traps, refer to the *MIB Reference Guide*.

About Dry Contacts

The Net-Net system supports three relays at the back of the Net-Net SBC chassis used for transmission of alarms called dry contacts. A dry contact is triggered for the following levels of severity:

- Critical
- Major
- Minor

Most often, the dry contact action is registered in the physical location of the Net-Net chassis. For example, there may be an LED signal on a communications cabinet.

Displaying Alarms to the Chassis

The Net-Net system can display a message concerning the alarm condition on the chassis itself. If this action is taken, a brief message appears in the VED graphic display window on the front panel of the Net-Net chassis.

Hardware and Environmental Faults

This section describes the hardware and environmental faults. It includes information about fan speed, voltage, temperature, and power supply for the Net-Net system.

Note: If you suspect you have a hardware fault, contact Acme Packet Technical Support for assistance with running the diagnostics image loaded on the Net-Net SBC.

Hardware Temperature Alarm

The following table describes the hardware temperature alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
TEMPERATURE HIGH	65538	SD1: CRITICAL: $\geq 70^{\circ}\text{C}$ MAJOR: $\geq 60^{\circ}\text{C}$ MINOR: $\geq 50^{\circ}\text{C}$ SD2: CRITICAL: $\geq 75^{\circ}\text{C}$ MAJOR: $\geq 65^{\circ}\text{C}$ MINOR: $\geq 55^{\circ}\text{C}$	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XXC (where XX.XX is the temperature in degrees)	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated apEnvMonStatusChangeEventNotification apSysMgmtTempTrap critical, major, minor dry contact 	CRITICAL: -100 MAJOR: -50 MINOR: -25
If this alarm occurs, the Net-Net system turns the fan speed up to the fastest possible speed.						

Fan Speed Alarm

The following table describes the fan speed alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
FAN STOPPED	65537	CRITICAL: any fan speed is <50%. Or speed of two or more fans is >50% and ≤75%. MAJOR: speed of two or more fans is > 75% and ≤ 90%. Or speed of one fan is >50% and ≤75% and the other two fans are at normal speed. MINOR: speed of one fan > 75% and ≤90%, the other two fans are at normal speed	Fan speed failure.	Fan speed: XXXX XXXX XXXX where xxxx xxxx xxxx is the Revolutions per Minute (RPM) of each fan on the fan module	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated apEnvMonStatusChangeEventNotification apSysMgmtFanTrap critical, major, minor dry contact 	CRITICAL: -100 MAJOR: -50 MINOR: -25

If this alarm occurs, the Net-Net system turns the fan speed up to the fastest possible speed.

Environmental Sensor Alarm

The following table describes the environmental sensor alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
ENVIRONMENTAL SENSOR FAILURE	65539	CRITICAL	The environmental sensor component cannot detect fan speed and temperature.	Hardware monitor failure! Unable to monitor fan speed and temperature!	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated critical, major, minor dry contact syslog <p>Acme Packet recommends you perform the following:</p> <ul style="list-style-type: none"> power cycle the standby Net-Net SBC peer using the power supply on/off switches located on the rear panel of the Net-Net chassis force a manual switchover by executing the ACLI notify berpd force command power cycle the active Net-Net SBC peer 	CRITICAL: -10

Media Link Alarms

Media link alarms include the following:

- Major

If the Net-Net SBC's media link goes from being up to being down, it is considered a major alarm. This alarm applies to both slots 1 and 2 on the Net-Net SBC. A message appears on the front panel of the Net-Net SBC's chassis, similar to the following:

```
MAJOR ALARM
Gig Port 1 DOWN
```

- Minor

If the Net-Net SBC's media link goes from being down to being up, it is considered a minor alarm. This alarm applies to both slots 1 and 2 on the Net-Net SBC.

Power Supply Alarms

The following table describes the power supply alarms

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PLD POWER A FAILURE	65540	MINOR (-10)	Power supply A has failed.	Back Power Supply A has failed!	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • minor dry contact • syslog
PLD POWER A UP	65541	MINOR	Power supply A is now present and functioning.	Back Power Supply A is present!	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • minor dry contact • syslog
If the Net-Net system boots up with one power supply, the health score will be 100, and no alarm will be generated. If another power supply is then added to that same Net-Net system, this same alarm will be generated, but the health score will not be decremented.					
PLD POWER B FAILURE	65542	MINOR (-10)	Power supply B has failed.	Back Power Supply B has failed!	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • minor dry contact • syslog
PLD POWER B UP	65543	MINOR	Power supply B is now present and functioning.	Back Power Supply B is present!	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • minor dry contact • syslog

Voltage Alarms

The following table describes the voltage alarms, which are only available for Net-Net SBC 2:

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PLD VOLTAGE ALARM 2P5V	65544	MINOR EMERGENCY		<ul style="list-style-type: none"> Voltage 2.5V CPU has minor alarm Voltage 2.5V CPU has emergency alarm, the system should shutdown 	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated dry contact syslog
PLD VOLTAGE ALARM 3P3V	65545	MINOR EMERGENCY		<ul style="list-style-type: none"> Voltage 3.3V has minor alarm Voltage 3.3V has emergency alarm, the system should shutdown 	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated dry contact syslog
PLD VOLTAGE ALARM 5V	65546	MINOR EMERGENCY		<ul style="list-style-type: none"> Voltage 5V has minor alarm Voltage 5V has emergency alarm, the system should shutdown 	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated dry contact syslog
PLD VOLTAGE ALARM CPU	65547	MINOR EMERGENCY		<ul style="list-style-type: none"> Voltage CPU has minor alarm Voltage CPU has emergency alarm, the system should shutdown 	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated dry contact syslog

Physical Interface Card Alarms

The following table describes the physical interface card alarms.

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PHY0 Removed	65550	MAJOR	Physical interface card 0 was removed.	PHY card 0 has been removed.	
PHY0 Inserted	65552	MAJOR	Physical interface card 0 was inserted.	None	
PHY1 Removed	65553	MAJOR	Physical interface card 1 was removed.	PHY card 1 has been removed.	
PHY1 Inserted	65554	MAJOR	Physical interface card 1 was inserted.	None	

Viewing PROM Statistics (Net-Net SBC 1 only)

Display PROM statistics for the following Net-Net SBC 1 components by using the `show prom-info` command:

- mainboard (chassis)
- CPU
- PHY0
- PHY1
- CAM (Net-Net SBC2 IDT PROM only)
- all

For example:

ACMEPACKET# **show prom-info mainboard**

Contents of Main Board PROM

```

Assy, Session Director with CAM
Part Number:                102-1001-00
Serial Number:              010323001127
Functional Rev:             1.18
Board Rev:                  2
PCB Family Type:           Session Director
ID:                         Session Director I
Format Rev:                 3
Options:                    0
Manufacturer:               MSL, Lowell
Week/Year:                  23/2003
Sequence Number:            001127
Number of MAC Addresses:    16
Starting MAC Address:       00 08 25 01 07 60
    
```

The following example shows the host CPU PROM contents.

ACMEPACKET# **show prom-info cpu**

Contents of Host CPU PROM

```

Assy, Processor 7455 Daughter Card
Part Number:                002-0300-01
Serial Number:              010303000456
Functional Rev:             1.10
Board Rev:                  4
PCB Family Type:           Session Director
ID:                         Host CPU (7451/7455)
Format Rev:                 3
Options:                    0
Manufacturer:               MSL, Lowell, MA
Week/Year:                  03/2003
Sequence Number:            000456
    
```


Graphic Window Display

The Environment display lets you scroll through information about the operational status of the hardware displayed in the Net-Net SBC chassis's graphic window. For example, you can view hardware- and link-related alarm information, highest monitored temperature reading, and fan speed.

The graphic display window presents the following Environment information in the order listed:

Alarm state
temperature
fan speed

- alarm state: HW ALARM: X (where X is the number of hardware alarms, excluding ENVIRONMENTAL SENSOR FAILURE) and LINK ALARM: X (where X is the number of link down alarms)
- temperature: format is XX.XX C, where XX.XX is the temperature in degrees
- fan speed: XXXX, where XXXX is the RPM of the failing fan on the fan module

For example:

HW ALARM: 1
LINK ALARM: 2
TEMPERATURE: 38.00 C
FAN SPEED: 5800

From this display, pressing <Enter> for the Return selection refreshes the information and returns you to the main Environment menu heading.

Note: Environmental sensor failure alarms are not displayed in the graphic display window on the front panel.

Fan Stopped Alarm

The fan stopped alarm presents the following in the graphic display window:

X HW ALARM(S) (where X indicates the number of HW alarms that exist on the Net-Net system)

Temperature High Alarm

The temperature high alarm presents the following in the graphic display window:

X HW ALARM(S) (where X indicates the number of HW alarms that exist on the Net-Net system)

System Fault Statistics

This section contains information about system faults. System faults include problems related to CPU usage, memory usage, and license capacity. System faults also include the functionality of the Address Resolution Protocol (ARP) on the Net-Net system.

System State

You can use the following commands to view system uptime and state information:

- **show uptime**
- **show system-state**

Viewing System Uptime

Display current date and time information and the length of time the system has been running in days, hours, minutes, and seconds by using the **show uptime** command. For example:

```
ACMEPACKET# show uptime
FRI FEB 25 13:02:55 2005 - up 0 days, 3 hours, 42 minutes, 30 seconds
```

Viewing System State

Display whether the Net-Net SBC is currently online or offline by using the **show system-state** command. For example:

```
ACMEPACKET# show system-state
The current system state is online
```

System Resources

You can use the following command to view the system resource statistics:

- **show processes cpu**

Viewing CPU Usage

Display CPU usage information, categorized on a per task/process basis, for your Net-Net SBC by using the **show processes cpu** command.

For example:

```
ACMEPACKET# show processes cpu
```

Task Name	Task Id	Pri	Status	Total CPU	Avg	Now
tAl arm	1be43bb0	60	DELAY	29.524	0.0	0.0
tAndMgr	1335f370	95	PEND+T	11.450	0.0	0.0
tNetTask	06acf730	50	READY	6.809	0.0	0.0
tAtcpd	18ba1130	75	PEND+T	4.236	0.0	0.0
tTffsPTask	06a0eae0	100	DELAY	2.956	0.0	0.0
tSSH	1bfab580	55	PEND+T	2.419	0.0	0.0
tNpwbTmr	1883abd0	0	DELAY	1.881	0.0	0.0
tSysmand	1320a960	75	PEND+T	1.879	0.0	0.0
tExcTask	027588e8	0	PEND	1.680	0.0	0.0
tTaskCheck	132d09c0	100	DELAY	1.116	0.0	0.0
tH323d	1ba661f0	80	PEND+T	1.086	0.0	0.0
tSi pd	1b970c50	80	PEND+T	1.032	0.0	0.0
tArpMgr	188614e0	61	PEND	0.691	0.0	0.0
tArpTmr	18861890	61	DELAY	0.490	0.0	0.0
ti fXCheck	1be28db0	60	DELAY	0.483	0.0	0.0

```

tXbdService      131d9ba0  50  PEND+T              0. 428   0. 0   0. 0
-----
Appl i cati ons              55. 998   0. 0
System              18: 10: 21              0. 2

```

The output of the **show processes cpu** command includes the following information:

- Task Name—Name of the Net-Net system task or process
- Task Id—Identification number for the task or process
- Pri—Priority for the CPU usage
- Status—Status of the CPU usage
- Total CPU—Total CPU usage since last reboot in hours, minutes, and seconds
- Avg—Displays percentage of CPU usage since the Net-Net system was last rebooted
- Now—CPU usage in the last second

CPU Utilization Alarm

The following table lists the CPU utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
CPU UTILIZATION	131099	MINOR	CPU usage reached 90% or greater of its capacity.	CPU usage X% over threshold X%	<ul style="list-style-type: none"> • apSysMgmtGroupTrap trap generated • minor dry contact • syslog

Memory Usage

You can use the following commands to view memory statistics:

- **show memory usage**
- **check-space-remaining**
- **show buffers**

Viewing Memory Usage Statistics

Display memory usage statistics by using the **show memory usage** command. For example:

```

ACMEPACKET# show memory usage
  status      bytes      blocks   avg block   max block
-----
current
free         809685728        153    5292063   809068608
all oc       225332816        4203     53612      -
i n t e r n a l         448           2        224      -
cumul at i v e
all oc       228178000       17335     13162      -
peak
all oc       225504896          -          -          -
Memory Errors:
  Li n k s   Repai red          0

```

Paddi ng Modi fi ed	0
Nodes Removed	0
Removal Fai lures	0
Fatal Errors	0

Checking Remaining Boot Directory Space

Display the remaining amount of space in the boot directory, code (or flash memory), and ramdrv devices by using the **check-space-remaining** command. You can check the following three directories:

- boot
- code
- ramdrv

For example:

```
ACMEPACKET# check-space-remaini ng boot
boot: 29759488/29760512 bytes (99%) remaini ng
```

```
ACMEPACKET# check-space-remaini ng code
code: 26351616/29760512 bytes (88%) remaini ng
```

```
ACMEPACKET# check-space-remaini ng ramdrv
ramdrv: 131218944/132104192 bytes (99%) remaini ng
ACMEPACKET#
```

Viewing Memory Buffer Statistics

Display memory buffer statistics by using the **show buffers** command. The memory buffer statistics are divided into three sections:

- Number of specific buffer types
- Total number of buffers and number of times the system failed, waited, or had to empty a protocol to find space
- Cluster pool table

For example:

```
ACMEPACKET# show buffers
type          number
-----
FREE   :    20990
DATA   :         1
HEADER :         1
TOTAL  :    20992
number of mbufs: 20992
number of times failed to find space: 0
number of times waited for space: 0
number of times drained protocols for space: 0
```

CLUSTER POOL TABLE

size	clusters	free	usage	mi nsi ze	maxsi ze	empty
------	----------	------	-------	-----------	----------	-------

64	8192	8192	116	4	56	0
128	8192	8191	152266	128	128	0
256	2048	2047	35296	131	255	0
512	2048	2048	644	258	512	0
1024	256	256	4	595	718	0
2048	256	256	7	1444	2048	0

Memory Utilization Alarm

The following table describes the memory utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MEMORY UTILIZATION	131100	MAJOR	Memory usage reached 90% or greater of its capacity.	Memory usage X% over threshold X%	<ul style="list-style-type: none"> apSysMgmtGroupTrap trap generated minor dry contact syslog

License Capacity

If the total number of active sessions on the system (across all protocols) is within 98-100% of the system's licensed capacity, an alarm and trap will be generated. The severity of this application alarm is MAJOR, but is not HA health-affecting.

The total number of active sessions is checked at an interval of 5 seconds (just as the system temperature and fans speed are). Once an *approaching capacity* alarm is triggered, another one will not be triggered until after the current alarm is cleared. This alarm will be cleared (and the trap sent, apLicenseNotApproachingCapacityNotification) after the total number of active sessions has gone to or below 90% of capacity, but no sooner than 15 seconds after the original alarm was triggered.

The following table describes the license capacity alarm

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LICENSE ALARM APPROACHING SESSION CAPACITY	327684	MAJOR	Total number of active sessions on the system (across all protocols) is within 98 to 100% of the Net-Net system's licensed capacity.	Total number of sessions (<#>) is approaching licensed capacity (<#>)	<ul style="list-style-type: none"> apLicenseApproachingCapacityNotification

Configuration Statistics

You can use the following commands to display configuration information:

- show configuration
- show running-config
- realm-specifics <realm ID>
- show virtual-interfaces

Specifying a Configuration Element

Both the **show configuration** and the **show running-config** commands let you include a configuration element name as an argument to view only instances for that configuration element. The list of valid configuration elements you can use as an argument include the following:

- account-config—Show account-config object
- h323-config—Show h323-config object
- h323-stack—Show all h323-stack objects
- iwf-stack—Show iwf-stack object
- host-route—Show all host-route objects
- local-policy—Show all local-policy objects
- media-profile—Show all media-profile objects
- media-manager—Show media-manager object
- mgcp-config—Show mgcp-config object
- dns-config—Show all dns-config objects
- network-interface—Show all network-interface objects
- ntp-config—Show ntp-config object
- phys-interface—Show all phys-interface objects
- realm—Show all realm objects
- MediaPolicy—Show all MediaPolicy objects
- ClassPolicy—Show all ClassPolicy objects
- redundancy-config—Show redundancy-config object
- ResponseMap—Show all ResponseMap objects
- session-agent—Show all session-agent objects
- session-group—Show all session-group objects
- session-translation—Show all session-translation objects
- translation-rules—Show all translation-rules objects
- session-router—Show session-router object
- sip-config—Show all sip-config objects
- sip-feature—Show all sip-feature objects
- sip-interface—Show all sip-interface objects
- sip-nat—Show all sip-nat objects
- snmp-community—Show all snmp-community objects
- static-flow—Show all static-flow objects
- steering-pool—Show all steering-pool objects
- system-config—show system-config object
- TrapReceiver—Show all TrapReceiver objects
- call-recording-server—Show call-recording-server configurations
- capture-receiver—Show capture-receiver configurations
- rph-profile—Show rph-profile configurations

- rph-policy—Show rph-policy configurations
- password-policy—Show password-policy configuration
- enforcement-profile—Show enforcement-profile configurations
- realm-group—Show realm-group configurations
- inventory—Displays an inventory of all configured elements on the Net-Net SBC

Viewing Current Configuration

Display information about the current configuration (used once the **activate-config** command is executed) by using the **show configuration** command. You can include the name of a configuration element with the **show configuration** command to display only instances for that configuration element.

For example:

```
ACMEPACKET# show configuration media-manager
media-manager
    state                      enabled
    latching                   enabled
    flow-time-limit            86400
    initial-guard-timer        300
    subsq-guard-timer          300
    tcp-flow-time-limit        86400
    tcp-initial-guard-timer     300
    tcp-subsq-guard-timer      300
    tcp-number-of-ports-per-flow 2
    hnt-rtcp                   disabled
    algd-log-level             NOTICE
    mbcdd-log-level            NOTICE
    red-flow-port              1985
    red-mgcp-port              1986
    red-max-trans               10000
    red-sync-start-time         5000
    red-sync-comp-time          1000
    max-signaling-bandwidth    10000000
    max-untrusted-signaling     100
    min-untrusted-signaling     30
    app-signaling-bandwidth     0
    tolerance-window           30
    rtcp-rate-limit            0
    min-media-allocation       32000
    min-trusted-allocation     1000
    deny-allocation            1000
    anonymous-sdp               disabled
    arp-msg-bandwidth           32000
    last-modified-date          2007-04-05 09:27:20
task done
```

Viewing Running Configuration

Display the running configuration information currently in use on the Net-Net system by using the **show running-config** command. You can include the name of a configuration element with the **show configuration** command to display only the instances for that configuration element.

For example:

```

ACMEPACKET# show running-config realm
realm-config
    identifier                testrealm
    address                    0.0.0.0
    network-interfaces
    mm-in-realm                disabled
    mm-in-network              enabled
    mm-same-ip                 enabled
    mm-in-system               disabled
    bw-cac-non-mm              disabled
    msm-release                disabled
    qos-enable                 disabled
    max-bandwidth              0
    ext-policy-svr              boffo.com
    max-latency                 0
    max-jitter                  0
    max-packet-loss            0
    observ-window-size         0
    parent-realm
    dns-realm
    media-policy
    in-translation
    out-translation
    in-manipulation
    out-manipulation
    class-profile
    average-rate-limit         0
    access-control-trust-level low
    invalid-signal-threshold   0
    maximum-signal-threshold   0
    untrusted-signal-threshold 758
    deny-period                 30
    symmetric-latching         disabled
    pai-strip                   disabled
    trunk-context
    early-media-allow         reverse
    additional-prefixes
                                10.0.0.0/24
                                172.16.0.0

    restricted-latching        peer-ip
    restriction-mask             17
    accounting-enable            enabled
    user-cac-mode                none
    user-cac-bandwidth           0
    user-cac-sessions            0
    net-management-control       disabled
    delay-media-update           disabled
    codec-policy
    codec-manip-in-realm         disabled
    last-modified-date           2006-07-06 12:43:39

```

Viewing Realm-Specific Configuration

Display realm-specific configuration based on the input realm ID by using the **realm-specifics <realm ID>** command. The information displayed includes the following:

- realm-config
- steering-pool
- session-agent
- session-translation
- class-policy
- local-policy (if the source realm or destination realm are defined)

For example:

```

ACMEPACKET# realm-specifics testrealm
realm-config
    identifier                testrealm
    addr-prefix               0.0.0.0
    network-interfaces
    mm-in-realm               disabled
    mm-in-network             enabled
    mm-same-ip                enabled
    mm-in-system              disabled
    bw-cac-non-mm             disabled
    msm-release               disabled
    qos-enable                disabled
    max-bandwidth             0
    ext-policy-svr            boffo.com
    max-latency               0
    max-jitter                0
    max-packet-loss           0
    observ-window-size        0
    parent-realm
    dns-realm
    media-policy
    in-translation
    out-translation
    in-manipulation
    out-manipulation
    class-profile
    average-rate-limit        0
    access-control-trust-level low
    invalid-signal-threshold  0
    maximum-signal-threshold  0
    untrusted-signal-threshold 758
    deny-period               30
    symmetric-latching        disabled
    pai-strip                 disabled
    trunk-context
    early-media-allow        reverse
    additional-prefixes
                                10.0.0.0/24
                                172.16.0.0

    restricted-latching       peer-ip
    restriction-mask           17
    accounting-enable          enabled
    user-cac-mode              none
    user-cac-bandwidth         0
    user-cac-sessions          0

```

net-management-control	disabled
delay-media-update	disabled
codec-policy	
codec-manip-in-real m	disabled
last-modified-date	2006-07-06 12:43:39
sip-interface	
state	enabled
realm-id	testrealm
sip-port	
address	192.168.10.12
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	register-prefix
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	maddr
nat-traversal	none
nat-interval	30
tcp-nat-interval	30
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
options	disable-privacy
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401, 407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass

```

ccf-address
ecf-address
term-tgrp-mode           none
implicit-service-route    disabled
rfc2833-payload          101
rfc2833-mode              transparent
constraint-name
response-map
local-response-map
last-modified-date        2006-06-12 12:08:34

```

Configuration Save Failed Alarm

The following table lists the CFG ALARM SAVE FAILED alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby Net-Net SBC peer operating as part of an HA pair.	save-config failed on <i>targetName</i> /code full, config sync stopped! or save-config failed on <i>targetName</i> /code full, config sync stopped! (where the <i>targetName</i> is the target name (tn) configured in the boot parameters)	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated syslog

HA Functionality

You can monitor HA Net-Net SBC functionality using the following ACLI commands:

- **show health** to view information about the HA Net-Net architecture and associated HA Net-Net SBC peers.
- **show redundancy** to view information about the synchronization of media flows and signaling for the members of an HA Net-Net SBC pair.

You can also view state displays on the chassis's graphical window display.

Viewing Health Information

Display the following information for HA architectures by using the **show health** command:

Note: The spaces are intentionally used in the following examples because they appear on the screen.

- Health score
- Whether the current HA Net-Net SBC is active, standby, or out of service
- Whether the media flow information is synchronized for all supported protocols: SIP, H.323, and MGCP (*true/false*)
- If media flow information is not available, "Media Synchronized disabled" will be displayed in the **show health** output.
- Whether SIP signaling information is synchronized (*true/false*)
- If SIP signaling is not available, "SIP Synchronized disabled" will be displayed in the **show health** output.

- Whether or not MGCP signaling information is synchronized (true/false)
- If MGCP signaling is not available, “MGCP Synchronized disabled” is displayed in the show health output.
- Whether configuration information is synchronized (true/false)
- If configuration checkpointing is not available, “Config Synchronized disabled” will be displayed in the show health output.
- The IPv4 address of the current HA Net-Net SBC’s active peer (an HA Net-Net SBC that is currently active does not have an active Net-Net SBC peer and shows 0.0.0.0)
- The last message received from the HA Net-Net SBC peer
- A switchover log containing the last 20 switchover events (whether becoming active or relinquishing the active role)

The following example shows a currently active Net-Net SBC.

ACMEPACKET# **show health**

```
Media Synchronized      enabled
SIP Synchronized        enabled
MGCP Synchronized       enabled
H248 Synchronized       enabled
Config Synchronized     enabled
Collect Synchronized    enabled
Radius CDR Synchronized enabled
Rotated CDRs Synchronized enabled
Active Peer Address      163.4.12.2
```

Redundancy Protocol Process (v2):

```
State                Active
Health               100
Lowest Local Address 11.0.0.1:9090
1 peer(s) on 1 socket(s):
systest3B: v2, Standby, health=100, max silence=1050
last received from 11.0.0.2 on wancom1:0
```

Switchover Log:

```
Jul 11 14:18:21.442: Active to RelinquishingActive
Jul 11 14:24:00.872: Standby to BecomingActive, active peer
systest3B has timed out. The following example that follows shows a
currently standby Net-Net SBC.
```

Viewing Redundancy Information

Display the following information about HA architecture by using the **show redundancy** command:

- General HA statistics
- Statistics related to HA transactions that have been processed
- Timestamp showing when the current period began
- The numerical identifier for the last redundant transaction processed (each transaction is numbered)

In an HA architecture that is functioning properly, the number for the last redundant transaction processed on a standby Net-Net SBC peer should not be far behind (if not exactly the same as) the one shown for the active Net-Net SBC peer.

Several subcommands appear under the **show redundancy** command. Within this set of subcommands, Net-Net system administrators can view information related to HA transactions, including specific transaction information.

The following example shows the subcommands available for the **show redundancy** command.

```
ACMEPACKET# show redundancy ?
```

al gd	MGCP Redundancy Statistics
col lect	Collect Redundancy Statistics
confi g	Configuration Redundancy Statistics
l i nk	Shows Link Redundancy Configuration
mbcd	MBC Redundancy Statistics
radi us-cdr	Radius CDR Redundancy Statistics
rotated-cdr	Rotated Radius CDR Redundancy Statistics
si pd	SIP Redundancy Statistics

HA Alarms

There are currently five alarms directly associated with the HA feature. A Net-Net system alarm is triggered when any of the following HA conditions occurs:

- When the health score falls below 60.
This is a hard-coded threshold value. It is not configurable.
- By the Active-BecomingStandby peer upon switchover.
- By the Standby-BecomingActive peer upon switchover.
- When the HA Net-Net SBC peer times out.
- When the standby system is unable to synchronize with its active Net-Net SBC peer within the amount of time set for the becoming standby time field of the redundancy element.

When certain alarms associated with the HA feature are triggered, traps are sent via the appropriate MIB (for example, syslog or system management). Traps for switchover alarms indicate that a switchover has occurred and identify the state transition of the HA Net-Net SBC reporting the switchover. For example:

- Standby to BecomingActive
- BecomingStandby to BecomingActive
- Active to RelinquishingActive and so on

In the case of an alarm from the Standby to BecomingActive peer, the associated trap also indicates the reason for switchover (as far as high availability is concerned). These reasons might include reporting the degraded health of the HA Net-Net SBC peer or indicating that the HA Net-Net SBC peer has timed out or that a switchover was forced by command.

The following table provides a list, by name, of the Net-Net SBC's HA-related alarms, including their alarm IDs, severities, causes, associated log messages, and actions.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
HEALTH SCORE	131101	MAJOR	Net-Net system's health score fell below 60.	Health score X is under threshold (where X is the health score)	<ul style="list-style-type: none"> apSysMgmtGroupTrap
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	<ul style="list-style-type: none"> apSysMgmtGroupTrap
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	<ul style="list-style-type: none"> apSysMgmtGroupTrap
REDUNDANT SWITCH-TO-ACTIVE	131104	CRITICAL	A state transition occurred from Standby/BecomingStandby to BecomingActive.	Switchover, <state to state>, active peer <name of HA peer> has timed out or Switchover, <state to state>, active peer <name of HA peer> has unacceptable health (x) (where x is the health score) or Switchover, <state to state>, forced by command	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtRedundancyTrap
REDUNDANT SWITCH-TO-STANDBY	131105	CRITICAL	A state transition occurred from Active/BecomingActive to BecomingStandby/RelinquishingActive.	Switchover, <state to state>, peer <name of HA peer> is healthier (x) than us (x) (where x is the health score) or Switchover, <state to state>, forced by command	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtRedundancyTrap
REDUNDANT TIMEOUT	131106	MAJOR	An HA Net-Net system peer was not heard from within a time period.	Peer <name of HA peer> timed out in state x, my state is x (where x is the state (for example, BecomingStandby))	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtRedundancyTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
REDUNDANT OUT OF SERVICE	131107	CRITICAL	Unable to synchronize with Active HA Net-Net system peer within BecomingStandby timeout.	Unable to synchronize with Active redundant peer within BecomingStandby timeout, going OutOfService	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtRedundancyTrap
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby Net-Net SBC peer operating as part of an HA pair.	save-config failed on <i>targetName</i> /code full, config sync stopped! or save-config failed on <i>targetName</i> /code full, config sync stopped! (where the <i>targetName</i> is the target name (tn) configured in the boot parameters)	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated syslog

Base Display Level

The base display level of the graphic display window on the front panel of the Net-Net chassis shows the state of an HA Net-Net SBC. The base display appears when the Net-Net SBC first starts up and when the graphic display times out at any menu level.

Net-Net system administrators can distinguish between an active Net-Net SBC and a standby Net-Net SBC in an HA architecture by looking at the front of the chassis. The Net-Net chassis operating as the standby Net-Net SBC in an HA architecture displays an “(s)” in the graphic display window to indicate its status as the standby system. The Net-Net chassis operating as the active Net-Net SBC in an HA architecture does not display anything in parentheses in the graphic display window.

HA State Display Stats

The Net-Net chassis’s graphic display window shows the current state of the HA Net-Net SBC using an abbreviation that follows the Net-Net SBC name. The states are defined in the following table.

State Abbreviation	Description
(I)	Initial (the Net-Net SBC is in this state when it is booting)
(O/S)	Out of service
(B/S)	Becoming standby
(S)	Standby
(nothing displayed after the Net-Net SBC name)	Active

Refer to the following sections for examples of the graphic display window output.

Initial State Displays

The following example shows the output in the graphic display window of a Net-Net SBC in the initial state:

```
NET - NET
SESSION DIRECTOR (I)
```

Out Of Service State Displays

The following examples show the output in the graphic display window of an out-of-service Net-Net SBC:

```
NET - NET
SESSION DIRECTOR (O/S)
```

Becoming Standby State Displays

The following example shows the output in the graphic display window of a Net-Net SBC becoming standby:

```
NET - NET
SESSION DIRECTOR (B/S)
```

Standby State Displays

The following example shows the output in the graphic display window of a standby Net-Net SBC:

```
NET - NET
SESSION DIRECTOR (S)
```

Active State Displays

HA Net-Net SBCs in the active state use the default graphic display. The following example show the display of an active Net-Net SBC.

```
NET - NET
SESSION DIRECTOR
```

For further information about the Net-Net SBC chassis and graphic display window, refer to the Net-Net Session Director Hardware Installation Guide, which can be found on your Acme Packet documentation CD.

ARP Functionality

You can use the following command to view ARP functionality information:

- **arp-check**
- **show arp**

Testing Address Resolution

Test a specific address resolution by using the **arp-check** command; which causes a test message to be sent. The test is successful when an OK is returned.

To run this test, you must enter the following information after typing **arp-check** and a <Space>:

- media interface slot (either of two values: 1 is for the left, and 2 is for the right)
- VLAN identifier

Note: If there is no VLAN identifier to be entered, enter a value of 0.

- IPv4 address (in dotted notation).

For example:

```
ACMEPACKET# arp-check 1 6 192.168.100.1
```

```
ARP: Sendi ng  ARP REQ port=0, vl an=6, source_i pa=192.168.200.10,
target_i pa=192.168.100.1
```

```
ACMEPACKET#
```


Viewing Current Address Mappings

Display the current Internet-to-Ethernet address mappings in the ARP table by using the **show arp** command. The first section of this display shows the following information: destination, gateway, flags, reference count, use, and interface. The second section shows the interface, VLAN, IP address, MAC address, timestamp, and type.

The intf (interface) column in the ARP includes both slot and port information. If a value of 0/1 appears, 0 refers to the slot and 1 refers to the port. For example:

ACMEPACKET# **show arp**

LINK LEVEL ARP TABLE

destination	gateway	flags	Refcnt	Use	Interface
172.30.0.1	00:0f:23:4a:d8:80	405	1	0	wancom0

Total ARP Entries = 3

Intf	VLAN	IP-Address	MAC	time-stamp	type
0/0	0	010.000.045.001	00:00:00:00:00:00	1108462861	invalid

Special Entries:

0/0	0	000.000.000.000	00:00:00:00:00:00	1108462861	gateway
0/0	0	010.000.045.000	00:00:00:00:00:00	1108462861	network

Gateway Status:

Intf	VLAN	IP-Address	MAC	time-stamp	hb status
0/0	0	010.000.045.001	00:00:00:00:00:00	1108462861	unreachable

-- ARP table info --

```
Maximum number of entries : 512
Number of used entries    : 3
Length of search key      : 1 (x 64 bits)
First search entry address : 0x3cb0
Length of data entry      : 2 (x 64 bits)
First data entry address  : 0x7960
Enable aging              : 0
Enable policing           : 0
```

ARP Table Utilization Alarm

The following table describes the ARP table utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	<ul style="list-style-type: none"> apSysMgmtGroupTrap trap generated syslog

Local Policy

Use the following commands to view local policy statistics and information:

- **show running-config local-policy**
- **show configuration local-policy**

Viewing Running Configuration Local Policy

Display information about the local policy in the running configuration information in use on the Net-Net system by using the **show running-config local-policy** command. For example:

```
ACMEPACKET# show running-config local-policy
local-policy
    from-address                192.168.0.50
    to-address                  10.10.10.10
    source-realm                *
    activate-time               N/A
    deactivate-time             N/A
    state                       enabled
    policy-priority             urgent
    last-modified-date          2006-06-12 08:48:57
    policy-attribute
        next-hop                172.168.0.10
        realm
        action                   none
        terminate-recursion     enabled
        carrier
        start-time               0000
        end-time                 2400
        days-of-week             U-S
        cost                     0
        app-protocol
        state                     enabled
        media-profiles
task done
```

Viewing Current Configuration Local Policy

Display information about the local policy in the current configuration that will be used once the **activate-config** command is executed by using the **show configuration** command. For example:

ACMEPACKET# **show configuration local-policy**

ACMEPACKET# show running-config local-policy

local-policy

```

from-address
192.168.0.50

to-address
10.10.10.10

source-realm
*

activate-time
N/A

deactivate-time
N/A

state
enabled

policy-priority
urgent

last-modified-date
2006-06-12 08:48:57

policy-attribute
    next-hop
    172.168.0.10
    realm
    action
    none
    terminate-recursion
    enabled
    carrier
    start-time
    0000
    end-time
    2400
    days-of-week
    U-S
    cost
    0
    app-protocol
    state
    enabled
    media-profiles

```

task done

Session and Protocol Statistics

You can use the following commands to access protocol tracing statistics:

- **notify**
- **monitor sessions**

Viewing Runtime Protocol Tracing

Display information about runtime protocol tracing for UDP/ TCP sockets by using the **notify** command. This command provides information for all protocol messages for ServiceSocket sockets to be written in a log file or sent out of the Net-Net system to a UDP port.

This mechanism allows for tracing to be enabled for any socket, provided that the class has a *logit* method for displaying and formatting the protocol message. All ACP classes support this, as do SIP and MGCP. Tracing can be enabled for all processes, specific sockets, all sockets, or specific processes. Tracing for specific sockets is specified by the local IPv4 address and port on which the socket is connected.

```
notify all |<process-name> trace all |<socket-address><file-name> [<out-udp-
port>]
```

```
notify all |<process-name> notrace all |<socket-address>
```

The <socket-address> is the IPv4 address and the port on which the socket is connected. The <out-udp-port> is the UDP IPv4 address and port to which the log messages are sent. If the <out-udp-port> is not specified, the logs are written to the <file-name>.

Viewing Real-Time SIP Session Statistics

If you have Superuser access, you can display real-time SIP session statistics by using the **monitor sessions** command. For example:

ACMEPACKET# **moni tor sessi ons**

09: 10: 26-172

SIP Status	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Sessi ons	0	0	0	0	0	0
Subscri pti ons	0	0	0	0	0	0
Di al ogs	0	0	0	0	0	0
Cal l ID Map	0	0	0	0	0	0
Rej ecti ons	-	-	0	0	0	
ReINVIT ES	-	-	0	0	0	
Medi a Sessi ons	0	0	0	0	0	0
Medi a Pendi ng	0	0	0	0	0	0
Cl ient Trans	0	0	0	0	0	0
Server Trans	0	0	0	0	0	0
Resp Contexts	0	0	0	0	0	0
Saved Contexts	0	0	0	0	0	0
Sockets	0	0	0	0	0	0
Req Dropped	-	-	0	0	0	
DNS Trans	0	0	0	0	0	0
DNS Sockets	0	0	0	0	0	0
DNS Resul ts	0	0	0	0	0	0

Real-time statistics for the following categories appear on the screen:

- Dialogs
- Sessions
- CallID Map
- Rejections
- ReINVITES
- Media Sessions
- Media Pending
- Client Trans
- Server Trans
- Resp Contexts
- Sockets
- Reqs Dropped
- DNS Trans
- DNS Sockets
- DNS Results

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the Net-Net system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Media and Bandwidth Statistics

You can use the following commands to display media and bandwidth statistics:

- `show mbcd errors`
- `show mbcd realms`
- `monitor media`

Viewing MBCD Task Errors

Display Middle Box Control Daemon (MBCD) task error statistics by using the `show mbcd errors` command. There are two categories of MBCD error statistics: Client and Server.

For example:

```
ACMEPACKET# show mbcd errors
16: 19: 18-139
MBC Errors
```

	Recent	Total	PerMax
Client Errors	0	0	0
Client IPC Errors	0	0	0
Open Streams Failed	0	0	0
Drop Streams Failed	0	0	0
Exp Flow Events	0	0	0
Exp Flow Not Found	0	0	0
Transaction Timeouts	0	0	0
Server Errors	0	0	0
Server IPC Errors	0	0	0
Flow Add Failed	0	0	0
Flow Delete Failed	0	0	0
Flow Update Failed	0	0	0
Flow Latch Failed	0	0	0
Pending Flow Expired	0	0	0
ARP Wait Errors	0	0	0
Exp CAM Not Found	0	2	2
Drop Unknown Exp Flow	0	0	0
Drop/Exp Flow Missing	0	0	0
Exp Notify Failed	0	0	0
Unacknowledged Notify	0	0	0
Invalid Realm	0	5	5
No Ports Available	0	0	0
Insufficient Bandwidth	0	0	0
Stale Ports Reclaimed	0	0	0
Stale Flows Replaced	0	0	0
Pipe Alloc Errors	0	0	0
Pipe Write Errors	0	0	0

Client statistics count errors and events encountered by applications that use the MBCD to set up and tear down media sessions:

- Client Errors—Number of errors in the client application related to MBC transactions that are otherwise uncategorized

- Open Streams Failed—Number of errors related to sending Add or Modify requests to MBCD
- Drop Streams Failed—Number of errors related to sending Subtract requests to MBCD
- Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications
- Exp Flow Not Found—Number of flow timer expiration notifications received from the MBCD by all applications for which no media session or flow information was present in the application
- Transaction Timeouts—Number of MBC transaction timeouts
- Server statistics count errors and events encountered by MBCD
- Server Errors—Number of uncategorized errors in the MBC server
- Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table
- Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table
- Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow
- Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow
- Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table
- ARP Wait Errors—Number of errors and timeouts related to obtaining the Layer 2 addressing information necessary for sending media
- Exp CAM Not Found—This statistic shows the number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD from the NP
- Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification
- Drop/Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables. Also includes when a flow for a Subtract request to MBCD cannot be found
- Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application.
- Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner.
- No Ports Available—Number of steering port allocation requests not be satisfied due to a lack of free steering ports in the realm
- Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application
- Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm

Viewing Steering Port and Bandwidth Usage

Display steering ports and bandwidth usage for home, public, and private realms by using the **show mbcd realms** command.

For example:

```
acmepacket# show mbcd realms
```

```
18: 26: 39-1629
```

```

      --- Steering Ports ---  ----- Bandwidth Usage -----
Real m      Used   Free   No Ports   Flows Ingrss Egress   Total   Insuf BW
acme          0      0       0         0    OK    OK    OK       0
h323172       2 29999       0         0    OK    OK    OK       0
si p172       2 29999       0         0    OK    OK    OK       0
si p192       0 30001       0         0    OK    OK    OK       0

```

Information in the following categories is displayed:

- Used—Number of steering ports used
- Free—Number of free steering ports
- No Ports—Number of times that a steering port could not be allocated
- Flows—Number of established media flows
- Ingrss—Amount of bandwidth being used for inbound flows
- Egress—Amount of bandwidth being used for outbound flows
- Total—Maximum bandwidth set for this realm
- Insuf BW—Number of times that a session was rejected due to insufficient bandwidth

Viewing Real-Time Media Monitoring Statistics

If you have Superuser access, you can display real-time media monitoring statistics by using the **monitor media** command. For example:

```
acmepacket# monitor media
```

```
17: 31: 00-160
```

```

MBCD Status      Active  -- Period --  ----- Li fetime -----
                High   Total    Total   PerMax   High
Client Sessions  143    182    1930    1218332  4225    683
Client Trans     0      18     5744    2500196  8439    625
Contexts         144    182    1930    834745   2783    2001
Flows            296    372    3860    1669498  5566    3689
Flow-Port        286    362    3860    1669488  5566    3679
Flow-NAT         294    365    3788    1658668  5563    2051
Flow-RTCP        0      0      0        0        0        0
Flow-Hai rpin    0      0      0        0        0        0
Flow-Rel eased   0      0      0        0        0        0
MSM-Rel ease     0      0      0        0        0        0
Rel -Port        0      0      0        0        0        0
Rel -Hai rpin    0      0      0        0        0        0
NAT Entries      295    365    3791    1658671  5563    2051
Free Ports       7430   7518   7828    3346410  11604   8002
Used Ports       572    724    7724    3338980  11132   8000
Port Sorts       -      -      0       14796    4156
MBC Trans        1141   1234   5748    2503147  8440    2974
MBC Ignored      -      -      0        0        0
ARP Trans        0      0      0        8        8        1

```

Real-time statistics for the following categories appear on the screen:

- Client Sessions
- Client Trans
- Contexts
- Flows
- Flow-Port
- Flow-NAT
- Flow-RTCP
- Flow-Hairpin
- Flow-Release
- MSM-Release
- NAT Entries
- Free Ports
- Used Ports
- Port Sorts
- MBC Trans
- MBC Ignored
- ARP Trans

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the Net-Net system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Media Alarms

The following table describes the Media alarms:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	<ul style="list-style-type: none"> • apSyslogMessageGenerated (ap-slog.mib) • apSysMgmtMediaOutOfMemory
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	<ul style="list-style-type: none"> • apSyslogMessageGenerated (ap-slog.mib) • apSysMgmtUnknownRealm

MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	<ul style="list-style-type: none"> • apSyslogMessageGenerated (ap-slog.mib) • apSysMgmtMediaBandwidthTrap
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	<ul style="list-style-type: none"> • apSyslogMessageGenerated (ap-slog.mib) • apSysMgmtMediaPortsTrap

Task Statistics

You can use the following commands to display task information.

- **stack**
- **check-stack**

There is also an alarm that occurs when a system task is suspended.

Viewing Function Call Stack Traces

Display the function call stack trace for a specified task by using the **stack** command. It displays a list of nested routine calls for that specified task. Each routine call and its parameters are shown. The command takes a single argument, which is the task name or the task ID.

To use the stack command, enter stack followed by a <Space>, the task name or task ID, then <Enter>. (You can access a list of tasks by using the **show processes** command.)

For example:

```
acmepacket# stack sipd
0x001034f4 vxTaskEntry +60 : sipd(char *, semaphore *) ()
0x007e5404 sipd(char *, semaphore *)+1e0: sip_proxy_daemon(int, char **, semaphore *) ()
0x00a69ea4 sip_proxy_daemon(int, char **, semaphore *)+ae8:
Process::Run(int, int) ()
0x00f2c298 Process::Run(int, int)+5d8: Selector::do_select(const Time &, Time &) ()
0x00f3a7ec Selector::do_select(const Time &, Time &)+1a8: select ()
0x000eb640 select +1f8: semTake ()
0x000ed114 semTake +94 : semBTake ()
```

Viewing the Stack Trace

Display the stack trace for a specific task by using the **check-stack** command. For example:

```
ACMEPACKET# check-stack
```

NAME	ENTRY	TID	SIZE	CUR	HIGH	MARGIN
tMgrTask	mgrTask	0x3df00b50	12240	392	440	11800
tExcTask	excTask	0x3df185f0	8144	296	768	7376
tLogTask	logTask	0x3df19470	8144	344	1032	7112
tWatchDog	0x0000088334	0x3df197d0	4048	176	904	3144
tNpwbTmr	0x0001d02320	0x3df4c560	20432	168	1168	19264
ubsec_bh_han	0x0001d62f6c	0x3df22fe0	4048	176	248	3800
tCliSSH0	accli(tagCLI_	0x3df24ac0	65488	1920	9888	55600

tCliSSH1	accli(tagCLI_	0x3df66f80	65488	1920	9888	55600
tCliSSH2	accli(tagCLI_	0x3df67460	65488	1920	9888	55600
tCliSSH3	accli(tagCLI_	0x3df67940	65488	1920	9888	55600
tCliSSH4	accli(tagCLI_	0x3df67e20	65488	1920	9888	55600
tCli	cliInterface	0x3df68460	65488	6056	21432	44056
tCliTelnet	cliInterface	0x3df68840	65488	1968	19672	45816
tCliTelnet	cliInterface	0x3df68c20	65488	1968	9936	55552
tCliTelnet	cliInterface	0x3df69000	65488	1968	9936	55552
tCliTelnet	cliInterface	0x3df693e0	65488	1968	9936	55552
tCliTelnet	cliInterface	0x3df697c0	65488	1968	9936	55552
tWdbTask	wdbTask	0x3df1bfff0	8144	280	352	7792
tNetTask	netTask	0x3df1abd0	12240	224	1136	11104
tTelnetd	telnetd	0x3df1b5b0	32720	480	1208	31512
tl dmaInt	idma5700IntT	0x3df46be0	8144	272	344	7800
tSSH	SSH_startSer	0x3df68100	65488	424	760	64728
tFtp6d	0x00000433fc	0x3df1bb90	65488	408	1136	64352
tBrokerd	brokerd(char	0x3df24fc0	65488	1648	10920	54568
tNpFrmTx	app_send_tas	0x3df47440	20432	344	696	19736
tNpFrmRx	app_frame_rx	0x3df47820	20432	304	736	19696
tNpCellRx	app_cell_rx_	0x3df47b80	20432	304	376	20056
tNpDmaTx	app_idma_sen	0x3df48140	20432	304	2440	17992
tNpwbNpmRx	npwbNpmRxTas	0x3df4c840	20432	312	4592	15840
tlpFrag	0x0001ce1634	0x3df5af40	20432	272	344	20088
tAl arm	0x0001450910	0x3df66220	40912	336	1376	39536
tNpDmaRx	app_idma_fra	0x3df47e60	20432	280	2392	18040
tArpMgr	arp_manager_	0x3df5a0c0	20432	336	4968	15464
tArpTmr	arp_manager_	0x3df5a3a0	20432	304	392	20040
tPktCapMgr	pktpcpt_main	0x3df5bb80	20432	344	616	19816
tFlowGdTmr	nApp_fg_mai	0x3df5b320	20432	208	568	19864
tSysmand	sysmand	0x3df234c0	163792	2968	17880	145912
tAtcpd	atcpd(char *	0x3df5d6a0	65488	1928	12488	53000
tMbcd	mbcd_daemon(0x3df5ec60	65488	2784	17400	48088
tEbmd	ebmd_daemon(0x3df622c0	65488	3744	15864	49624
tLi d	li_daemon(ch	0x3df5f540	65488	1992	14880	50608
tAl gd	algd_daemon(0x3df603a0	65488	2088	15656	49832
tSi pd	si pd(char *,	0x3df62e20	98256	2488	17488	80768
tH323d	h323d(char *	0x3df63980	65488	2360	14720	50768
tH248d	h248d(char *	0x3df64360	65488	1864	10920	54568
tRadd	radd(char *,	0x3df60d80	65488	1456	12016	53472
tPusher	pusher(char	0x3df61960	65488	2096	12656	52832
tEvtMgrTask	evtMgr	0x3df1c5a0	4048	360	432	3616
tAndMgr	AND_start	0x3df46100	40912	536	2216	38696
tSnmpd	snmpd	0x3df64bc0	65488	1360	15216	50272
tLemd	lcmd(char *,	0x3df5c940	65488	2448	21592	43896
tAtcpApp	atcpAppTask(0x3df5e000	65488	1392	11952	53536
tDumper	tDumperMain	0x3df241a0	16336	240	600	15736

tTaskCheck	taskCheckMai	0x3df24480	16336	208	5856	10480
tCl i Worker	cl i WorkerTas	0x3df5c1e0	65488	240	14072	51416
tDcacheUpd	dcacheUpd	0x3df20f80	8144	160	248	7896
tPanel	0x0000021dc4	0x3df19f90	8144	240	312	7832
tI dl e	0x00000370f0	0x3df1a270	4048	96	96	3952
I N T E R R U P T			10000	0	928	9072

System Task Suspended Alarm

The following table describes the system task suspended alarm information.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
SYSTEM TASK SUSPENDED	131108	CRITICAL	A Net-Net system task (process) suspends or fails.	Task X suspended, which decremented health by 75! (where X is the task/process name)	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • major dry contact • syslog • reboot (if the Net-Net system is configured to do so)

System Problem Statistics

Packet Tracing

When you enable packet tracing (using the **packet-capture** configuration and related ACLI commands), the Net-Net SBC can mirror any communication between two endpoints, or between itself and a specific endpoint. To accomplish this, the Net-Net SBC replicates the packets sent and received, and can then send them to a trace server that you designate. Using the trace server, you can display the packets on software protocol analyzer. Currently, the Net-Net SBC supports:

- One configurable trace server (on which you have installed your software protocol analyzer)
- Sixteen concurrent endpoint traces

For more information about how to set up packet tracing, refer to the *Net-Net 4000 ACLI Configuration Guide*.

You can see statistics for packet traces initiated on the Net-Net SBC by using the **show packet-trace** command. The display shows you a summary of the active packet traces on the Net-Net SBC. Displayed information includes: the IP address, local and remote port (which displays as 0 if no ports have been designated), slot, port, and VLAN.

ACMEPACKET# **show packet-trace**

IP Address	Local -Port	Remote-Port	Slot	Port	VLAN
192. 168. 10. 1	0	0	0	1	0
192. 168. 10. 99	5060	5060	0	1	0
10. 0. 0. 1	23	0	1	0	0

Capturing and Viewing Packets

You can capture and view packets for debugging purposes by using the **packet-capture** command. For example, if you detect an issue with the Net-Net system flows, you can capture certain packets so that you can resolve the problem. Using

this command, you can examine the packets in question and then perform any debugging that might be necessary.

When you use packet-capture, you work with the following subcommands:

- **packet-capture enable**
- **packet-capture show**
- **packet-capture detail**

Use the **packet-capture enable** command to enable packet-capture before using it. Because enabling this function uses system resources that should otherwise be kept free, you should enable it only when you need it and then disable it when you finish debugging.

Use the **packet-capture show** command to view a summary of the most recently captured packets, including the following:

- ingress interface
- frame format
- type/length
- VLAN identifier
- source IPv4 address
- destination IPv4 address
- protocol
- source port
- destination port

For example:

acmepacket# **packet-capture show**

Entry #	Ingress IF	Frame Format	Type/Length	VLAN ID	Source IP address	Destination IP address
Protocol	Src Port	Dest Port				
1	1/0	unknown	0x0026	-	-	-
-	-	-				
2	1/0	unknown	0x0026	-	-	-
-	-	-				
3	1/0	unknown	0x0026	-	-	-
-	-	-				
4	1/0	unknown	0x0026	-	-	-
-	-	-				
5	1/0	unknown	0x0026	-	-	-
-	-	-				
6	1/0	unknown	0x0026	-	-	-
-	-	-				
7	1/0	unknown	0x0026	-	-	-
-	-	-				
8	1/0	unknown	0x0026	-	-	-
-	-	-				
9	1/0	unknown	0x0026	-	-	-
-	-	-				
10	1/0	unknown	0x0026	-	-	-
-	-	-				

11	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
12	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
13	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
14	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
15	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
16	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-
17	1/0	unknown	0x0026	-	-	-
-	-	-	-	-	-	-

Use the **packet-capture detail** command to view the details of a particular packet, including: the ingress interface, MAC source address, MAC destination address, VLAN identifier, and the length/type. For example:

```
acmepacket# packet-capture detail 30
Ingress Slot/Port: 1/0
FF FF FF FF FF FF 00 0D 28 74 A2 01 08 00
45 00 00 4C 08 E9 00 00 40 11 61 18 AC 10 64 90 FF FF FF FF
00 7B 00 7B 00 38 00 00
1B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00
```

DIX header ---

```
MAC Src Addr      : 0x FF FF FF FF FF FF
MAC Dest Addr     : 0x 00 0D 28 74 A2 01
VLAN ID           : 0x XX
Length/Type       : 0x 0800
```

IP Header ---

```
IP Version        : 4
IP Header Length  : 5
Type-of-Servic e  : 0
Total Length      : 76
Identifi caton    : 2281
Flags             : 0
Fragment Offset   : 0
Time-to-Live      : 64
protocol          : 17
Header Checksum   : 0x6118
Source IP Addr    : 172. 16. 100. 144
Destination IP Addr : 255. 255. 255. 255
```

UDP Header ---

```
Source Port       : 123
```

```

Destination Port    : 123
Length              : 56
Checksum            : 0x0000
  
```

System ACLs

This section provide information about system ACL removal, and about viewing system ACL statistics and configurations.

Notes on Deleting System ACLs

If you delete a system ACL from your configuration, the Net-Net SBC checks whether or not there are any active FTP or Telnet client was granted access when the entry was being removed. If such a client were active during ACL removal, the Net-Net SBC would warn you about the condition and ask you to confirm the deletion. If you confirm the deletion, then the Net-Net SBC's session with the active client is suspended.

The following example shows you how the warning message and confirmation appear. For this example, and ACLI has been deleted, and the user is activating the configuration that reflects the change.

```

ACMEPACKET# activate-config
Object deleted will cause service disruption:
system-access-list: identifier=172.30.0.24

** WARNING: Removal of this system-ACL entry will result
            in the lockout of a current FTP client

Changes could affect service, continue (y/n) y

Activate-Config received, processing.
  
```

Viewing System ACL Configurations

The **system-access-list** configuration has been added to the list of configurations you can display using the **show configuration** and **show running-config** CLI commands. It will display each system ACL entry.

```

ACMEPACKET# show running-config system-access-list
system-access-list
    dest-address      165.31.24.2
    netmask           225.225.0.0
    last-modified-date 2007-04-30 13:00:02
system-access-list
    dest-address      175.12.4.2
    netmask           225.225.225.0
    last-modified-date 2007-04-30 13:00:21
task done
  
```

Viewing System ACL Statistics

You can display statistics for system ACLs using the **show ip stats** CLI command. Two new entries have been added to let you see the total number of ACL denials and the last ACL denial the Net-Net SBC made.

```

ACMEPACKET# show ip stats
      total      3170
      badsum      0
      tooshort    0
  
```

toosmal l	0
badhl en	0
badl en	0
infragments	0
fragdropped	0
fragti meout	0
forward	0
fastforward	0
cantforward	14
redi rectsent	0
unknownprotocol	0
del i vered	1923
l ocal out	855
nobuffers	0
reassembl ed	0
fragmented	0
outfragments	0
cantfrag	0
badopti ons	0
noroute	0
badvers	0
rawout	0
tool ong	0
notmember	0
nogi f	0
badaddr	0
acl -deni al s	1233
l ast-srci p-denied	174. 35. 60. 72

ACMEPACKET#

Phy Link Redundancy

If you have two two-port GigE cards installed in your Net-Net SBC, you can configure them for phy link redundancy. This feature requires that two-port GigE cards be installed in both slots of your Net-Net SBC.

In this redundancy scheme, port 0 on slots 0 and 1 is the master port and port 1 is the backup port. The card receives and sends all traffic on one port, while the other acts as a standby in the event of failure. In this way, the two-port GigE card behaves as though it were a single-port card by only using one port as an active at one time.

Viewing phy link redundancy information tells you which ports are active on which cards, and how many switchover events have occurred.

Viewing Redundancy Link Information

Using the **show redundancy link** command, you can see information about the redundancy link, including which ports are active and what the link status is for each port.

To view redundancy link information:

1. In either User or Superuser mode, type **show redundancy link** and press <Enter>. A display similar to the one below will appear.

ACMEPACKET# **show redundancy l l nk**

```
Active port on Slot 0 is port:    0
Slot 0 Switchover Events:       0

Active port on Slot 1 is port:    0
Slot 1 Switchover Events:       0
```

Wancom Port Speed and Duplex Mode Display

You can display the negotiated duplex mode and speed for all Net-Net system control ports by using the ACLI **show wancom** command. This command allows you to diagnose network issues more efficiently.

When you use this command, the systems shows information for all three control ports with the numbers starting at 0. It will then tell you the negotiated duplex mode and speed, or that the link is down.

To display negotiated duplex mode and speed for control interfaces:

1. At the user prompt, type the ACLI **show wancom** command and press <Enter>.

```
ACMEPACKET> show wancom
wancom [unit number 0]:
    Duplex Mode: half
    Speed: 100 Mbps
wancom [unit number 1]:
    Link down
wancom [unit number 2]:
    Link down
```

Application Faults

This section contains information about application fault statistics. This category of alarm accounts for problems related to applications (protocols).

- H.323
- SIP
- MGCP
- RADIUS

Application alarms do not display an alarm message in the graphic display window on the front panel of the Net-Net chassis.

H.323 Statistics

You can use the following command to display H.323 statistics:

- **show h323d**

There is also an alarm that occurs when stack initialization fails.

Viewing H.323 Statistics

Display H.323 statistics by using the **show h323d** command.

For example:

```
acmepacket# show h323d
```

```
18: 32: 26-86
```

```
Session Stats
```

```
-- Period --  ----- Li fetime -----
Active  High  Total      Total  PerMax  High
```


Incoming Calls	5	5	1	18	6	5
Outgoing Calls	1	1	1	18	6	2
Connected Calls	1	1	1	8	2	1
Incoming Channels	2	2	2	17	4	2
Outgoing Channels	2	2	2	17	4	2
Contexts	5	5	1	18	6	5

H323D Status	Current	Lifetime
Queued Messages	1	1608
TPKT Channels	5	404
UDP Channels	0	0

Stack	State	Type	Mode	Registered	Gatekeeper
h323172	enabled	H323	Gateway	No	

In the first display section, the following statistics are displayed for period and lifetime durations in addition to an active count.

- Incoming Calls—Number of incoming H.323 calls.
- Outgoing Calls—Number of outgoing H.323 calls.
- Connected Calls—Number of currently connected H.323 calls.
- Incoming Channels—Number of established incoming channels.
- Outgoing Channels—Number of established outgoing channels.
- Contexts—Number of established H.323 contexts.

In the second section, the following statistics are displayed for current and lifetime durations.

- Queued Messages—Number of messages queued.
- TPKT Channels—Number of TPKT channels open(ed).
- UDP Channels—Number of UDP channels open(ed).

H.323 Stack Initialization Failure Alarm

The following table provides information about the H.323 ALARM STACK INITIALIZATION FAILURE application alarm, which is triggered by the failure of an H.323 stack to initialize properly.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
H.323 ALARM STACK INITIALIZATION FAILURE	327682	CRITICAL	The H.323 stack has failed to initialize properly and is terminated.	[H.323 IWF] stack <stack-name> has failed to initialize and is terminated	<ul style="list-style-type: none"> • apSyslogMessageGenerated trap generated • critical dry contact • syslog

H.323 Monitoring Stack Alarm

- Viewing the number of active calls—You can see the number of active calls using the **show h323 stack call** command at either the User or Superuser prompt. You can also access this information with an SNMP query.
- Viewing alarm information—Two ACLI commands allow you to view alarm information, but they provide different information:

- **display-alarms**—This command shows alarm the most recently generated by an H.323 stack and the total number of stack monitoring alarms the Net-Net SBC has generated. Since alarms can fire simultaneously, the alarm you can see using this command will only be the most recent one.

ACMEPACKET# **display-alarms**

1 alarms to show

ID	Task	Severity	First Occurred	Last Occurred
327694	462796192	3	2009-06-03 18:51:46	2009-10-03 18:51:46

Count Description

2 current calls are over critical threshold of 50 percent. Total no of h323 stack alarm generated are 2

- **show h323 stack stack-alarms**—This command refers to specific stacks by stack name, and provides shows the alarm severity and the current percentage of max-calls that triggered the alarm. The Net-Net SBC keeps track of how many alarms are raised by each stacks, and the severity of each of those alarms. When the alarm clears, the information relating to it is erased from the display.

ACMEPACKET# **show h323 stack stack-alarms**

Stack-Name	Alarm-Severity	%Max-Call
external	minor	50
internal	critical	50

MGCP Statistics

You can use the following show commands to display MGCP statistics:

- **show algd errors**
- **show processes algd**

There is also an alarm generated when a DNS failure occurs.

Viewing MGCP Errors

Display MGCP error statistics by using the **show algd errors** command. For example:

acmepacket# **show algd error**

18:33:06-186

MGCP Media Events	---- Lifetime ----		
	Recent	Total	PerMax
Calling SDP Errors	0	0	0
Called SDP Errors	0	0	0
Drop Media Errors	0	0	0
Transaction Errors	0	0	0
Application Errors	0	0	0
Media Exp Events	0	0	0
Early Media Exps	0	0	0
Exp Media Drops	0	0	0

Viewing MGCP Processes

Display MGCP process statistics by using the **show processes algd** command. For example:

```
ACMEPACKET# show processes algd
```

```
11: 31: 39-140 (algd) ID=1b69e570
```

```

Process Status      -- Period -- ----- Li f e t i m e -----
                        Act i v e   Hi gh   Total       Total   PerMax   Hi gh
Services             5       5       0           6       6       5
Messages             0       0       0           2       2       2
Transactions         0       0       0           0       0       0
Timed Objects        7       7       0          17      17      10
Total Buffers        10      10       0          10      10      10
Alloc Buffers         5       5       0           7       7       7
Memory Chunks        47      47       0          81      81      49
TOQ Entries          1       1       1        5306      10       2
Operations
Messages Received
Messages Sent
Partial Message
Partial Msg Expired
Partial Msg Dropped
Timed Events
Alarms
System Logs
Process Logs
Load Rate
CPU Usage

```

MGCP DNS Failure Alarm

The following table lists information about the MGCP DNS failure alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MGCP ALARM DNS FAILURE	327683	WARNING	Cannot authenticate the RSIP and need to drop the packet.	Endpoint <endpoint> from source <sourceHostname> could not be authenticated.	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated critical dry contact syslog

MGCP Congestion Control Information

The MGCP congestion control feature is designed to help customers handle large call events in an oversubscribed environment. When you enable this feature, the Net-Net SBC can send a system busy message back to the call agent for new calls when system resources have been exhausted.

If the Net-Net SBC's CPU utilization equals or exceeds the threshold you configure, the Net-Net SBC will reject calls (off-hook NTFY messages) by sending 403 messages. The "off-hook message" is the only message that the Net-Net SBC rejects with a 403 message. And the Net-Net SBC resends 403 Intermediary Failure messages for subsequent retransmissions of calls that the Net-Net SBC has already

rejected. CRCX and RSIP messages are not rejected, but instead are handled the same way they were prior to the implementation of MGCP congestion control. In addition, the Net-Net SBC tracks the number of NTFY Overload 403 Sent messages, which you can view using the ACLI **show algd NTFY** command.

To view the number of NTFY Overload 403 Sent messages sent:

1. At the command line, type **show algd ntly** and press <Enter>.

```
ACMEPACKET# show algd ntly
```

MGCP Endpoint Inactivity

The Net-Net SBC maintains a per-endpoint timer to track when traffic was last received from the gateway. If the timer expires, the Net-Net SBC deletes the endpoint and frees its resources. If all endpoints associated with a gateway are deleted, then the Net-Net SBC removes the gateway entry, too.

You can monitor the value of the timers assigned to endpoints by using the new ACLI **show algd mgcp-endpoints-inactivity-timer** command. If you want to see the timer assigned to a specific endpoint, you can enter this command with the endpoint's FQDN.

SIP Statistics

You can use the following commands to view SIP statistics:

- **show sipd errors**
- **show processes sipd**
- **show registration**

Viewing SIP Errors

Display SIP error statistics by using the **show sipd errors** command. For example:

```
ACMEPACKET# show sipd errors
```

```
11:34:13-194
```

SIP Errors/Events	---- Lifetime ----		
	Recent	Total	PerMax
SDP Offer Errors	0	0	0
SDP Answer Errors	0	0	0
Drop Media Errors	0	0	0
Transaction Errors	0	0	0
Application Errors	0	0	0
Media Exp Events	0	0	0
Early Media Exps	0	0	0
Exp Media Drops	0	0	0
Expired Sessions	0	0	0
Multiple OK Drops	0	0	0
Multiple OK Terms	0	0	0
Media Failure Drops	0	0	0
Non-ACK 2xx Drops	0	0	0
Invalid Requests	0	0	0
Invalid Responses	0	0	0
Invalid Messages	0	0	0
CAC Session Drop	0	0	0

CAC	BW	Drop	0	0	0
-----	----	------	---	---	---

Display statistics about SIP processes by using the **show processes sipd** command. For example:

```

ACMEPACKET# show processes sipd
11: 34: 49-130 (sipd) ID=1b89dfd0
Process Status      -- Period --      ----- Lifetime -----
                   Active   High   Total           Total   PerMax   High
Services            5       5       0              5       5       5
Messages            0       0       0              6       4       3
Transactions        0       0       0              0       0       0
Timed Objects       7       7       0             14      11       9
Total Buffers       5       5       0              5       5       5
Alloc Buffers       3       3       0              7       4       5
Memory Chunks      48      48       0             82      79      50
TOQ Entries         2       2      14            58301    19       4
Operations          14            52997      12
Messages Received           0           3       2
Messages Sent             4          17681    30
Partial Message           0           0       0
Partial Msg Expired       0           0       0
Partial Msg Dropped       0           0       0
Timed Events            14          58291    12
Alarms                  0           0       0
System Logs             4          17681    32
Process Logs            4          17684    35
Load Rate              0.0                0.0
CPU Usage              0.0                8.133/529935

```

Viewing IP Session Replication for Recording (SRR) Information

The **show call-recording-server** command displays information regarding the IP call recording feature configured on the Net-Net SBC. Entering this command without the optional call recording server (CRS) ID displays all CRS endpoints configured on the Net-Net SBC along with their state.

You can specify a CRS whose information you want to view. When you specify an ID, the ACLI displays all session agents created for the CRS endpoint, its IP address, its state, and the last time a failover occurred. For example:

Viewing SIP Registration Cache Status

Display SIP registration cache status by using the **show registration** command. The display shows statistics for the Period and Lifetime monitoring spans.

- **Cached Entries**—Number of registration entries for the address of record
- **Local Entries**—Number of entries for Contact messages sent to a real registrar.
- **Forwards**—Number of registration requests forwarded to the real registrar
- **Refreshes**—Number of registrations the Net-Net SBC answered without having to forward registrations to the real registrar
- **Rejects**—Number of unsuccessful registrations sent to real registrar
- **Timeouts**—Number of times a refresh from the HNT endpoint was not received before the timeout

For example:

ACMEPACKET# **show registration**

11:38:57-177

SIP Registrations	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
User Entries	0	0	0	0	0	0
Local Contacts	0	0	0	0	0	0
Via Entries	0	0	0	0	0	0
AURI Entries	0	0	0	0	0	0
Free Map Ports	0	0	0	0	0	0
Used Map Ports	0	0	0	0	0	0
Forwards	-	-	0	0	0	
Refreshes	-	-	0	0	0	
Rejects	-	-	0	0	0	
Timeouts	-	-	0	0	0	
Fwd Postponed	-	-	0	0	0	
Fwd Rejected	-	-	0	0	0	
Refr Extension	0	0	0	0	0	0
Refresh Extended	-	-	0	0	0	
Surrogate Regs	0	0	0	0	0	0
Surrogate Sent	-	-	0	0	0	
Surrogate Reject	-	-	0	0	0	
Surrogate Timeout	-	-	0	0	0	
HNT Entries	0	0	0	0	0	0
Non-HNT Entries	0	0	0	0	0	0

SIP NSEP Statistics

To view statistics related to the NSEP feature, the ACLI **show** command has been expanded. It now allows you to see all of the statistics for NSEP support, to see them for a specific r-value (namespace and r-priority combination), or to see all of these. You can also reset the NSEP statistics counters.

When you use the ACLI **show nsep-stats** command without further arguments, the system shows you information for inbound sessions.

To display general NSEP statistics for inbound sessions:

1. Type **show nsep-stats** and press <Enter>.

ACMEPACKET# **show nsep-stats**

	----- Lifetime -----		
	Current	Total	PerMax
Inbound Sessions	0	0	0

NSEP Statistics per R-Value Display

You can see statistics for specific r-value by entering it with the **show nsep-stats** command. An r-value is a namespace and priority combination entered in the following format: namespace. priority. The display will also show the specified r-value for which it is displaying data.

To display general NSEP statistics for specific r-values:

1. Type **show nsep-stats**, a <Space>, and then the r-value for which you want to display statistics. Then press <Enter>.

ACMEPACKET# **show nsep-stats ets.2**

RValue = ets.2

	-- Period --			----- Li f e t i m e -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Incomi ng Sessi ons	0	0	0	0	0	0
Outgoi ng Sessi ons	0	0	0	0	0	0
InbSessi ons Rej	-	-	0	0	0	-
OutbSessi ons Rej	-	-	0	0	0	-

You can see the full set of statistics for NSEP inbound sessions and for all r-values by using the **show nsep-stats all** command. The display for r-values is divided into individual sections for each r-value shown.

To display general NSEP statistics for specific r-values:

1. Type **show nsep-stats all** and press <Enter>.

```
ACMEPACKET# show nsep-stats all
```

```
Session Stats
```

	----- Li f e t i m e -----		
	Current	Total	PerMax
Inbound Sessions	0	0	0
Per RValue Stats			

	-- Period --			----- Li f e t i m e -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
RValue = ets. 2						
Incomi ng Sessi ons	0	0	0	0	0	0
Outgoi ng Sessi ons	0	0	0	0	0	0
InbSessi ons Rej	-	-	0	0	0	-
OutbSessi ons Rej	-	-	0	0	0	-

RValue = ets. 5						
Incomi ng Sessi ons	0	0	0	0	0	0
Outgoi ng Sessi ons	0	0	0	0	0	0
InbSessi ons Rej	-	-	0	0	0	-
OutbSessi ons Rej	-	-	0	0	0	-

Viewing NSEP Burst Statistics for SIP Session Agents

The ACLI **show sipd** command supports an **sa-nsep-burst** argument that displays the NSEP burst rate for all SIP session agents.

```
ACMEPACKET# show sipd sa-nsep-burst
```

Agent	Current Rate	Li f e t i m e Hi gh
192. 168. 1. 139	0	0
192. 168. 1. 6	0	0
192. 168. 200. 135	4	10

Resetting NSEP Statistics

You can reset the statistics for incoming sessions, for an individual r-value, or for the entire set of NSEP data. You use the same command syntax as you do when showing the statistics, except that you start your entry with the **reset** command.

In the example below, the command resets the statistics counters for the specific r-value ets. 2.

To reset the counters for a specific r-value:

1. For the set of statistics you want to reset, type **reset nsep-stats** and then the group that you want to reset. The press <Enter>.

ACMEPACKET# **reset nsep-stats ets.2**

To reset the counters for all NSEP statistics:

1. For the set of statistics you want to reset, type **reset nsep-stats** and then press <Enter>.

ACMEPACKET# **reset nsep-stats**

Viewing SIP Method Throttling Mechanism Statistics

You can monitor the SIP method throttling mechanism statistics for either a specific SIP interface or a session agent.

To display SIP method throttling mechanism statistics for a SIP interface:

1. Type **show sipd interface**, a <Space>, and then the SIP interface's name and the SIP method name for which you want statistics. Then press <Enter>.

ACMEPACKET# **show sipd interface net1 NOTI FY**

NOTI FY (15: 53: 42-57)

Message/Event	----- Server -----			----- Client -----		
	Recent	Total	PerMax	Recent	Total	PerMax
NOTI FY Requests	0	49	19	0	0	0
Retransmi ssi ons	0	0	0	0	0	0
100 Tryi ng	0	49	19	0	0	0
180 Ri ngi ng	0	38	19	0	0	0
200 OK	0	38	19	0	0	0
503 Servi ce Unavai l	0	11	11	0	0	0
Response Retrans	0	9	5	0	0	0
Transacti on Timeouts	-	-	-	0	0	0
Local l y Thrott l ed	-	-	-	0	0	0

Avg Latency=0.000 for 0

Max Latency=0.000

BurstRate Incomi ng=11 Outgoi ng=0

To display SIP method throttling mechanism statistics for a session agent:

1. Type **show sipd agents**, a <Space>, and then the session agent IP address and the SIP method name for which you want statistics. Then press <Enter>.

ACMEPACKET# **show sipd agents 198.167.1.60 NOTI FY**

NOTI FY (15: 53: 34-49)

Message/Event	----- Server -----			----- Client -----		
	Recent	Total	PerMax	Recent	Total	PerMax
NOTI FY Requests	0	50	31	0	0	0
Retransmi ssi ons	0	3	3	0	0	0
200 OK	0	25	18	0	0	0
503 Servi ce Unavai l	0	25	24	0	0	0
Transacti on Timeouts	-	-	-	0	0	0
Local l y Thrott l ed	-	-	-	0	24	24

Avg Latency=0.000 for 0

Max Latency=0.000

BurstRate Incoming=5 Outgoing=0

Viewing SIP IP CAC Statistics

You can display CAC parameters for an IP address using the **show sipd ip-cac** command. For example:

```
ACMEPACKET# show sipd sessions ipcac
09: 21: 22-164
SIP Session Status      -- Period -- ----- Lifetime -----
                        Active  High  Total      Total  PerMax  High
Sessions                2      2      4          6      2      2
  Initial               0      2      4          6      2      2
  Early                 0      2      4          6      2      2
  Established           2      2      4          6      2      2
  Terminated           0      2      2          4      2      2
Dialogs                 4      4      8         12      4      4
  Early                 0      4      8         12      4      4
  Confirmed             4      4      8         12      4      4
  Terminated           0      4      4          8      4      4
```

Viewing SIP PUBLISH Statistics

You can display statistics related to incoming SIP PUBLISH messages using the **show sipd publish** command. For example:

```
ACMEPACKET# show sipd sessions publish
09: 23: 06-167
SIP Session Status      -- Period -- ----- Lifetime -----
                        Active  High  Total      Total  PerMax  High
Sessions                2      2      2          6      2      2
  Initial               0      2      2          6      2      2
  Early                 0      2      2          6      2      2
  Established           2      2      2          6      2      2
  Terminated           0      2      0          4      2      2
Dialogs                 4      4      4         12      4      4
  Early                 0      4      4         12      4      4
  Confirmed             4      4      4         12      4      4
  Terminated           0      4      0          8      4      4
```

RADIUS Statistics

The ACLI **show radius** command, used with the three arguments described in this section, displays the status of any established RADIUS accounting connections and authentications. A working RADIUS connection displays **READY**, and a disabled connection displays **DISABLED**.

There is also an alarm that occurs when the RADIUS connection is down.

Viewing RADIUS Statistics

The **show radius** command can take one of the three available arguments:

- authentication—Shows authentication statistics for primary and secondary RADIUS servers, including: server IP address and port; round trip time; information about failed and successful requests/authentications; number of rejections; number of challenges; number of time-outs, number of retransmissions

- accounting—Shows the information described in the following table:

Section	Description
Client Display	General accounting setup (as established in the accounting configuration element), including: <ul style="list-style-type: none"> • Information about the state of the RADIUS client • Accounting strategy used (Hunt, Failover, RoundRobin, FastestRTT, or FewestPending) • IP address and port on which the Net-Net server is listening • Maximum message delay in seconds • Number of configured accounting servers
Waiting Queue	Amount of accounting (RADIUS) messages waiting to be sent. Waiting queue capacity is 4,096 messages.
<IP Address:Port>	Information about each configured accounting server (established in the accounting servers configuration). The heading above each accounting server section is the IPv4 address and port combination of the accounting server described. This section also includes information about the accounting server's state (e.g., Connect_Attempt, I N I T).

- all—Shows all of the information for both the authentication and accounting displays

The following is an example of the ACLI **show radius authentication** command output.

```
ACMEPACKET# show radius authentication
```

```
Active Primary Authentication Servers:
```

```
server ipAddr: 172.30.0.7
```

```
Active Secondary Authentication Servers:
```

```
server ipAddr: 172.30.0.8
```

```
Authentication Statistics:
```

```
Server: "172.30.0.7:1812"
```

```
RoundTripTime           : 0
MalformedAccessResponse: 0
AccessRequests           : 2
BadAuthenticators        : 0
AccessRetransmissions   : 5
AccessAccepts            : 0
Timeouts                 : 6
AccessRejects            : 0
UnknownPDUTypes          : 0
AccessChallenges         : 0
```

```
Server: "172.30.0.8:1812"
```

```
RoundTripTime           : 0
MalformedAccessResponse: 0
AccessRequests           : 2
BadAuthenticators        : 0
AccessRetransmissions   : 9
AccessAccepts            : 0
Timeouts                 : 10
AccessRejects            : 0
```

```
UnknownPDUTypes      : 0
AccessChallenges     : 0
```

The following is an example of the ACLI **show radius accounting** command output.

```
ACMEPACKET# show radius accounting
*****Client Display Start*****
Client State = READY, strategy=Hunt
Listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2

===== Waiting Queue =====
Waiting size = 89

=====
----- 10.0.0.189:1813 -----
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582,
Restart delay=30 s
----- 192.168.200.70:5050 -----
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569,
Restart delay=30 s
*****Client Display End*****
```

The following is an example of the ACLI **show radius all** command output.

```
ACMEPACKET# show radius all
*****Client Display Start*****
Client State = READY, strategy=Hunt
Listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2

===== Waiting Queue =====
Waiting size = 89

=====
----- 10.0.0.189:1813 -----
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582,
Restart delay=30 s
----- 192.168.200.70:5050 -----
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569,
Restart delay=30 s
*****Client Display End*****
```

```
Active Primary Authentication Servers:
server ipAddr: 172.30.0.7
```

```
Active Secondary Authentication Servers:
server ipAddr: 172.30.0.8
```

```
Authentication Statistics:
Server: "172.30.0.7:1812"
RoundTripTime           : 0
```

```

Mal formedAccessResponse: 0
AccessRequests           : 2
BadAuthenti cators       : 0
AccessRetransmi ssions   : 5
AccessAccepts            : 0
Ti meouts                 : 6
AccessRej ects            : 0
UnknownPDUTypes          : 0
AccessChal lenges        : 0

```

Server: "172. 30. 0. 8: 1812"

```

RoundTri pTi me          : 0
Mal formedAccessResponse: 0
AccessRequests           : 2
BadAuthenti cators       : 0
AccessRetransmi ssions   : 9
AccessAccepts            : 0
Ti meouts                 : 10
AccessRej ects            : 0
UnknownPDUTypes          : 0
AccessChal lenges        : 0

```

RADIUS Connection Down Alarm

The following table lists the alarm generated when the RADIUS accounting connection is down.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
RADIUS ACCOUNTING CONNECTION DOWN	327681	CRITICAL: if all enabled and configured Remote Authentication Dial-in User Service (RADIUS) accounting server connections have timed-out without response from the RADIUS server MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server.	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost! Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost! Check accounting status for more details.	<ul style="list-style-type: none"> apSyslogMessageGenerated trap generated apSysMgmtRadiusDownTrap trap generated syslog

Security Breach Statistics

You can view statistics about denied ACL entries by using the following commands:

- **acl-show**
- **show acl**

Viewing List of Denied ACL Entries

Display a list of denied ACL entries by using the **acl-show** command. If a IP address and realm ID is denied of service, its is added to the deny list. This command shows list of deny ACL entries. Information for each entry includes:

- Incoming port, slot, and VLAN tag
- Source IP, bit mask, port, and port mask
- Destination IP address and port
- Protocol
- ACL entry as static or dynamic
- ACL entry index

For example:

```
ACMEPACKET# acl -show
```

deny entries:

```
intf: vl an source-ip/mask: port/mask dest-ip/mask: port/mask  prot type
index
```

Total number of deny entries = 0

Denied Entries not allocated due to ACL constraints: 0

task done

Viewing ACL List Entries

Display entries in the deny, untrusted, and trusted lists using the **show acl** command.

- **show acl denied**
- **show acl untrusted**
- **show acl trusted**
- **show acl all**
- **show acl ip**

For example:

```
ACMEPACKET# show acl denied
```

deny entries:

```
intf: vl an source-ip/mask: port/mask dest-ip/mask: port/mask  prot type
index
```

Total number of deny entries = 0

Denied Entries not allocated due to ACL constraints: 0

task done

```
ACMEPACKET# show acl untrusted
```

untrusted entries:

```
intf: vl an source-ip/mask: port/mask dest-ip/mask: port/mask  prot type
index
```

Total number of untrusted entries = 0

Untrusted Entries not allocated due to ACL constraints: 0

task done

ACMEPACKET# **show acl trusted**

trusted entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
recvd					drop

recvd drop

Total number of trusted entries = 0

Trusted Entries not allocated due to ACL constraints: 0

task done

ACMEPACKET# **show acl all**

deny entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
-------	------------	---------------------------	-------------------------	------	------

Total number of deny entries = 0

trusted entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
recvd					drop

recvd drop

Total number of trusted entries = 0

untrusted entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
-------	------------	---------------------------	-------------------------	------	------

Total number of untrusted entries = 0

total deny entries: 0 (0 dropped)

total media entries: 0

total trusted entries: 0 (0 dropped)

total untrusted entries: 0 (0 dropped)

task done

Viewing ACL List Entries by IP Address

You can filter the output of **show acl all** based on IP address. For example:

ACMEPACKET# **show acl ip 192.168.69.65**

deny entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
-------	------------	---------------------------	-------------------------	------	------

index

Total number of deny entries = 0

trusted entries:

index	intf: vlan	source-ip/mask: port/mask	dest-ip/mask: port/mask	prot	type
recvd					drop

recvd drop

Total number of trusted entries = 0

untrusted entries:

```
intf: vlan source-ip/mask: port/mask dest-ip/mask: port/mask  prot type
index
```

Total number of untrusted entries = 0

Viewing ACL Entry Space in the CAM

Display how much space is used in the CAM for ACL entries, in a percentage and raw value breakdown of the use, by using the `show acl info` command. For example:

```
ACMEPACKET# show acl info
```

Access Control List Statistics:

	# of entries	% utilization	Reserved Entry Count
Denied	0	0.0%	200
Trusted	0	0.0%	200
Media	0	0.0%	3884
Untrusted	0	0.0%	100

Total CAM space used = 0 of 7768 (100.00% free)

```
Media Entries not allocated due to ACL constraints: 0
Trusted Entries not allocated due to ACL constraints: 0
Untrusted Entries not allocated due to ACL constraints: 0
Denied Entries not allocated due to ACL constraints: 0
```

Session Agent and Session Agent Group Faults

This section explains how to view fault information about SIP and H.323 session agents and session agent groups.

SIP Agent Statistics

You can use the following commands to view SIP agent statistics:

- `show sipd agents`
- `show sipd <agent ID>`

Viewing SIP Session Agent Statistics

Display SIP session agent information by using the `show sipd agents` command. With this command, the Net-Net SBC ascertains whether a session agent is in service. When the session agent stops responding to SIP requests, it transitions to the out-of-service state. You can configure the Net-Net SBC to periodically *ping* the session agent if it has gone out-of-service, or if no requests have been sent to it.

The `show sipd agents` command shows information about the number of active sessions, the average rate of session invitations, and the number of times that the constraints established in the session-agent element have been exceeded for sessions inbound to and outbound from each session agent, as well as the average and maximum latency and the maximum burst rate related to each session agent.

For example:

```
ACMEPACKET# show sipd agents
```

```

19: 39: 34-95
----- Inbound ----- Outbound ----- Latency -- Max -----
Session Agent Active Rate ConEx Active Rate ConEx Avg Max Burst InBurst OutBurst
192.168.200.131 I 0 0.0 0 0 0.0 0 0.000 0.000 0 0 0

```

Inbound statistics:

- Active: number of active sessions sent to each session agent listed
- Rate: average rate of session invitations (per second) sent to each session agent listed
- ConEx: number of times the constraints have been exceeded

Outbound statistics:

- Active: number of active sessions sent from each session agent
- Rate: average rate of session invitations (per second) sent from each session agent listed
- ConEx: number of times the constraints have been exceeded

Latency statistics:

- Avg: average latency for packets traveling to and from each session agent listed
- Max: maximum latency for packets traveling to and from each session agent listed
- Max Burst: total number of session invitations sent to or received from the session agent within the amount of time configured for the burst rate window of the session agent

The second column, which is not labeled, of the **show sipd agents** output shows the service state of each session agent identified in the first column. In the service state column, an *I* indicates that the particular session agent is in service and an *O* indicates that the particular session agent is out of service. An *S* indicates that the session agent is transitioning from the out-of-service state to the in-service state; it remains in this transitional state for a period of time that is equal to its configured in-service period, or 100 milliseconds (whichever is greater). A *D* indicates that the session agent is disabled.

Resetting Session Agent Statistics

Reset a specific session agent's statistics by using the **reset session-agent <hostname>** command.

For example:

```

ACMEPACKET# reset session-agent agent2
Accepted
Reset SA failover timer

```

Viewing SIP Session Agent Activity

Display a specific session agent's activity by using the **show sipd <agent ID>** command.

For example:

```

acmepacket# show sipd agent 69.69.69.22
19: 32: 17-47
Session Agent 172.16.0.10(sip172) [In Service]
-- Period -- Lifetime -----
Active High Total Total PerMax High

```


Inbound Sessions	0	0	0	234666	92	168
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Reg Rate Exceeded	-	-	0	0	0	-
Outbound Sessions	0	0	0	239762	126	200
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Reg Rate Exceeded	-	-	0	0	0	-
Out of Service	-	-	0	0	0	-
Trans Timeout	40928	40928	400	40928	800	40928
Requests Sent	-	-	400	519695	780	-
Requests Complete	-	-	0	478367	574	-
Seizure	-	-	0	239762	126	-
Answer	-	-	0	234661	93	-
ASR Exceeded	-	-	0	0	0	-
Messages Received	-	-	0	1431343	1415	-
Latency=0.000; max=0.000						

Inbound sessions:

- Rate Exceeded: number of times session or burst rate was exceeded for inbound sessions
- Num Exceeded: number of times time constraints were exceeded for inbound sessions

Outbound sessions:

- Rate Exceeded: number of times session or burst rate was exceeded for outbound sessions
- Num Exceeded: number of times time constraints were exceeded for inbound sessions
- Burst: number of times burst rate was exceeded for this session agent
- Out of Service: number of times this session agent went out of service
- Trans Timeout: number of transactions timed out for this session agent
- Requests Sent: number of requests sent via this session agent
- Requests Complete: number of requests that have been completed for this session agent
- Messages Received: number of messages received by this session agent

SIP Session Agent Group Statistics

You can use the following commands to display SIP agent group statistics:

- `show sipd groups`
- `show sipd groups -v`
- `show sipd groups <group name>`

Viewing Session Agent Group Statistics

Display session information for the session agent groups on the Net-Net system by using the `show sipd groups` command. This information is compiled by totaling the

session agent statistics for all of the session agents that make up a particular session agent group.

The Active column of the session agent group statistics output displays the first character of the session agent group state. The session agent group statistics can be in one of the following states.

- D—Disabled
- O—Out Of Service
- S—Standby
- I—In Service
- C—Constraints Exceeded
- N—No Response Timeout
- O—OOS Provisioned Response
- R—Reduction In Call Load

While the **show sipd groups** command accesses the subcommands that are described in this section, the main **show sipd groups** command (when executed with no arguments) displays a list of all session agent groups for the Net-Net system.

For example:

```
ACMEPACKET# show sipd groups
11: 00: 21-16

----- Inbound -----  ---- Outbound ----- -- Latency --
SAG      Active Rate  ConEx Active Rate  ConEx   Avg   Max
recursi on    I    0  0.0    0     1  0.1    0 0.005 0.005  2
```

If you carry out this command, but you do not specify the name of an existing session agent group, the Net-Net system will inform you that the group statistics are not available.

Viewing List of SIP Session Agents in a Group

List the session agents that make up the session agent group, along with statistics for each by using the **show sipd groups -v** command. The -v (verbose) option must be included with this command to provide this level of detail.

For example:

```
ACMEPACKET# show sipd groups -v
SAG:
11: 00: 07-32

----- Inbound -----  ---- Outbound ----- -- Latency --
Sessi on Agent Active Rate  ConEx Active Rate  ConEx   Avg   Max
150. 150. 150. 16 I    0  0.0    0     0  0.0    0 0.005 0.005  1
SAG:
150. 150. 150. 35 I    0  0.0    0     1  0.0    0 0.000 0.000  1

Total s:
recursi on    I    0  0.0    0     1  0.8    0 0.005 0.005  2
```

Viewing Statistics for a SIP Session Agent

Display statistics for a specific session agent group by using the **show sipd groups <group name>** command.

For example:

ACMEPACKET# **show sipd groups recursion**

11:00:28-23

	----- Inbound -----			----- Outbound -----			-- Latency --	
SAG	Active	Rate	ConEx	Active	Rate	ConEx	Avg	Max
recursion	1	0	0.0	0	0.0	0	0.005	0.005 2

Session Agent and Session Router Constraint Statistics

Net-Net SBC's support for session constraints is applicable not only to the system when configured for dialog-stateful or for session-stateful mode, but also when it operates in proxy (transaction or stateless) mode.

Notes on Statistics

When it runs in transaction mode, the Net-Net SBC counts INVITE transactions for calculating session agent statistics that are used to apply session agent constraints. The following describes how the Net-Net SBC performs its count:

- For calculating the **max-burst-rate** and the **max-inbound-burst-rate**, the Net-Net SBC counts the server transaction created when it receives an INVITE request.
- For calculating the **max-outbound-burst-rate**, the Net-Net SBC counts the client transaction when it sends an INVITE request to a session agent.
- The Net-Net SBC counts each INVITE transaction, except for in-dialog re-INVITE transactions. It detects in-dialog re-INVITE requests by checking the To tag.
- The Net-Net SBC does not count retransmitted INVITE requests, which it can detect.

Example 1: Statistics from Transaction Mode

This section shows sample output from the ACLI **show sipd agents** command. The sections that do not apply to transaction mode appear in *italics*.

ACMEPACKET# **show sipd agents acme5**

11:08:18-46

Session Agent acme5(private) [In Service]

	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Inbound Sessions	22	22	22	22	22	22
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Burst Rate	0	19	0	0	0	19
<i>Reg Rate Exceeded</i>	-	-	0	0	0	-
Outbound Sessions	0	0	0	0	0	0
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Burst Rate	0	0	0	0	0	0
<i>Reg Rate Exceeded</i>	-	-	0	0	0	-
Out of Service	-	-	0	0	0	-
Trans Timeout	0	0	0	0	0	0
Requests Sent	-	-	0	0	0	-
Requests Complete	-	-	0	0	0	-
<i>Seizure</i>	-	-	0	0	0	-
<i>Answer</i>	-	-	0	0	0	-
<i>ASR Exceeded</i>	-	-	0	0	0	-
Messages Received	-	-	65	65	65	-

Latency=0.000; max=0.000

Example 1: Statistics from Stateless Mode

This section shows sample output from the ACLI **show sipd agents** command. The sections that do not apply to stateless mode appear in italics.

```
acmesystem# show sipd agents uni
12: 11: 17-51
Session Agent uni (public) [In Service]

-- Period -- ----- Lifetime -----
Active High Total Total PerMax High
Inbound Sessions 0 0 0 0 0 0
Rate Exceeded - - 0 0 0 -
Num Exceeded - - 0 0 0 -
Burst Rate 0 0 0 0 0 0
Reg Rate Exceeded - - 0 0 0 -
Outbound Sessions 0 1 11 11 11 1
Rate Exceeded - - 0 0 0 -
Num Exceeded - - 0 0 0 -
Burst Rate 0 11 0 0 0 11
Reg Rate Exceeded - - 0 0 0 -
Out of Service - - 0 0 0 -
Trans Timeout 0 0 0 0 0 0
Requests Sent - - 0 0 0 -
Requests Complete - - 0 0 0 -
Seizure - - 0 0 0 -
Answer - - 0 0 0 -
ASR Exceeded - - 0 0 0 -
Messages Received - - 30 30 30 -
Latency=0.000; max=0.000
```

H.323 Session Agent Statistics

Display H.323 session agent information by using the following commands:

- **show h323d agentlist**
- **show h323d agentconfig**
- **show h323d agentstats**

Viewing H.323 Session Agent List

Display a list of session agents by using the **show h323d agentlist** command. For example:

```
ACMEPACKET# show h323d agentlist
H323-Session Agent List
hostname 192.168.200.20
hostname 192.168.200.30
hostname 10.10.10.3
```

Viewing Session Agent Configuration Statistics

Display information about the session agent configuration by using the **show h323d agentconfig** command. For example:

```
ACMEPACKET(session-agent)# show h323 agentconfig
session-agent
hostname testhostname.com
ip-address 192.168.200.13
```

port	5060
state	enabl ed
app-protocol	SI P
app-type	H323-GW
transport-method	UDP
real m-i d	h323192
descri pti on	
carri ers	
al low-next-hop-l p	enabl ed
constrai nts	di sabl ed
max-sessi ons	0
max-i nbound-sessi ons	4
max-outbound-sessi ons	5
max-burst-rate	0
max-i nbound-burst-rate	10
max-outbound-burst-rate	1
max-sustai n-rate	0
max-i nbound-sustai n-rate	0
max-outbound-sustai n-rate	0
mi n-sei zures	5
mi n-asr	0
ti me-to-resume	0
ttr-no-response	0
i n-servi ce-peri od	0
burst-rate-wi ndow	0
sustai n-rate-wi ndow	0
req-uri -carri er-mode	None
proxy-mode	Redi rect
redi rect-acti on	
l oose-routi ng	enabl ed
send-medi a-sessi on	enabl ed
response-map	
pi ng-method	
pi ng-i nterval	0
pi ng-i n-servi ce-response-codes	
out-servi ce-response-codes	
medi a-profi les	
i n-transl ati oni d	
out-transl ati oni d	
trust-me	di sabl ed
request-uri -headers	
stop-recurse	
l ocal -response-map	
pi ng-to-user-part	
pi ng-from-user-part	
l i -trust-me	di sabl ed
i n-mani pul ati oni d	
out-mani pul ati oni d	
p-asserted-i d	
trunk-group	
	tgname1: tgcontext1
	tgname2: tgcontext2
max-regi ster-sustai n-rate	0
early-medi a-al low	

```

invalid-date-registrations      disabled
rfc2833-mode                    none
rfc2833-payload                 0
codec-policy                    0
last-modified-date              2007-03-29 17:15:50
task done

```

Viewing H.323 Session Agent Statistics

Display statistics about the session agent by using the **show h323d agentstats** command. For example:

```

ACMEPACKET# show h323d agentstats
19:38:59-30
----- Inbound -----
Session Agent  Active Rate ConEx  Active Rate ConEx  Avg  Max Burst InBurst OutBurst
192.168.1.15   I    0  0.0  0    0  0.0  0  0.000 0.000 0  0  0
192.168.1.6    I    0  0.0  0    0  0.0  0  0.000 0.000 0  0  0

```

H.323 Session Agent Group Statistics

You can use the following commands to view H.323 session agent group statistics:

- **show h323d grouplist**
- **show h323d groupconfig**
- **show h323d groupstats**

Viewing List of H.323 Session Agent Groups

Display a list of session agent groups by using the **show h323d grouplist** command. For example:

```

ACMEPACKET# show h323d grouplist
H323-Session Agent Group List
group-name                h323
session-agent
hostname                  testhostname.com
ip-address
port                      5060
state                     enabled
app-protocol              SIP
app-type
transport-method          UDP
realm-id
description
carriers
allow-next-hop-ip         enabled
constraints                disabled
max-sessions              0
max-inbound-sessions      4
max-outbound-sessions     5
max-burst-rate            0
max-inbound-burst-rate    10
max-outbound-burst-rate   1
max-sustain-rate          0
max-inbound-sustain-rate  0
max-outbound-sustain-rate 0
min-seizures              5
min-asr                   0
time-to-resume            0
ttr-no-response           0
in-service-period         0
burst-rate-window         0
sustain-rate-window       0
req-uri-carrier-mode      None
proxy-mode

```

```

redirect-action
loose-routing          enabled
send-media-session    enabled
response-map
ping-method
ping-interval          0
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translated
out-translated
trust-me                disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me            disabled
in-manipulated
out-manipulated
p-asserted-id
trunk-group

                                tgname1: tgcontext1
                                tgname2: tgcontext2
max-register-sustain-rate 0
early-media-allow
invalid-date-registrations disabled
rfc2833-mode           none
rfc2833-payload         0
codec-policy
last-modified-date      2007-03-29 17:15:50

```

Viewing H.323 Session Agent Group Configuration Statistics

Display information about the session agent group configuration by using the **show h323d groupconfig** command. For example:

```

ACMEPACKET# show h323d groupconfig
session-group
  group-name              h323
  description
  state                   enabled
  app-protocol            H323
  strategy                Hunt
  dest
                                172.16.0.13
                                1.1.1.1
  trunk-group
  last-modified-date      2006-07-11 19:12:22

```

Viewing H.323 Session Agent Group Statistics

Display statistics about the session agent group by using the **show h323d groupstats** command. For example:

```

ACMEPACKET# show h323d groupstats
19:38:59-30
----- Inbound ----- Outbound ----- Latency -- Max -----
SAG      Active Rate ConEx Active Rate ConEx Avg Max Burst InBurst OutBurst
H323Group 1    0  0.0    0    0  0.0    0  0.000 0.000 0    0    0

```

Realm Faults

This section explains how to access realm fault statistics.

Signaling

Use the following command to display SIP realm statistics:

- **show sipd realms**

Viewing SIP Realm Statistics

Display SIP realm statistics by using the **show sipd realms** command. For example:

```
ACMEPACKET# show sipd realms
19: 38: 17-18
```

Realm	----- Inbound -----			---- Outbound ----			-- Latency --		----- Max -----		
	Active	Rate	ConEx	Active	Rate	ConEx	Avg	Max	Burst	InBurst	OutBurst
external	0	0.0	0	0	0.0	0	0.000	0.000	0	0	0
external-child	0	0.0	0	0	0.0	0	0.000	0.000	0	0	0
internal	0	0.0	0	0	0.0	0	0.000	0.000	0	0	0

Media Statistics

You can use the following commands to display information about mbcd realms:

- **show mbcd realms**
- **show mbcd realms <realm name>**
- **show flows**

There are also alarms that occur when the following events happen:

- out of memory
- internal
- unknown realm
- realm change
- out of bandwidth
- out of ports

Viewing MBCD Steering Port and Bandwidth Usage for Realms

Display steering ports and bandwidth usage for home, public, and private realms by using the **show mbcd realms** command.

For example:

```
acmepacket# show mbcd realms
18: 46: 29-2819
```

Realm	--- Steering Ports ---			----- Bandwidth Usage -----				
	Used	Free	No Ports	Flows	Ingrss	Egress	Total	Insuf BW
acme	0	0	0	0	OK	OK	OK	0
h323172	0	30001	0	0	OK	OK	OK	0
si p172	2	29999	0	0	OK	OK	OK	0
si p192	2	29999	0	0	OK	OK	OK	0

The information displayed includes the following:

- Used—Number of steering ports used
- Free—Number of free steering ports
- No Ports—Number of times that a steering port could not be allocated

- Flows—Number of established media flows
- Ingress—Amount of bandwidth being used for inbound flows
- Egress—Amount of bandwidth being used for outbound flows
- Total—Maximum bandwidth set for this realm
- Insuf BW—Number of times that a session was rejected due to insufficient bandwidth.

Viewing MBCD Statistics for a Specific Realm

Display media statistics for a specific realm by using the **show mbcd realms <realm-name>** command. This information is given for period and lifetime durations.

- Ports Used—Number of ports used
- Free Ports—Number of free ports
- No Ports Avail—Number of times no steering ports were available
- Ingress Band—Amount of bandwidth used for inbound flows
- Egress Band—Amount of bandwidth used for outbound flows
- BW Allocations—Number of times that bandwidth was allocated
- Band Not Avail—Number of times a session was rejected due to insufficient bandwidth

For example:

acmepacket# **show mbcd realms sip172**

18: 47: 31-2881 Realm=sip172

	-- Period --			Lifetime		
	Active	High	Total	Total	PerMax	High
Ports Used	2	2	18	18	18	2
Free Ports	29999	30001	30017	30017	30017	30001
No Ports Avail	-	-	0	0	0	-
Ingress Band	OK	OK	0	0	0	OK
Egress Band	OK	OK	0	0	0	OK
BW Allocations	0	0	0	0	0	0
Band Not Avail	-	-	0	0	0	-
Total Bandwidth=OK						

Steering Ports: 100% Success

Viewing MBCD Task Errors

The **show mbc d errors** command displays MBCD task error statistics, starting with a time stamp that shows when the current period began.

For example:

```
ACMEPACKET# show mbc d errors
11: 42: 37-198
MBC Errors/Events          ---- Li fetime ----
                          Recent      Total    PerMax
Client Errors              0          0        0
Client IPC Errors          0          0        0
Open Streams Failed        0          0        0
Drop Streams Failed        0          0        0
Exp Flow Events            0          0        0
Exp Flow Not Found         0          0        0
Transaction Timeouts       0          0        0

Server Errors              0          0        0
Server IPC Errors          0          0        0
Flow Add Failed            0          0        0
Flow Delete Failed         0          0        0
Flow Update Failed         0          0        0
Flow Latch Failed          0          0        0
Pending Flow Expired       0          0        0
ARP Wait Errors            0          0        0
Exp CAM Not Found          0          0        0
Drop Unknown Exp Flow      0          0        0
Drop/Exp Flow Missing      0          0        0
Exp Noti fy Failed         0          0        0
Unacknowledged Noti fy    0          0        0
Invalid Realm              0          0        0
No Ports Avail able        0          0        0
Insuffi cient Bandwi dth   0          0        0
Stale Ports Reclai med     0          0        0
Stale Flows Replaced       0          0        0
Telephone Events Gen       0          0        0
Pipe Alloc Errors          0          0        0
Pipe Write Errors          0          0        0
```

There are two categories of MBCD error statistics: Client and Server.

Client statistics count errors and events encountered by applications that use the MBCD to set up and tear down media sessions:

- Client Errors—Number of errors in the client application related to MBC transactions that are otherwise uncategorized
- No Session (Open)—Number of MBC transactions creating or updating a media session that could not be sent to MBCD because the media session state information could not be located
- No Session (Drop)—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located
- Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications

- Exp Flow Not Found—Number of flow timer expiration notifications received from the MBCD by all applications for which no media session or flow information was present in the application.
- Transaction Timeouts—Number of MBC transaction timeouts
- Server statistics count errors and events encountered by MBCD
- Server Errors—Number of uncategorized errors in the MBC server
- Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table
- Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table
- Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow
- Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow
- Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table
- ARP Wait Errors—Number of errors and timeouts related to obtaining the Layer 2 addressing information necessary for sending media
- Exp CAM Not Found—This statistic shows the number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD from the NP
- Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification
- Unk Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables
- Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application
- Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner
- No Ports Available—Number of steering port allocation requests not be satisfied due to a lack of free steering ports in the realm
- Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application
- Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm

Viewing Realm Configurations

You can use the **show realm** command to display all realm-specific configurations. For example:

```
ACMEPACKET# show realm
14: 27: 38-56SIP Realm Statistics
```

Realm	Active	Rate	High	Total	Total	PerMax	High
realm1							
Inbound	0	0.0	0	0	0	0	0

Outbound 0 0.0 0 0 0 0 0

Viewing Realm Configurations for a Specific Realm

```
ACMEPACKET# show realm realm1
realm stats for : Realm: realm1
14: 29: 22-40
Realm realm1 NO ACTIVITY
```

Viewing Monthly Minutes for a Specific Realm

You can use the **show monthly minutes <realm-id>** command to display the monthly minutes for a specified realm. For example:

```
ACMEPACKET# show monthly-minutes realm1
14: 31: 33-51
Realm      MinutesAllowed  MinutesLeft      Minutes Exceed Rejects
-----
Recent    Total    PerMax
realm1    10       10           0         0         0
```

Media Alarms

The following table lists information about the different media alarms.

Table 1:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtMediaOutOfMemory trap generated
MBCD ALARM INTERNAL	262146	MINOR	An internal software error.	Internal Error. No agent for socket <IPPort>.	None
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtUnknownRealm
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtMediaBandwidth Trap
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	<ul style="list-style-type: none"> apSyslogMessageGenerated apSysMgmtMediaPortsTrap

Viewing Deny ACL List

Display a list of deny ACLI entries by using the **acl-show** command at the topmost ACLI prompt. The following information is displayed:

- Incoming port, slot, and VLAN tag
- Source IP, bit mask, port, and port mask
- Destination IP address and port
- Protocol
- ACL entry as static and dynamic
- ACL entry index

For example:

```
ACMEPACKET# acl -show
```

deny entries:

```
intf: v1an source-ip/mask: port/mask dest-ip/mask: port/mask  prot type
index
```

Total number of deny entries = 0

Denied Entries not allocated due to ACL constraints: 0

task done

Network Faults

This section explains how to access network fault information. Network alarms account for problems related to low-level network issues and might occur when the software is unable to communicate with the hardware.

NAT Statistics

Use the following command to display NAT table information.

- **show nat**

There is also an alarm that occurs when the NAT table usage reaches 90% or greater of its capacity.

Viewing Information from the NAT Table

Display information from the NAT table by using the **show nat** command along with one of the following subcommands.

Caution: Do not display the entire contents of the NAT table on your screen. The size of the table can interfere with call processing.

- **by-index:** specify the range of entries to display, up to a maximum of 5024 entries. For example, to see entries on lines 10 through 50 of the NAT table, enter the following:

```
show nat by-index 10 50
```

A <Space> separates the two numbers defining the range. If you do not specify a range, the system uses the default range of 1 through 200. The range you enter here corresponds to line numbers in the table, and not to the number of the entry itself.

- **by-addr:** specify the entries to display according to SA and DA values. For example, to view entries with an SA of 192.168.112.25 and a DA 101.102.103.104, enter the following:

```
show nat by-addr 192.168.112.25 101.102.103.104
```

The system matches these values to the NAT table entries and displays the pertinent information. If no addresses are entered, the system displays all of the table entries (all of the table entries will match).

- **in-tabular:** Display a specified range of entries in the NAT table display in table form, maximum of 5024 entries. The syntax is modeled on the **show nat by-index** command: **show nat in-tabular <starting entry> <ending entry>**

- info: Display general NAT table information. The output is used for quick viewing of a Net-Net SBC's overall NAT functions, including the maximum number of NAT table entries, the number of used NAT table entries, the length of the NAT table search key, the first searchable NAT table entry address, the length of the data entry, the first data entry address, and whether or not aging and policing are enabled in the NAT table.
- flow-info: Display NAT table entry debug information. The syntax is:

```
show nat flow-info <all | by-addr | by-switchid>
```

Viewing NAT Information By Index

The following example shows the output of the **show nat by-index** command:

```
ACMEPACKET# show nat by-index 1 2
-----
Total number of entries in the Database = 395
NAT table search address 1, xsmAddr 62580 :
Flow type: Traditional weighted flow
SA_flow_key      : 192.168.200.041      SA_prefix       : 32
DA_flow_key      : 000.000.000.000      DA_prefix       : 0
SP_flow_key      : 0                    SP_prefix       : 0
DP_flow_key      : 0                    DP_prefix       : 0
VLAN_flow_key    : 0
Protocol_flow_key : 0
Ingress_flow_key : 64
Ingress Slot     : 64
Ingress Port     : 0
XSA_data_entry   : 000.000.000.000
XDA_data_entry   : 000.000.000.000
XSP_data_entry   : 0
XDP_data_entry   : 0
Egress_data_entry : 0
Egress Slot      : 0
Egress Port      : 0
flow_action      : 0x1
optional_data    : 0
FPGA_handle      : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry  : 0
host_table_index : 1
Switch ID        : 0x00034000
average-rate      : 0
weight           : 0x10
init_flow_guard   : 4294967295
inact_flow_guard   : 4294967295
max_flow_guard    : 4294967295

q - quit, return - next entry, space - through to the end :
```

Viewing NAT Information By Address

```
ACMEPACKET# show nat by-addr
sip_key = (null), dip_key = (null)
-- Total number of entries in the NAT table is 407
```

NAT table search address 1 :

Flow type: Traditional weighted flow. Weight = 16

```
SA_flow_key      : 192.168.200.041      SA_prefix      : 32
DA_flow_key      : 000.000.000.000      DA_prefix      : 0
SP_flow_key      : 0                    SP_prefix      : 0
DP_flow_key      : 0                    DP_prefix      : 0
VLAN_flow_key    : 0
Protocol_flow_key : 0
Ingress_flow_key : 64
Ingress Slot     : 64
Ingress Port     : 0
XSA_data_entry   : 000.000.000.000
XDA_data_entry   : 000.000.000.000
XSP_data_entry   : 0
XDP_data_entry   : 0
Egress_data_entry : 0
Egress Slot     : 0
Egress Port     : 0
flow_action      : 0x1
optional_data     : 0
FPGA_handle      : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry  : 0
host_table_index : 1
Switch ID        : 0x00034000
average-rate     : 0
weight           : 0x10
init_flow_guard  : 4294967295
inact_flow_guard  : 4294967295
max_flow_guard   : 4294967295
```

q - quit, return - next entry, space - through to the end :

Viewing NAT Information In Tabular

acmepacket# **show nat In-tabular**

NAT	SA_key	DA_key	SP_key	DP_key	VLAN_key
ING	PROTO	WEIGHT			
addr= 1,	si p=0xac100056,	di p=0x00000000,	SP=0x0000,	DP=0x0000,	VLAN=0,
Intf=64,	proto= 0,	weight=0x10			
addr= 2,	si p=0x7f000064,	di p=0x00000000,	SP=0x0000,	DP=0x0000,	VLAN=999,
Intf=64,	proto= 0,	weight=0x10			
addr= 3,	si p=0x00000000,	di p=0xac100056,	SP=0x0000,	DP=0x0000,	VLAN=0,
Intf= 0,	proto= 6,	weight=0x9			
addr= 4,	si p=0x00000000,	di p=0xac100056,	SP=0x0000,	DP=0x0000,	VLAN=0,
Intf= 0,	proto= 17,	weight=0x9			
addr= 5,	si p=0x00000000,	di p=0x7f000064,	SP=0x0000,	DP=0x13c4,	VLAN=999,
Intf= 0,	proto= 17,	weight=0xd			
addr= 6,	si p=0x00000000,	di p=0xac100058,	SP=0x0000,	DP=0x13c4,	VLAN=0,
Intf= 0,	proto= 17,	weight=0xd			

```

addr= 7, sip=0x00000000, dip=0xc0a86458, SP=0x0000, DP=0x13c4, VLAN=
0, Intf= 1, proto= 17, weight=0xd
addr= 8, sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0001, VLAN=
0, Intf= 0, proto= 6, weight=0x63

```

Viewing General NAT Table Information

```

acmepacket# show nat info
-- NAT table info --
Maximum number of entries : 7768
Number of used entries    : 10
Length of search key      : 2 (x 64 bits)
First search entry address : 0x0
Length of data entry      : 4 (x 64 bits)
First data entry address  : 0x0
Enable aging              : 1
Enable policing           : 0

```

Viewing NAT Flow Information

You can view NAT flow information by using the `show nat flow-info <all | by-addr | by switchid>` command. For example:

```

ACMEPACKET# show nat flow-info all
SA_flow_key      : 001.000.002.003      SA_prefix       : 32
DA_flow_key      : 000.000.000.000      DA_prefix       : 0
SP_flow_key      : 0                    SP_prefix       : 0
DP_flow_key      : 0                    DP_prefix       : 0
VLAN_flow_key    : 0
Protocol_flow_key : 0
Ingress_flow_key : CPU PORT(64)
Ingress Slot     : 64
Ingress Port     : 0
XSA_data_entry   : 000.000.000.000
XDA_data_entry   : 000.000.000.000
XSP_data_entry   : 0
XDP_data_entry   : 0
Egress_data_entry : 0
Egress Slot      : 0
Egress Port      : 0
flow_action      : 0
optional_data    : 0
FPGA_handle      : 0x00000000
assoc_FPGA_handle : 0x00000000
VLAN_data_entry  : 0
host_table_index : 1
Switch ID        : 0x00034000
average-rate     : 0
weight           : 0x0
init_flow_guard  : 4294967295
inact_flow_guard  : 4294967295
max_flow_guard   : 4294967295
payload_type_2833 : 0
index_2833       : 0
pt_2833_egress   : 0
LI_X3 Index      : 0x00000000

```



```

-----
IFD Index   IFD Info                               Input Admissi on Params
0x00034000 Static = No                           Word 0 =Valid, Word 1 = Valid
           Enabled for CPU Traffic = Yes         ABJ Mode = Enabled,
EPD Mode = Disabled
           Enabled for Data Traffic = Yes         IFD enabled = Disabled,
IFD assigned = Unassigned
           IQD Assigned = No                     Thresholding Enabled,
TG Index = 0x0
                                           WRED Disabled.

```

```

OFD Index   OfT          DestID   QueueIndex   Scheduling Parameters.

0x00034000 0x00034000 0x00000000 0x00000001   Word 0 = Valid,
Word 1 = Valid
id
                                           Word 2 = Valid, Word 3 = Valid
id
                                           Word 4 = Valid
                                           Packet Mode = Yes
                                           SPWRR Parameters
                                           Delta = 0x00000001
                                           Credit Min Exponent = 0x0
00000000
           Pipe Index   Pipe Scheduler Parameters
           0x00008000   Packet Max Mode Set = Enabled
                           Delta = 0x00000001
                           mticke = 0x00000007
                           Credit Min Exponent = 0x00000008
                           Credit Min Mantissa = 0x00000000
                           Credit Max Exponent = 0x00000007
                           Credit Max Mantissa = 0x00000018

```

```

Total Dropped = 0x0
Total Received = 0x5
-----

```

```

01.000.011.012   SA_prefix   : 32
DA_flow_key      : 192.168.050.001   DA_prefix       : 32
SP_flow_key      : 80                 SP_prefix       : 16
DP_flow_key      : 0                 DP_prefix       : 0
VLAN_flow_key    : 0
Protocol_flow_key : 6
Ingress_flow_key : 0
Ingress Slot     : 0
Ingress Port     : 0
XSA_data_entry   : 000.000.000.000
XDA_data_entry   : 192.168.050.001
XSP_data_entry   : 0
XDP_data_entry   : 0
Egress_data_entry : 0
Egress Slot      : 0

```

```

Egress Port      : 0
flow_action      : 0
optional_data     : 0
FPGA_handle      : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry  : 0
host_table_index : 2
Switch ID        : 0x00000002
average-rate     : 0
weight           : 0x0
init_flow_guard   : 4294967295
inact_flow_guard  : 4294967295
max_flow_guard    : 4294967295
payload_type_2833 : 0
index_2833       : 0
pt_2833_egress   : 0
LI_X3_Index      : 0x00000000

```

```

-----
IFD Index  IFD Info                                Input Admission Params
0x00000002 Static = No                               Word 0 = Valid, Word 1 = Valid
                Enabled for CPU Traffic = Yes         ABJ Mode = Enabled,
EPD Mode = Disabled
                Enabled for Data Traffic = Yes         IFD enabled = Disabled,
IFD assigned = Unassigned
                IQD Assigned = No                       Thresholding Enabled,
TG Index = 0x0
                WRED Disabled.

```

```

OFD Index  OfT      DestID  QueueIndex  Scheduling Parameters.

0x00040002 0x00040002 0x00000000 0x00000001  Word 0 = Valid,
Word 1 = Valid
id
                Word 2 = Valid, Word 3 = Valid
id
                Word 4 = Invalid
                Packet Mode = Yes
                Shaping Parameters
                Sustained Cell Rate Exp =
0x00000005
                Sustained Cell Rate Mantissa =
ssa = 0x000000e8
                Peak Cell Rate Exp = 0x00
000000
                Peak Cell Rate Mantissa =
0x00000000
                Max Burst Threshold Exp =
0x00000000
                Max Burst Threshold Mantissa =
ssa = 0x00000000
                Latency Sensitive = Disabled
led

```

```

Pipe Index      Pipe Scheduler Parameters
0x00008000      Packet Max Mode Set = Enabled
                  Delta = 0x00000001
                  mticke = 0x00000007
                  Credit Min Exponent = 0x00000008
                  Credit Min Mantissa = 0x00000000
                  Credit Max Exponent = 0x00000007
                  Credit Max Mantissa = 0x00000018

```

```

Total Dropped = 0x0
Total Received = 0x0

```

NAT Table Utilization Alarm

The following table describes the NAT table utilization alarm:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	<ul style="list-style-type: none"> apSysMgmtGroupTrap trap generated syslog

ARP Statistics

You can use the following command to view ARP statistics:

- **show arp**

There is also an alarm that occurs when a gateway is unreachable.

Viewing Address Mappings

Display the current Internet-to-Ethernet address mappings in the ARP table by using the **show arp** command. The first section of this display shows the following information: destination, gateway, flags, reference count, use, and interface. The second section shows the interface, VLAN, IP address, MAC address, timestamp, and type.

The intf (interface) column in the ARP includes both slot and port information. If a value of 0/1 appears, 0 refers to the slot and 1 refers to the port.

ACMEPACKET# **show arp**

```

LINK LEVEL ARP TABLE
desti nation      gateway      flags  Refcnt  Use      Interface
-----
172. 30. 0. 1      00: 0f: 23: 4a: d8: 80  405    1        0      wancom0
-----

```

Total ARP Entries = 3

```

-----
Intf  VLAN  IP-Address      MAC      time-stamp  type
0/0   0     010. 000. 045. 001  00: 00: 00: 00: 00: 00  1108462861  invalid

```

Special Entries:

```

0/0   0     000. 000. 000. 000  00: 00: 00: 00: 00: 00  1108462861  gateway

```

```
0/0    0    010.000.045.000    00:00:00:00:00:00    1108462861    network
```

Gateway Status:

Intf	VLAN	IP-Address	MAC	time-stamp	hb	status
0/0	0	010.000.045.001	00:00:00:00:00:00	1108462861		unreachabl e

-- ARP table info --

```
Maximum number of entries : 512
Number of used entries    : 3
Length of search key      : 1 (x 64 bits)
First search entry address : 0x3cb0
Length of data entry      : 2 (x 64 bits)
First data entry address  : 0x7960
Enable aging              : 0
Enable policing           : 0
```

Gateway Unreachable Alarm

The Net-Net SBC supports polling for and detection of front interface links to the default gateway when monitoring ARP connectivity. Based on configured gateway link parameter, the Net-Net SBC detects connectivity loss, generates an alarm when it loses ARP-connectivity to the front interface gateway, and decrements its health score accordingly.

The GATEWAY UNREACHABLE network-level alarm is generated in the following circumstances:

- If the ARP manager has not received any ARP messages from a front interface gateway (assigned when the network interface was configured) within the configured *heartbeat* time period, it will send out ARP requests and wait for a reply.

You can set this heartbeat time period when configuring the gateway heartbeat interval for the redundancy element or when configuring the gw heartbeat's heartbeat field for the network interface element.

- If no reply is received after retrying (re-sending) ARP requests for a configured number of times.

You can set this *retry* value when configuring the gateway heartbeat retry field for the redundancy element or the gw heartbeat's retry count field for the network interface element.

The GATEWAY UNREACHABLE alarm decrements the health score of the Net-Net SBC by the amount you set for either the gateway heartbeat health field of the redundancy element or the gw heartbeat's health score field for the network interface. The alarm is cleared once a front interface gateway ARP entry is valid again.

After the initial alarm is triggered, the Net-Net SBC continues to attempt to connect to the front interface gateway. It issues ARP requests (retries) every five seconds until front interface gateway ARP connectivity is achieved.

You can set the gateway link failure detection and polling parameters, and the health score decrement (reduction) value for the entire Net-Net SBC by configuring the redundancy element or for each individual network interface by configuring the gw heartbeat for the network interface.

The following table lists information about the GATEWAY UNREACHABLE alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
GATEWAY UNREACHABLE	dynamicID	MAJOR	The Net-Net SBC lost ARP connectivity to the front interface gateway.	gateway X.X.X.X unreachable on slot Y port Z subport ZZ (where X.X.X.X is the IPv4 address of the front interface gateway, Y is the front interface slot number, Z is the front interface port number, and ZZ is the subport ID)	<ul style="list-style-type: none"> apSysMgmtGatewayUnreachableTrap generated syslog

The value of this alarm changes based on a number of factors. The total alarm ID range falls between 12288 - 229357. The alarm ID is calculated based on a compilation of a hexadecimal number that represents the VLAN ID and the front interface slot/port numbers.

View Network Interfaces Statistics

Display statistics for network interfaces by using **show interfaces** command. The following is an example of the C6.0.0 output:

```
ACMEPACKET# show interfaces
wancom (unit number 0):
  Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 172.30.55.127
  Broadcast address: 172.30.255.255
  Netmask 0xffff0000 Subnetmask 0xffff0000
  Ethernet address is 00:08:25:01:07:60
  Metric is 0
  Maximum Transfer Unit size is 1500
  3481 octets received
  93 octets sent
  3481 packets received
  93 packets sent
  3389 non-unicast packets received
  0 non-unicast packets sent
  92 unicast packets received
  93 unicast packets sent
  0 input discards
  0 input unknown protocols
  0 input errors
  0 output errors
  0 collisions; 0 dropped
lo (unit number 0):
  Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
  Type: SOFTWARE_LOOPBACK
  Internet address: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  Metric is 0
  Maximum Transfer Unit size is 32768
```

```

69 packets received; 69 packets sent
0 multi cast packets received
0 multi cast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped

```

The following is an example of the Cx6.0.0 output:

```

# show interfaces
lo (unit number 0):
    Flags: (0xc8049) UP LOOPBACK MULTI CAST TRAI LERS ARP RUNNI NG I NET_UP
    I NET6_U
    P
    Type: SOFTWARE_LOOPBACK
    inet: 127.0.0.1
    Netmask 0xff000000 Subnetmask 0xff000000
    inet6: ::1 prefix len 128
    Metric is 0
    Maximum Transfer Unit size is 1536
    198 packets received; 198 packets sent
    0 multi cast packets received
    0 multi cast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
    0 output queue drops
eth (unit number 0):
    Flags: (0x78843) UP BROADCAST MULTI CAST ARP RUNNI NG I NET_UP
    Type: ETHERNET_CSMACD
    inet: 172.30.1.186
    Broadcast address: 172.30.255.255
    Netmask 0xfffff000 Subnetmask 0xfffff000
    Ethernet address is 00:08:25:a0:78:50
    Metric is 0
    Maximum Transfer Unit size is 1500
    123096284 octets received
    12747 octets sent
    23 uni cast packets received
    198 uni cast packets sent
    96295 mul ti cast packets received
    0 multi cast packets sent
    1396154 broadcast packets received
    1 broadcast packets sent
    0 incoming packets discarded
    0 outgoing packets discarded
    0 incoming errors
    0 outgoing errors
    0 unknown protos
    0 collisions; 0 dropped
    0 output queue drops
sp (unit number 0):
    Flags: (0x68043) UP BROADCAST MULTI CAST ARP RUNNI NG I NET_UP
    Type: ETHERNET_CSMACD
    inet: 192.168.69.10
    Broadcast address: 192.168.69.255
    Netmask 0xffffffff Subnetmask 0xffffffff

```

```

Ethernet address is 00:08:25:a0:78:53
Metric is 0
Maximum Transfer Unit size is 1500
0 octets received
0 octets sent
0 unicast packets received
0 unicast packets sent
0 non-unicast packets received
0 non-unicast packets sent
0 incoming packets discarded
0 outgoing packets discarded
0 incoming errors
0 outgoing errors
0 unknown protocols
0 collisions; 0 dropped
0 output queue drops
lefty (media slot 0, port 0)
  Flags: Down
  Type: GIGABIT_ETHERNET
  Admin State: enabled
  Auto Negotiation: enabled
  Internet address: 192.168.69.10      Vlan: 69
  Broadcast Address: 192.168.69.255
  Netmask: 0xffffffff00
  Gateway: 192.168.69.10
  Internet address: 172.16.0.10      Vlan: 0
  Broadcast Address: 172.16.255.255
  Netmask: 0xffff0000
  Gateway: 0.0.0.0
  Ethernet address is 00:08:25:a0:78:53
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  0 packets received
  0 packets sent
  0 non-unicast packets received
  0 non-unicast packets sent
  0 unicast packets received
  0 unicast packets sent
  0 input discards
  0 input unknown protocols
  0 input errors
  0 output errors
  0 collisions; 0 dropped
righty (media slot 1, port 0)
  Flags: Down
  Type: GIGABIT_ETHERNET
  Admin State: enabled
  Auto Negotiation: enabled
  Internet address: 192.168.200.10    Vlan: 0
  Broadcast Address: 192.168.200.255
  Netmask: 0xffffffff00
  Gateway: 0.0.0.0

```

```

Ethernet address is 00:08:25:a0:78:55
Metric is 0
Maximum Transfer Unit size is 1500
0 octets received
0 octets sent
0 packets received
0 packets sent
0 non-unicast packets received
0 non-unicast packets sent
0 unicast packets received
0 unicast packets sent
0 input discards
0 input unknown protocols
0 input errors
0 output errors
0 collisions; 0 dropped

```

You can also view key running statistics about the interfaces within a single screen by using the **show interfaces [brief]** command.

For example:

ACMEPACKET# **show interfaces brief**

Sl t	Prt	Vlan	Interface	IP	Gateway	Adm	Oper
Num	Num	ID	Name	Address	Address	Stat	Stat

-	-	-	lo0	127.0.0.1/8	-	-	up
-	-	-	lo0	::1/128	-	-	up
-	-	-	eth0	172.30.43.1/16	-	-	up
-	-	-	sp0	172.16.0.208/24	-	-	up
-	-	-	sp1	192.168.10.10/24	-	-	up
0	0	0	access	172.16.0.208/24	172.16.0.1	up	up
0	*1	-	access	Redundant Link State:		stby	up
1	0	0	core	192.168.10.10/24	192.168.10.1	up	dn

Physical Interface Faults

This section contains information about the statistics you can view for network and media interfaces, and alarms that occur for physical interface faults.

Viewing Network Interface Statistics

Display information about the network interfaces by using the **show interfaces** command.

For example:

ACMEPACKET# show interfaces

wancom (unit number 0):

Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING

Type: ETHERNET_CSMACD

Internet address: 172.30.55.127

Broadcast address: 172.30.255.255

Netmask 0xffff0000 Subnetmask 0xffff0000

Ethernet address is 00:08:25:01:07:60

Metric is 0

Maximum Transfer Unit size is 1500

236354 octets received

847 octets sent

236354 packets received

847 packets sent

235526 non-unicast packets received

0 non-unicast packets sent

828 unicast packets received

847 unicast packets sent

0 input discards

0 input unknown protocols

0 input errors

0 output errors

0 collisions; 0 dropped

lo (unit number 0):

Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING

Type: SOFTWARE_LOOPBACK

Internet address: 127.0.0.1

Netmask 0xff000000 Subnetmask 0xff000000

Metric is 0

Maximum Transfer Unit size is 32768

104 packets received; 104 packets sent

0 multicast packets received

0 multicast packets sent

0 input errors; 0 output errors

0 collisions; 0 dropped

**Viewing Media
Interface Statistics**

Display information about the Net-Net system's media interfaces, if any, by using the show media command. You can also display information about loopback (internal) interfaces, which are logical interfaces used for internal communications.

You can use the following arguments to specify the information you want to view:

- classify—network processor statistics; requires slot and port arguments
- host-stats—host processor statistics, including number of packets received at a specific port and types of packets received; requires slot and port arguments
- frame-stats—frame counts and drops along the host path; does not require port and slot specification

- network—network interface details; does not require port and slot specification
- physical—physical interface information; does not require port and slot specification
- phy-stats—data/packets received on the front interface (media) ports; shows the physical level of front interface statistics according to slot and port numbers and is displayed according to received data/packets and transmitted data/packets; requires slot and port arguments

For the slot arguments, 1 corresponds to the left Phy slot and 2 corresponds to the right Phy slot on the front of the Net-Net chassis. For the port argument, the values are 0, 1, 2, and, 3, with 0 corresponding to the leftmost port and 3 corresponding to the rightmost port.

For example:

The `RECEIVE STATISTICS` and `TRANSMIT STATISTICS` in the following examples have been abbreviated.

Viewing Network Interface Statistics

ACMEPACKET# `show media network`

Slot/Port:	VI an	IP Address	Mask	Gateway Status
1/0:	4	192. 168. 200. 10	255. 255. 255. 0	192. 168. 200. 1 enable
	2	192. 168. 200. 10	255. 255. 255. 0	192. 168. 200. 1 enable
2/3:	0	63. 67. 143. 8	255. 255. 255. 0	63. 67. 143. 1 enable

Viewing Physical Interface Statistics

ACMEPACKET# `show media physical`

Slot/Port:	MAC Address	Encap	Connection ID	Frames Rx
1/1: 0:	8: 25: 1: 0: 53	0x0	0x0 0x0	
2/3: 0:	8: 25: 1: 0: 54	0x0	0x0 0x0	

Viewing Front Interface Physical Level Statistics

ACMEPACKET# `show media phy-stats 0 0`

*** `RECEIVE STATISTICS` ***

Statistics Counter Name	:	Count (hex)	:	Count (decimal)
Rx bytes recd - Upper 32 bits :		0x0000		0x002E : 46
Rx bytes recd - Lower 32 bits :		0xB132		0xE69D : 2972903069
Rx 64 (Bad + Good) :		0x0005		0x3392 : 340882
Rx 65 to 127 (Bad + Good) :		0x006F		0x6F88 : 7303048
Rx 128 to 255 (Bad + Good) :		0x36BA		0xB44C : 918205516
Rx 256 to 511 (Bad + Good) :		0x0004		0x531C : 283420
Rx 512 to 1023 (Bad + Good) :		0x0000		0x02D0 : 720
Rx 1024 to 1518 (Bad + Good) :		0x0000		0x0000 : 0
Rx 1519 to 1530 (Bad + Good) :		0x0000		0x0000 : 0
Rx > 1530 (Good) :		0x0000		0x0000 : 0
Rx Error Oversized > 1530 :		0x0000		0x0000 : 0
Rx Good Undersized < 64 :		0x0000		0x0000 : 0
Rx Error Undersized < 64 :		0x0000		0x0000 : 0
Rx Unicast Frames In (Good) :		0x3732		0xBCF4 : 926072052
Rx Multicast Frames In (Good) :		0x0000		0x93A2 : 37794
Rx Broadcast Frames In (Good) :		0x0000		0x5CBC : 23740

```

Rx Sync loss / Rx PHY Error      : 0x0000 0x0000 : 0
Rx GMAC Fifo Full Errors        : 0x0000 0x0000 : 0
Rx FCS Errors                   : 0x0000 0x0000 : 0
Rx Delimiter Sequence Errors    : 0x0000 0x0000 : 0
Rx GMAC Drop count              : 0x0000 0x0000 : 0
Rx Symbol Error/Alignment err   : 0x0000 0x0000 : 0
Rx Pause Control Frames In      : 0x0000 0x0000 : 0
Rx Control Frames In            : 0x0000 0x0000 : 0
Rx Threshold Oversize           : 0x0000 0x0000 : 0

```

*** TRANSMIT STATISTICS ***

Statistics Counter Name	Count (hex)	Count (decimal)
Total Xmitted - Upper 32 bits	0x0000 0x002E	46
Total Xmitted - Lower 32 bits	0xC35B 0x3BCC	3277536204
Tx 64	0x0011 0x3635	1127989
Tx 65 to 127	0x0084 0xC730	8701744
Tx 128 to 255	0x36AC 0xEA43	917301827
Tx 256 to 511	0x0000 0x0000	0
Tx 512 to 1023	0x0000 0x0000	0
Tx 1024 to 1518	0x0000 0x0000	0
Tx 1519 to 1530	0x0000 0x0000	0
Tx > 1530	0x0000 0x0000	0
Tx Unicast Frames Out	0x3742 0xE767	927131495
Tx Multicast Frames Out	0x0000 0x0000	0
Tx Broadcast Frames Out	0x0000 0x0041	65
Tx FCS Error	0x0000 0x0000	0
Tx Pause Control Frames Out	0x0000 0x0000	0
Tx Control Frames Out	0x0000 0x0000	0
Tx Bad Frames Fifo Underrun	0x0000 0x0000	0
Tx Bad Frames Fifo Overrun	0x0000 0x0000	0
Tx Drop Frames Fifo Overrun	0x0000 0x0000	0
Tx Bad Frames Parity Error	0x0000 0x0000	0
Tx Drop Frames Parity Error	0x0000 0x0000	0
Tx Bad Frames Sequence Error	0x0000 0x0000	0
Tx Drop Frames Sequence Error	0x0000 0x0000	0
Tx Bad Frames Jam Bit Error	0x0000 0x0000	0
Tx Drop Frames Jam Bit Error	0x0000 0x0000	0
Tx Undersized < 64	0x0000 0x0000	0
Tx Excess Collisions	0x0000 0x0000	0
Tx One Collision	0x0000 0x0000	0
Tx > One Collision	0x0000 0x0000	0

Physical Interface Alarms

The following table lists the physical interface alarms.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK UP ALARM GIGPORT	131073	MINOR	Gigabit Ethernet interface 1 goes up.	Slot 1 port 0 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM GIGPORT	131074	MINOR	Gigabit Ethernet interface 2 goes up.	Slot 2 port 0 UP	<ul style="list-style-type: none"> linkUp trap generated syslog

LINK DOWN ALARM GIGPORT	131075	MAJOR	Gigabit Ethernet interface 1 goes down.	Slot 1 port 0 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK DOWN ALARM GIGPORT	131076	MAJOR	Gigabit Ethernet interface 2 goes down.	Slot 2 port 0 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK UP ALARM VXINTF	131077	MINOR	Control interface 0 goes up.	Port 0 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM VXINTF	131078	MINOR	Control interface 1 goes up.	Port 1 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM VXINTF	131079	MINOR	Control interface 2 goes up.	Port 2 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK DOWN ALARM VXINTF	131080	MAJOR	Control interface 0 goes down.	Port 0 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK DOWN ALARM VXINTF	131081	MAJOR	Control interface 1 goes down.	Port 1 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK DOWN ALARM VXINTF	131082	MAJOR	Control interface 2 goes down.	Port 2 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK UP ALARM FEPORT	131083	MAJOR	Fast Ethernet slot 1, port 0 goes up.	Slot 1 port 0 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131084	MAJOR	Fast Ethernet slot 2, port 0 goes up.	Slot 2 port 0 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131085	MINOR	Fast Ethernet slot 1, port 1 goes up.	Slot 1 port 1 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131086	MINOR	Fast Ethernet slot 2, port 1 up.	Slot 2 port 1 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131087	MINOR	Fast Ethernet slot 1, port 2 goes up.	Slot 1 port 2 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131088	MINOR	Fast Ethernet slot 2, port 2 goes up.	Slot 2 port 2 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131089	MINOR	Fast Ethernet slot 1, port 3 goes up.	Slot 1 port 3 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK UP ALARM FEPORT	131090	MINOR	Fast Ethernet slot 2, port 3 goes up.	Slot 2 port 3 UP	<ul style="list-style-type: none"> linkUp trap generated syslog
LINK DOWN ALARM FEPORT	131091	MAJOR	Fast Ethernet slot 1, port 0 goes down.	Slot 1 port 0 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131092	MAJOR	Fast Ethernet slot 2, port 0 goes down.	Slot 2 port 0 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog

LINK DOWN ALARM FEPORT	131093	MAJOR	Fast Ethernet slot 1, port 1 goes down.	Slot 1 port 1 DOWN	<ul style="list-style-type: none">• linkDown trap generated• minor dry contact• syslog
LINK DOWN ALARM FEPORT	131094	MAJOR	Fast Ethernet slot 2, port 1 goes down.	Slot 2 port 1 DOWN	<ul style="list-style-type: none">• linkDown trap generated• minor dry contact• syslog
LINK DOWN ALARM FEPORT	131095	MAJOR	Fast Ethernet slot 1, port 2 goes down.	Slot 1 port 2 DOWN	<ul style="list-style-type: none">• linkDown trap generated• minor dry contact• syslog
LINK DOWN ALARM FEPORT	131096	MAJOR	Fast Ethernet slot 2, port 2 goes down.	Slot 2 port 2 DOWN	<ul style="list-style-type: none">• linkDown trap generated• minor dry contact• syslog

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK DOWN ALARM FEPORT	131097	MAJOR	Fast Ethernet slot 1, port 3 goes down.	Slot 1 port 3 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131098	MAJOR	Fast Ethernet slot 2, port 3 goes down.	Slot 2 port 3 DOWN	<ul style="list-style-type: none"> linkDown trap generated minor dry contact syslog

Verifying an IP Address

This section explains how to determine the existence of an IP address, and whether it is up and accepting requests.

You can use the ping command with the IPv4 address to send echo messages that indicate whether a given address is available. In addition the ping command returns the following information:

- time in milliseconds it took the ICMP packets to reach the destination and return
- statistics that indicate the number of packets transmitted, the number of packets received, and the percentage of packet loss.
- time in milliseconds for the minimum, average, and maximum RTTs. The default timeout is 64 milliseconds.

The following example shows the ping command used with IPv4 address 10.0.0.1:

```
ACMEPACKET# ping 172. 30. 1. 150
PING 172. 30. 1. 150: 56 data bytes
64 bytes from 172. 30. 1. 150: icmp_seq=0. time=1. ms
64 bytes from 172. 30. 1. 150: icmp_seq=1. time=0. ms
64 bytes from 172. 30. 1. 150: icmp_seq=2. time=0. ms
64 bytes from 172. 30. 1. 150: icmp_seq=3. time=0. ms
----172. 30. 1. 150 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/1
```

Specifying a Source Address for ICMP Pings

The Net-Net 4000's ping command can also be used to set the source IP address (a valid network interface) to use when sending ICMP pings. You must enter the IP address for the entity you want to ping first, followed by the source IP address.

To specify a source address for an ICMP ping:

- At the main system prompt, type ping and a <Space>, the IP address of the entity you want to ping, the network interface, and then the source IP address you want to use, and then press <Enter>.

```
ACMEPACKET # ping 124. 7. 58. 6 core: 0 172. 30. 56. 6
```

DNS Statistics

You can monitor DNS statistics using the ACLI **show dns** command. The information displayed includes the following:

- Queries—The number of DNS queries initiated.
- Successful—The number of DNS queries completed successfully.
- NotFound—The number of DNS queries that did not result in DNS resolution.
- TimedOut—The number of DNS queries that timed out.

To get DNS statistics, use either the ACLI **show dns** or **show dns stats** command. Both return the same output. For example:

```
ACMEPACKET# show dns
```

```
18: 20: 18-16
```

```

      ---Queries--- --Successful-- ---NotFound--- ---TimedOut---
DNS Intf Name  Current  Total  Current  Total  Current  Total  Current
Total
M10              1      1      0      0      0      0      1
1

```

```
ACMEPACKET# show dns stats
```

```
12: 33: 57-43
```

```

      ---Queries--- --Successful-- ---NotFound--- ---TimedOut---
DNS Intf Name  Current  Total  Current  Total  Current  Total  Current
Total
M10              0      0      0      1      0      0      0
0

```

Viewing DNS Statistics for Specific Cache Entries

To view DNS statistics for specific cache entries, use the **show dns cache-entry** command. You must include both the realm name and the entry ID as arguments to avoid receiving an error message. Your cache key entries must appear in one of the following formats:

- NAPTR records—NAPTR:abc.com
- SRV records—SRV:_sip._tcp.abc.com
- A records—A:abc.com

A successful inquiry appears as follows:

```
ACMEPACKET# show dns cache-entry core A: abc. sip. com
```

```
Query-->
```

```
Q: A abc. sip. com ttl=86329
```

```
Answers-->
```

```
172. 16. 0. 191
```

Clearing ENUM and DNS Statistics

To clear statistics for DNS, you can use additions to the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the **show dns** command.

The **reset** command takes the DNS arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

You can **reset all** system statistics using the reset all command.

This section shows you how to clear DNS statistics. The sample below shows the error message that appears if the command fails.

To clear DNS statistics:

1. At the command line, type **reset dns** and then press <Enter>.

```
ACMEPACKET# reset dns
SIP DNS statistics not available
```

System Support Information for Troubleshooting

The **show support-info** command allows you to gather a set of information commonly requested by the Acme Packet TAC when troubleshooting customer issues.

The command is available in both User and Superuser mode. You send the output from this command to a specified file by entering a <filename> argument. If no filename is specified, the output is directed to the screen. You can also view this command's output one page at a time by typing **more** at the end of the command-line entry:

```
ACMEPACKET# show support-info more
```

You can include an optional <custom> argument which displays information in the `/code/supportinfo.cmds` file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.

Included Data

This command combines the output of several other ACLI commands into a single command, which are listed in the table below.

Data Group	Included Data
General System Commands	<ul style="list-style-type: none"> • show clock • show version image • show version boot • show prom-info all • display-alarms • show uptime • show process • show arp • show sessions • show features • show memory • show buffer • show health • show running-config
Physical Interface Commands	<ul style="list-style-type: none"> • show interface • show media physical • show media phy-stats • show media host-stats • show media classify • show media network • show media frame-stats • show media tm-stats
SIP Commands	<ul style="list-style-type: none"> • show reg • show sipd all • show sipd agent • stack sipd
H323 Commands	<ul style="list-style-type: none"> • show h323 • show h323 h323stats • show h323 agentstats • show h323 stackCallstats • show h323 stackPvtStats • show h323 stackDisconnectInstate • show h323 stacklist • stack h323d
MGCP Commands	<ul style="list-style-type: none"> • show algd all • show algd rsip • show algd errors • stack algd
Call Media Commands	<ul style="list-style-type: none"> • show mbcd all • show mbcd realms • stack mbcd

Using the ACLI show support-info command

To gather and ship information to Acme Packet TAC using the `show support-info` command:

1. Select a meaningful filename for the file to which you will send data.
2. In either User or Superuser mode, type **show support-info** at the prompt. Include the name of the file you want to send the information to as follows:

```
ACMEPACKET# show support-info 10102006
```

3. FTP the file to Acme Packet TAC as follows:
 - 3a. Check the IP address of the Net-Net system's management port (wancom0). (You might think of this as a management address since it is used in the management of your Net-Net system.)
 - 3b. Create the connection to your Net-Net system. In your terminal window, type **ftp** and the IPv4 address of your Net-Net system's management port (wancom0), and then press <Enter>. Once a connection has been made, a confirmation note appears followed by the FTP prompt.
 - 3c. When prompted, enter your FTP username and FTP password information. The username is always user, and the password by default is acme.
 - 3d. Invoke binary mode


```
ftp> bi nary
```

Caution: Caution: Be sure to use binary transfer mode. If you do not, transfers will be corrupted.

- 3e. From the FTP prompt, change the directory to **/ramdrv/logs**.


```
ftp> cd /ramdrv/logs
```
- 3f. Go to the directory where you are putting the file. The /code directory is used by Acme Packet TAC. To do this, type **dir** at the FTP prompt.


```
ftp> di r
```
- 3g. At the FTP prompt, enter the **get** command, a <Space>, the name of the file from the directory that you want to be transferred, and then press <Enter>.


```
ftp> get <filename>
```

Confirmation that the connection is opening and that the transfer is taking place appears.

- 3h. After the file transfer is complete, type **bye** to end the FTP session.


```
ftp> bye
```
- 3i. Once you have confirmed that Acme Packet TAC has received the file, delete it from the /code in order to free up directory space.

To Display information on the screen gathered from the show support-info command:

1. In either User or Superuser mode, type **show support-info** at the prompt. Include **more** if you want to view the information one page at a time.


```
ACMEPACKET# show support-info more
```
2. At the prompt at the bottom of the window, select one of the following ways to view further information:
 - Enter a **q** to exit and return to the system prompt
 - Press the <enter> key to view the next page
 - Press the <space> bar to view the information through the end

SIP Interface Constraints Monitoring

The session constraints configuration allows you to set up a body of constraints that you can then apply them to a SIP interface. Using the constraints you have set up, the Net-Net SBC checks and limits traffic according to those settings for the SIP interface.

SIP interfaces have two states: “In Service” and “Constraints Exceeded.” When any one of the constraints is exceeded, the status of the SIP interface changes to “Constraints Exceeded” and remains in that state until the time-to-resume period ends. The session constraint timers that apply to the SIP interface are the time-to-resume, burst window, and sustain window.

You can view information about constraints for a SIP interface by using the **show sipd interface** command. Using that command, you can show statistics for all SIP interfaces, or for one that you specify when you carry out the command.

All SIP Interfaces

To display statistical information for all SIP interfaces:

1. Type **show sipd interface** at the command line and then press <Enter>. The results will resemble the following example.

```
ACMEPACKET# show sipd interface
19: 38: 17-18
```

	----- Inbound -----			----- Outbound -----			----- Latency -----		----- Max -----		
Realm	Active	Rate	ConEx	Active	Rate	ConEx	Avg	Max	Burst	InBurst	OutBurst
external	1	0	0.0	0	0.0	0	0.000	0.000	0	0	0

Single SIP Interface

To display statistical information for a single SIP interfaces:

1. Type **show sipd interface** at the command line, followed by the realm identifier for that interface, and then press <Enter>. The results will resemble the following example.

```
ACMEPACKET# show sipd interface internal
19: 46: 10-37
Sip Interface internal (internal) [In Service]
```

	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Inbound Sessions	0	0	0	0	0	0
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Outbound Sessions	1	1	1	1	1	1
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Out of Service	-	-	0	0	0	-
Trans Timeout	0	0	0	0	0	0
Requests Sent	-	-	1	1	1	-
Requests Complete	-	-	1	1	1	-
Messages Received	-	-	3	3	2	-

Latency=0.013; max=0.013

Displaying and Clearing Registration Cache Entries

The Net-Net SBC's registration cache management for all protocols offers detailed information (beyond basic registration cache displays) and flexible ways to work with SIP, H.323, and MGCP registrations. You can query, clear, and audit entries.

Working with the SIP Registration Cache

There are two ways to view basic SIP registration cache statistics. The **show sipd endpoint-ip** command displays information regarding a specific endpoint, and the **show registration** command displays statistics for the SIP registration. These commands still remain.

There are additional commands let you view SIP registration cache information, and to clear and audit information from the cache.

Displaying the SIP Registration Cache

You can view the SIP registration cache by using one of the following commands:

- **show registration sipd by-ip <ipaddress>**—Displays the Net-Net SBC's SIP process registration cache for a specified IP address. The IP address value can be a single IP address or a wildcarded IP address value that has an asterisk (*) as its final character.

This command is only available if you configure the **reg-via-key** parameter in the SIP interface configuration prior to endpoint registration. The **reg-via-key** parameter keys all registered endpoints by IP address and username.

- **show registration sipd by-realm <realm>**—Display information for calls that have registered through a specified ingress realm. Enter the realm whose registration cache information you want to view. This value can be wildcarded.
- **show registration sipd by-registrar <ipaddress>**—Display information for calls that use a specific registrar. Enter the IP address of the registrar whose registration cache information you want to view. This value can be wildcarded.
- **show registration sipd by-route <ipaddress>**—Display information for calls by their Internet-routable IP address. This allows you to view the endpoints associated with public addresses. Enter the IP address whose registration cache information you want to view. This value can be wildcarded.
- **show registration sipd by-user <endpoint>**—Displays the Net-Net SBC's SIP process registration cache for a specified phone number or for a user name. That is, the **<endpoint>** portion of the command you enter depends on how the SIP endpoint is registered. For example, an endpoint might be registered as 7815551234@10.0.0.3 or as username@10.0.0.3. The value preceding the at-sign (@) is what you enter for the **<endpoint>**.

The phone number can be a single number (such as 7815551234) or a single number wildcarded by placing an asterisk (*) (such as 7815551*) at the end of the phone number. The user name can be a single name (such as user), or a single name wildcarded by using an asterisk at the end of the user name (such as us*).

There are brief and detailed versions of this display. To see the detailed version, add the **detail** argument to the end of your entry.

The following is a sample of this command's output for the brief view:

```
ACMEPACKET> show registration sipd by-user user*
```

```
Registration Cache
```

```
TUE JUL 11:29:50 UTC 2007
```

```
Num
```

User	Contacts	Registered at
-----	-----	-----
si p: user@acme. com	1	2007-07-26-11: 29: 50
si p: username@acme. com	1	2007-07-26-11: 29: 51
si p: username2@acme. com	1	2007-07-26-11: 29: 51

ACMEPACKET>

You can add the **detail** argument to view this command's output with detailed information:

ACMEPACKET> **show registration sipd by-user user@acme. com detail**

Registration Cache (Detailed View) TUE JUL 11: 32: 21 UTC 2007

User: si p: user@acme. com
Registered at: 2007-07-26-11: 32: 21 Surrogate User: false

Contact Information:

Contact Name: si p: user@acme. com valid: false, challenged: false
Via-Key: 172. 30. 80. 4
Registered at: 2007-07-26-11: 32: 21
Last Registered at: 2007-07-26-11: 32: 21
state: <expired>

Transport: <none>, Secure: false
Local IP: 172. 30. 80. 180: 5060

User Agent Info:

Contact: si p: user-acc-
m2vmeh72n09kb@127. 0. 0. 15: 5060; transport=udp
Realm: access, IP: 172. 30. 80. 4: 5060

SD Contact: si p: user-p3rrurj vp0l vf@127. 0. 0. 10: 5060
Realm: backbone

ACMEPACKET>

The following is a sample of the **show registration sipd by-realm** command's output:

ACMEPACKET# **show registration sipd by-realm access**

Registration Cache WED JUN 25 2008 09: 12: 03

Realm	User	Registered at
-----	-----	-----
access	si p: 16172345687@192. 168. 12. 200	2008-06-25-
09: 00: 32		
access	si p: 3397654323@192. 168. 12. 200	2008-06-25-
09: 00: 40		
-----	-----	-----

Total: 2 entries

The following is a sample of the **show registration sipd by-registrar** command's output:

ACMEPACKET# **show registration sipd by-registrar ***

Registration Cache WED JUN 25 2008 09:06:28

Registrar IP Address	User	Registered at
0.0.0.0 09:00:32	sip: 16172345687@192.168.12.200	2008-06-25-
0.0.0.0 09:00:40	sip: 3397654323@192.168.12.200	2008-06-25-

Total: 2 entries

The following is a sample of the **show registration sipd by-route** command's output:

ACMEPACKET# **show registration sipd by-route 192.168.11.101**

Registration Cache WED JUN 25 2008 09:06:04

Routable IP Address	User	Registered at
192.168.11.101 09:00:40	sip: 3397654323@192.168.12.200	2008-06-25-

Total: 1 entry

Clearing the SIP Registration Cache

You can clear the SIP registration cache by using one of the following commands:

- **clear-cache registration sipd all**—Clears all SIP registrations in the cache.
- **clear-cache registration sipd by-ip <ipaddress>**—Clears the Net-Net SBC's SIP process registration cache of a particular IP address. The IP address value can be a single IP address or an IP address range in the form n.n.n.n/nn.
- **clear-cache registration sipd by-user <endpoint>**—Clears the Net-Net SBC's SIP process registration cache of a particular phone number. The phone number can be a single number (7815554400). You can also enter a user name for this value.

Note that you cannot wildcard values for commands to clear the SIP registration cache. When you use one of these commands, the system asks you to confirm clearing the applicable cache entries.

Auditing the SIP Registration Cache

You can audit the SIP registration cache by using one of the following commands:

- **request audit registration sipd by-ip <ipaddress>**—Audits a specified IP address in the SIP registration cache.
- **request audit registration sipd by-user <endpoint>**—Audits a specific user by specifying the phone number in the SIP registration cache. You can also enter a user name for this value.

Note that you cannot wildcard values for commands to audit the SIP registration cache. Expired entries are automatically cleared.

Working with the H.323 Registration Cache

The ACLI displays the number of cached H.323 entries when you use the basic **show h323d registrations** command. Using this command with a registration key displays information about a single H.323 cached entry.

Additions to this command allow you to view detailed H.323 registration cache information based on a specific phone number or terminal identifier. You can also clear and audit the cache.

Displaying the H.323 Registration Cache

You can view the H.323 registration cache by using the **show registration h323d by-alias <endpoint>** command. For the **<endpoint>** portion of the entry, use a phone number or terminal identifier. You can wildcard the **<endpoint>** value by using an asterisk (*) as the final character in the terminalAlias string.

There are brief and detailed versions of this display. To see the detailed view, add the **detail** argument to the end of your entry.

The following is a sample of this command's output for the brief view:

```
ACMEPACKET# show registration h323d by-alias 4278_endp

Registration Cache                                FRI AUG 20: 22: 00 2007

Endpoint      Expiration      Registered at
-----
4278_endp     27              2007-08-03-19: 58: 34

ACMEPACKET#
```

You can add the **detail** argument to view this command's output with detailed information:

```
ACMEPACKET# show registration h323d by-alias 4224_endp detail

Registration Cache (Detailed View)                TUE JUL 14: 51: 59 007

Endpoint: 4224_endp, state: Registered
Registered at: 2007-04-24-14: 50: 05
Expiration: 204
Gatekeeper: open-gk1

Endpoint NAT Address: 192.168.200.56:1372
SD Call Signaling Address: 150.150.150.10:2048
SD RAS Address: 150.150.150.10:8200

Terminal Alias(s):
Alias: e164: 17815552222, Registered: true

Call Signaling Address(s):
Address: 192.168.200.56:1720

RAS Address(s):
```

Address: 192.168.200.56:1372

Clearing the H.323 Registration Cache

You can clear the H.323 registration cache by entering one of the following commands:

- **clear-cache registration h323d all**—Clears all H.323 registrations in the registration cache.
- **clear-cache registration h323d by-alias <endpoint>**—Clears H.323 registrations from the registration cache based on a phone number or terminal identifier.

Note that you cannot wildcard values for commands to clear the H.323 registration cache. When you use one of these commands, the system asks you to confirm clearing the appropriate cache entries.

Auditing the H.323 Registration Cache

You can audit the H.323 registration cache by entering one of the following commands:

- **request audit registration h323 <terminalAlias>**—Audits the H.323 registration cache based on a phone number or terminal identifier.

Working with the MGCP Registration Cache

This section describes ACLI commands that allow you to display, clear, or audit MGCP registration cache entries..

Note that all requests to the registration cache are made to the access registration.

Displaying the MGCP Registration Cache

You can view the MGCP registration cache by entering one of the **show registration mgcp by-endpoint <endpoint>** command. This command supports a regular view and a detailed view; the detailed view is entered with the additional **detail** argument at the end of the command.

You enter this command with one of the following arguments:

- **realm_id:local_name@host**
- **realm_id:host**
- **local_name@host**
- **host**

In these arguments, values are defined as follows:

- **realm_id**—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
- **local_name**—Local name of the endpoint; must end with the at-sign (@)
- **host**—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for in IP address value is optional

The following is a sample of this command's output for the regular view:

```
ACMEPACKET# show registration mgcp by-endpoint mgcp-
150: aal n/*@mta1.cablelabs.com
```

Registration Cache

WED MAR 17:58:01 2007

Endpoint	Call Agent Address	Registered at
-----	-----	-----
mgcp-150: aal n/*@mta1.cablelabs.com 28-17:56:54	150.150.150.20:2727	2007-03-
mgcp-150: aal n/1@mta1.cablelabs.com 28-17:56:54	150.150.150.20:2727	2007-03-

ACMEPACKET#

You can add the **detail** argument to view this command's output with detailed information:

ACMEPACKET# **show registration mgcp by-endpoint mgcp-150: aal n/1@mta1.cablelabs.com detail**

Registration Cache (Detailed View) THU JUN 14:03:42 2007

Endpoint: mgcp-150: aal n/1@mta1.cablelabs.com
 ID: 4,
 Registered at: 2007-06-21-14:01:14
 Public Side Registration: true
 Call Agent IP Address: 150.150.150.20:2727
 Full Call Agent Address: ca@[150.150.150.20]:2727

Session Information:
 Session ID: 5
 NAT Mode: OnlyHost

Endpoint name when sending an audit: mgcp-150: aal n/1@mta1.cablelabs.com

Call Agent View
 Gateway Address: 150.150.150.80:2427

Gateway View
 FQDN Gateway Address: mta1.cablelabs.com
 Gateway Address: 192.168.200.20:2427

Internal Key: mgcp-192: mta1.cablelabs.com
 Name Format: aal n/1

External Key: mgcp-150: mta1.cablelabs.com
 Name Format: aal n/1@mta1.cablelabs.com

Clearing the MGCP Registration Cache

You can clear the MGCP registration cache by entering one of the following commands:

- **clear-cache registration mgcp all**—Clears all MGCP registrations in the registration cache.
- **clear-cache registration by-endpoint <endpoint>**—Clears the MGCP registration cache of a particular endpoint. You enter this command with one of the following arguments:

- realm_id:local_name@host
- realm_id:host

In these arguments, values are defined as follows:

- realm_id—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
- local_name—Local name of the endpoint; must end with the at-sign (@)
- host—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for in IP address value is optional

Auditing the MGCP Registration Cache

You can audit the MGCP registration cache by entering the following command:

- **request audit registration mgcp by-endpoint <endpoint>**—Audits the MGCP registration cache for a certain endpoint.

When you audit the MGCP registration cache, the Net-Net SBC sends an audit endpoint message (AUEP) to the MGCP endpoint to determine reachability, and a reply is expected from the endpoint.

Note that MGCP audit messages are only sent to the endpoints in private realms. Requests sent to public realms are rejected and error messages are returned.

Session Management for SIP, H.323, and IWF

Using the session management feature, you can display and manage SIP, H.323, and IWF sessions using a range of new ACLI commands. You can choose to view summary or detailed displays.

If you choose to terminate a session that is already in progress, the Net-Net SBC tears down the session and returns:

- SIP BYE with a reason header naming administrative preemption as a cause, and where the cause code is 3
- H.323 Disconnect with Q.850 disconnect cause code 8, preemption

Note that if your system is carrying a heavy traffic load, it could take a good amount of time to display or clear sessions. When you use these commands, a reminder will appear about the fact that it can take up to thirty seconds for the command to complete.

Displaying Sessions

You can display SIP, H.323 and IWF sessions using the ACLI **show <protocol type> sessions** command. This command now takes the following additional arguments:

- **all**—Displays all SIP or H.323 sessions for the protocol you specify.
- **by-agent**—When entered with the name of a configured session agent, displays session information for the specified session agent: adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information
- **by-ip**—When entered with the IP address of an endpoint, displays session information for the specific endpoint; adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information

Entries for the IP address portion of this command must be enclosed in quotation marks (" ")

- **by-user**—When entered with the calling or called number, displays session information for the specified user; adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information
- **by-callid**—Display H.323 sessions for the call ID specified; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information

Example 1: Displaying All SIP Sessions

The following is an example of a display showing all SIP sessions.

```
ACMEPACKET# show sipd sessions all
-----
Displaying Sessions 'all' expression ''
This may take up to 30 seconds
-----
CallID(S) 1139b3d8-1d0010ac-13c4-12557b-146c746b-12557b@127.0.0.11
(ESTABLISHED)
CallID(C) SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1
IWF Call Leg is = SERVER
From (Server)
Realm sip172 SA=127.0.0.11
From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=113783f0-1d0010ac-13c4-12557b-426bb44b-12557b
To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SDo6d9699-0000012000088798
Contact-URI <sip:2180000@127.0.0.11:5060;transport=UDP>
To (Client)
Realm h323192fs;SA=192.168.200.29
From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d0010ac-13c4-12557b-426bb44b-12557b
To-URI
<sip:1180000@192.168.200.29:1720;acme_sa=192.168.200.29;acme_real m=h323192fs;acme_i real m=sip172;acme_i wf_i trusted>;tag=0000012000088798
Contact-URI
<sip:1180000@127.0.0.1:5070;acme_sa=192.168.200.29;acme_real m=h323192fs;acme_i wf_i trusted>
-----
Displayed 1 out of total of 1 Sessions (msg=1)
-----
ACMEPACKET#
```

Example 2: Displaying All H.323 Sessions

The following is an example of a display showing all H.323 sessions.

```
ACMEPACKET# show h323d sessions all
-----
Displaying Sessions 'all' expression ''
This may take up to 30 seconds
-----
CallID(S) SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1 ( )
CallID(C) 80834d3a4200001f0110090e2f3cc51b
IWF Call Leg is = SERVER
From (Server)
```

```

      Real m
      From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDo6d9601-113783f0-
1d0010ac-13c4-12557b-426bb44b-12557b
      To-URI      <si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>
      To (Cl ient)
      Real m      ; SA=192. 168. 200. 29
      From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDo6d9601-113783f0-
1d0010ac-13c4-12557b-426bb44b-12557b
      To-URI      <si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>
-----
Di splay ed 1 out of total of 1 Sessi ons (msg=1)
-----
ACMEPACKET#

```

Example 3: Displaying SIP Sessions for a Session Agent

The following is an example of a display showing SIP sessions for a specified session agent.

```

ACMEPACKET# show si pd sessi ons by-agent 127. 0. 0. 11
-----
Di splay i ng Sessi ons 'by-agent' expressi on '127. 0. 0. 11'
This may take up to 30 seconds
-----
      Cal l I D(S) 1139b3d8-1d0010ac-13c4-12557b-146c746b-12557b@127. 0. 0. 11
(ESTABL I SHED)
      Cal l I D(C) SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i 1
      I WF Cal l Leg i s = SERVER
      From (Server)
      Real m      si p172 SA=127. 0. 0. 11
      From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=113783f0-1d0010ac-
13c4-12557b-426bb44b-12557b
      To-URI
<si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>; tag=SDo6d9699-
0000012000088798
      Contact-URI <si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>
      To (Cl ient)
      Real m      h323192fs; SA=192. 168. 200. 29
      From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDo6d9601-113783f0-
1d0010ac-13c4-12557b-426bb44b-12557b
      To-URI
<si p: 1180000@192. 168. 200. 29: 1720; acme_sa=192. 168. 200. 29; acme_real m=h3
23192fs; acme_i real m=si p172; acme_i wf_i trusted>; tag=0000012000088798
      Contact-URI
<si p: 1180000@127. 0. 0. 1: 5070; acme_sa=192. 168. 200. 29; acme_real m=h323192
fs; acme_i wf_i trusted>
-----
Di splay ed 1 out of total of 1 Sessi ons (msg=1)
-----
ACMEPACKET#

```

Example 3: Displaying H.323 Sessions for a Session Agent

The following is an example of a display showing H.323 sessions for a specified session agent.

```

ACMEPACKET# show h323d sessi ons by-agent 192. 168. 200. 29
-----
Di splay i ng Sessi ons 'by-agent' expressi on '192. 168. 200. 29'

```

This may take up to 30 seconds

```
-----
Call ID(S)   SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i 1 ( )
Call ID(C)   80834d3a4200001f0110090e2f3cc51b
IWF Call Leg is = SERVER
From (Server)
  Realm
  From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDo6d9601-113783f0-
1d0010ac-13c4-12557b-426bb44b-12557b
  To-URI      <si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>
To (Client)
  Realm      ; SA=192. 168. 200. 29
  From-URI
<si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDo6d9601-113783f0-
1d0010ac-13c4-12557b-426bb44b-12557b
  To-URI      <si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>
-----
Di splayed 1 out of total of 1 Sessi ons (msg=1)
-----
ACMEPACKET#
```

Example 4: Displaying SIP Sessions for a Call ID

The following is an example of a display showing SIP sessions for a specified call ID.

```
ACMEPACKET# show sipd sessions by-call id A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192. 168. 11. 101

<call id>                                Call ID

< sessions by-call id A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192. 168. 11. 101
-----
Di splaying Sessi ons 'by-call id' expressi on 'A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192. 168. 11. 101'
This may take up to 30 seconds
-----
Call ID      A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192. 168. 11. 101
(ESTABLISHED)
From (Server)
  Realm      access SA=192. 168. 12. 100
  From-URI    "poza"<si p: 333@192. 168. 12. 200: 5060>; tag=43629539029921
  To-URI      <si p: 1234@192. 168. 12. 200: 5060>; tag=EE9B4A00-BFF07BF1
  Contact-URI <si p: 333@192. 168. 11. 101: 5060>
To (Client)
  Realm      core
  From-URI    "poza"<si p: 333@192. 168. 12. 200: 5060>; tag=43629539029921
  To-URI      <si p: 1234@192. 168. 12. 200: 5060>; tag=EE9B4A00-BFF07BF1
  Contact-URI <si p: 1234-
dcgkuvfb53ne8@192. 168. 12. 100: 5060; transport=udp>
-----
Call ID      A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192. 168. 11. 101
(ESTABLISHED)
From (Server)
  Realm      core
  From-URI    "poza"<si p: 333@192. 168. 12. 200: 5060>; tag=43629539029921
  To-URI      <si p: 1234@192. 168. 12. 200: 5060>; tag=EE9B4A00-BFF07BF1
  Contact-URI <si p: 333-
3sd0uq3ad3a65@192. 168. 12. 100: 5060; transport=udp>
```

```
To (Client)
  Realm      access
  From-URI    "poza" <si p: 333@192. 168. 12. 200: 5060>; tag=43629539029921
  To-URI      <si p: 1234@192. 168. 12. 200: 5060>; tag=EE9B4A00-BFF07BF1
  Contact-URI <si p: 1234@192. 168. 11. 102>
```

 Displayed 2 out of total of 2 Sessions (msg=1)

Clearing Sessions

You can clear sessions from the Net-Net SBC with the **clear-sess** command. You can clear all sessions, or you can:

- Clear sessions for a specific session agent (**by-agent**)
- Clear sessions for a specific call by using the call identifier (**by-callid**)
- Clear sessions for a specific IP address (**by-ip**, where you enter the IP address in quotation marks (" "))
- Clear sessions for a specific user by using the called or calling number (**by-user**)

Example 1: Clearing All SIP Sessions

The following is an example of clearing all SIP sessions from the Net-Net SBC.

```
ACMEPACKET# clear-sess sipd sessions all
-----
Clearing Sessions 'all' expression ''
This may take up to 30 seconds
-----
CallID(S) 1139b3d8-1d0010ac-13c4-12568b-333eb709-12568b@127. 0. 0. 11
(ESTABLISHED)
CallID(C) SDpmd9601-8a9346384f02a41972cf4e65d7b692be-v3000i 1
IWF Call Leg is = SERVER
From (Server)
  Realm      sip172 SA=127. 0. 0. 11
  From-URI    <si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=113783f0-1d0010ac-13c4-12568b-3ce7f7a6-12568b
  To-URI      <si p: 1180000@127. 0. 0. 100: 5060; transport=UDP>; tag=SDpmd9699-0000022c000a0e38
  Contact-URI <si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>
To (Client)
  Realm      h323192fs; SA=192. 168. 200. 29
  From-URI    <si p: 2180000@127. 0. 0. 11: 5060; transport=UDP>; tag=SDpmd9601-113783f0-1d0010ac-13c4-12568b-3ce7f7a6-12568b
  To-URI      <si p: 1180000@192. 168. 200. 29: 1720; acme_sa=192. 168. 200. 29; acme_real m=h323192fs; acme_i real m=sip172; acme_i wf_i trusted>; tag=0000022c000a0e38
  Contact-URI <si p: 1180000@127. 0. 0. 1: 5070; acme_sa=192. 168. 200. 29; acme_real m=h323192fs; acme_i wf_i trusted>
Clear Call [y/n]?: y
*** Call Cleared ***
-----
Cleared 1 Sessions
-----
ACMEPACKET#
```

Example 2: Clearing an H.323 Session by User

The following is an example of clearing an H.323 session for a specific user from the Net-Net SBC.

```

ACMEPACKET# clear-sess h323d sessions by-user 2180000
-----
Clearing Sessions 'by-user' expression '2180000'
This may take up to 30 seconds
-----
Call ID(S) SD70bp801-c3ab2f185aa73aca37d1fc619ec16a2f-v3000i1 ()
Call ID(C) c080c5f0c600001f0112090e2f3cc51b
IWF Call Leg is = SERVER
From (Server)
  Realm
  From-URI
<si p: 2180000@127.0.0.11: 5060; transport=UDP>; tag=SD70bp801-1138cd28-
1d0010ac-13c4-1257b5-1a5eebc4-1257b5
  To-URI <si p: 1180000@127.0.0.100: 5060; transport=UDP>
To (Client)
  Realm ; SA=192.168.200.29
  From-URI
<si p: 2180000@127.0.0.11: 5060; transport=UDP>; tag=SD70bp801-1138cd28-
1d0010ac-13c4-1257b5-1a5eebc4-1257b5
  To-URI <si p: 1180000@127.0.0.100: 5060; transport=UDP>
Clear Call [y/n]?: y
*** Call Cleared ***

Retrying the command
-----
Cleared 1 Sessions
-----
ACMEPACKET#

```


Overview

This chapter explains how to access and view statistics to help you monitor and manage Net-Net SBC performance. Gathering statistical information to help monitor system performance effectively helps you decide on the actions you need to take to correct or improve system behavior. For example, you can access statistics to monitor the calls per second capability of the Net-Net SBC and make decisions based on that information.

You can collect performance data to establish a baseline before making changes to the system. This helps determine what effect the change has on performance. You can use the baseline to compare future trends. You can collect performance data on a daily, weekly, and monthly basis for trend analysis. This allows you to pro-actively solve problems before they result in degraded performance.

Viewing System Information

This section explains how to access system level performance statistics. All the commands defined in this section are accessible in User mode.

ACLI Credit Information

Display the credit information, including the version number, for the ACLI that you are running on your Net-Net system by using the **show about** command.

```
ACMEPACKET> show about
- ACLI /Network Configuration Shell 1.0-1
ACMEPACKET>
```

User Privilege Mode

Display the current level of privilege at which the user is operating on the Net-Net system by using the **show privilege** command.

```
ACMEPACKET> show privilege
console user - privilege level 0
ACMEPACKET>
```

Privilege level 0 means the current user is in User mode and privilege level 1 means the current user is in Superuser mode.

System Uptime

Display information about the length of time the system has been running in days, hours, minutes, and seconds (as well as the current date and time) by using the **show uptime** command.

```
ACMEPACKET# show uptime
FRI SEP 06 12:57:23 2002 - up 0 days, 22 hours, 58 minutes, 57 seconds
ACMEPACKET#
```

Current Date and Time

Display the current date and time for your Net-Net system by using the **show clock** command.

```
ACMEPACKET# show clock
11:51:41 est TUE APR 03 2007
```

Software Release Current Version

Display the version information for the release, including: the version number, the date that the current copy of the OS was made, and other information by using the **show version** command.

```
ACMEPACKET# show version
ACME Net-Net 4250 Firmware C5.0.0
Build Date=05/22/07
```

Viewing System Resource Information

This section explains how to access system resource statistics.

System Memory

Display the memory statistics for the system by using the **show memory** command. It displays the number of bytes, the number of blocks, the average block size in both free and allocated memory, and the maximum block size of free memory in table form. In addition, it displays the number of blocks currently allocated, the average allocated block size, and the maximum number of bytes allocated at any given time (peak use, for example).

```
ACMEPACKET# show memory
```

status	bytes	blocks	avg block	max block

current				
free	826292736	179	4616160	825573472
al loc	211642160	3398	62284	-
i n t e r n a l	448	2	224	-
cumul at i v e				
al loc	212286912	5105	41584	-
peak				
al loc	211643792	-	-	-
Memory Errors:				
Li n k s	Repai red	0		
Paddi ng	Modi fi ed	0		
Nodes	Removed	0		
Removal	Fai l ures	0		
Fatal	Errors	0		

Listing Memory Subcommands

You can access a list of available **show memory** subcommands.

```
ACMEPACKET# show memory ?
ap p l i c a t i o n      application memory usage statistics
l 2                      layer 2 cache status
l 3                      layer 3 cache status
usage                   memory usage statistics
```

Application Object Allocation and Use

Display information about application object allocations and usage by using subcommands associated with the **show memory application** command.

ACMEPACKET# **show memory application**

14: 06: 47-153

```
Memory Statistics          -- Period -- ----- Lifetime -----
Active  High  Total      Total  PerMax  High
Processes      27    27    0        29    28    27
Messages        3     4    12     23768  298   27
Services      133   133    0       142   139   134
Sockets       120   120    0       129   126   121
Buffers       338   338    0       350   325   338
Transactions    0     0     0        22    11    11
Timed Objects 16164 16164  0     16486 16218 16176
TOQ Entries     25    25   1893   4178055 1334   37
SIP Messages    0     0     0         0     0     0
MBC Messages    0     0     0         0     0     0
Pipe Messages   30    30     0         30    30    30
Message Blocks  0     0     0         0     0     0
```

The following table lists and defines the subcommands of the **show memory application** command.

show memory application Subcommand	Description
Processes	Process object statistics
Message	Message class and all derived classes statistics
Services	Service class and all derived classes statistics
Sockets	ServiceSocket class and all derived classes statistics
Buffers	Mallocced buffers in various classes statistics
Transactions	All classes derived from the transactions template statistics
Timed Objects	TimedObject class and all derived classes statistics
TOQ Entries	Timed out queue (TOQEntry) class statistics
SIP Messages	Sip request (SipReq) and SIP response (SipResp) entry classes statistics
MBC Messages	MbcprMessage class statistics
Pipe Messages	Pipe message class statistics

Memory Buffer

Display memory buffer statistics information by using the **show buffers** command.

ACMEPACKET# **show buffers**

type number

FREE : 20990

DATA : 1

HEADER : 1

TOTAL : 20992

number of mbufs: 20992

number of times failed to find space: 0

number of times waited for space: 0

number of times drained protocols for space: 0

CLUSTER POOL TABLE

size	clusters	free	usage	min size	max size	empty
64	8192	8192	116	4	56	0
128	8192	8191	169342	128	128	0
256	2048	2047	35893	131	255	0
512	2048	2048	20357	258	512	0
1024	256	256	4	595	718	0
2048	256	256	7	1444	2048	0

The first column of the two column list shows the type of buffer, and the second column shows the number of buffers of that type. The first line of the list shows the number of buffers that are free; all subsequent lines show buffers of each type that are currently in use. Next you see four lines that describe the total number of buffers and how many times the system failed, waited, or had to empty a protocol to find space.

Following this information, the next section of the displayed information shows the cluster pool table. The **size** column lists the size of the clusters. The **clusters** column lists the total number of clusters of a certain size that have been allocated. The **free** column lists the number of available clusters of that size. The **usage** column lists the number of times that clusters have been allocated (and not the number of clusters currently in use).

Control and Maintenance Interfaces

Display all information concerning the Net-Net system's control and maintenance interfaces by using the **show interfaces** command.

ACMEPACKET# **show interfaces**

lo (unit number 0):

Flags: (0xc8049) UP LOOPBACK MULTICAST TRAILERS ARP RUNNING INET_UP INET6_UP

Type: SOFTWARE_LOOPBACK

inet: 127.0.0.1

Netmask 0xff000000 Subnetmask 0xff000000

inet6: ::1 prefixlen 128

```

Metric is 0
Maximum Transfer Unit size is 1536
0 packets received; 5262 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
0 output queue drops
wancom (unit number 0):
  Flags: (0xe8043) UP BROADCAST MULTICAST ARP RUNNING I NET_UP I NET6_UP
  Type: ETHERNET_CSMACD
  inet6: fe80::208:25ff:fe01:760%wancom0 scopeid 0x2 prefixlen 64
  inet: 172.30.55.127
  Broadcast address: 172.30.255.255
  Netmask 0xfffff0000 Subnetmask 0xfffff0000
  Ethernet address is 00:08:25:01:07:60
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  259331 unicast packets received
  2069 unicast packets sent
  0 non-unicast packets received
  5 non-unicast packets sent
  0 incoming packets discarded
  0 outgoing packets discarded
  0 incoming errors
  0 outgoing errors
  0 unknown protos
  0 collisions; 0 dropped
  0 output queue drops
f00 (media slot 0, port 0)
  Flags: Down
  Type: GIGABIT_ETHERNET
  Admin State: enabled
  Auto Negotiation: enabled
  Internet address: 10.10.0.10 Vlan: 0
  Broadcast Address: 10.10.255.255
  Netmask: 0xfffff0000
  Gateway: 10.10.0.1
  Ethernet address is 00:08:25:01:07:64
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  0 packets received
  0 packets sent
  0 non-unicast packets received
  0 non-unicast packets sent
  0 unicast packets received

```

```

0 unicast packets sent
0 input discards
0 input unknown protocols
0 input errors
0 output errors
0 collisions; 0 dropped
f01 (media slot 1, port 0)
  Flags: Down
  Type: GIGABIT_ETHERNET
  Admin State: enabled
  Auto Negotiation: enabled
  Internet address: 10.10.0.11      Vlan: 0
  Broadcast Address: 10.10.255.255
  Netmask: 0xffff0000
  Gateway: 10.10.0.1
  Ethernet address is 00:08:25:01:07:6a
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  0 packets received
  0 packets sent
  0 non-unicast packets received
  0 non-unicast packets sent
  0 unicast packets received
  0 unicast packets sent
  0 input discards
  0 input unknown protocols
  0 input errors
  0 output errors
  0 collisions; 0 dropped

```

The following information is listed for each interface:

- Internet address
- broadcast address
- netmask
- subnet mask
- Ethernet address
- route metric
- maximum transfer unit
- number of octets sent and received
- number of packets sent and received
- number of input discards
- number of unknown protocols
- number of input and output errors
- number of collisions

- number of drops
- flags (such as loopback, broadcast, promiscuous, ARP, running, and debug)

This command also displays information for loopback (internal) interfaces, which are logical interfaces used for internal communications.

You can also view key running statistics about the interfaces within a single screen by using the **show interfaces [brief]** command.

For example:

```
ACMEPACKET# show interfaces brief
```

Slot Num	Port Num	Vlan ID	Interface Name	IP Address	Gateway Address	Admin State	Oper State
----	----	----	-----	-----	-----	-----	-----
----	----	----	-----	-----	-----	-----	-----

```

lo (unit number 0):
  Flags: (0xc8049) UP LOOPBACK MULTI CAST TRAI LERS ARP RUNNI NG I NET_UP
I NET6_U
P
  Type: SOFTWARE_LOOPBACK
  inet: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  inet6: ::1 prefixlen 128
  Metric is 0
  Maximum Transfer Unit size is 1536
  238 packets received; 238 packets sent
  0 mul ti cast packets received
  0 mul ti cast packets sent
  0 i nput errors; 0 output errors
  0 col li sions; 0 dropped
  0 output queue drops
wancom (unit number 0):
  Flags: (0xe8043) UP BROADCAST MULTI CAST ARP RUNNI NG I NET_UP
I NET6_UP
  Type: ETHERNET_CSMACD
  inet6: fe80::208:25ff:fe02:2280%wancom0 scopeid 0x2 prefixlen 64
  inet: 172.30.1.186
  Broadcast address: 172.30.255.255
  Netmask 0xfffff0000 Subnetmask 0xfffff0000
  Ethernet address is 00:08:25:02:22:80
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  638311 uni cast packets received
  129 uni cast packets sent
  0 non-uni cast packets received
  5 non-uni cast packets sent
  0 i ncoming packets discarded
  0 outgoi ng packets discarded
  0 i ncoming errors
  0 outgoi ng errors
  21 unknown protos
  0 col li sions; 0 dropped
  0 output queue drops

```

```

sp (unit number 0):
  Flags: (0x68043) UP BROADCAST MULTICAST ARP RUNNING INET_UP
  Type: ETHERNET_CSMACD
  inet: 1.0.2.3
  Broadcast address: 1.0.2.255
  Netmask 0xff000000 Subnetmask 0xffffffff00
  Ethernet address is 00:08:25:02:22:84
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  0 unicast packets received
  0 unicast packets sent
  0 non-unicast packets received
  0 non-unicast packets sent
  0 incoming packets discarded
  0 outgoing packets discarded
  0 incoming errors
  0 outgoing errors
  0 unknown protocols
  0 collisions; 0 dropped
  0 output queue drops
  0 0 0 lefty 192.168.50.1/24 192.168.0.1 up down
  1 0 0 righty 192.168.50.5/24 192.168.0.1 up down
-----

```

Viewing Active Processes

This section explains how to display statistics for active processes by displaying the task information for the Net-Net system. By using the **show processes** command, you can view the Net-Net system tasks in a table.

The information in this table is useful not only for viewing the process running on the system, but also for obtaining task names and identification numbers (TIDs in this table) for carrying out **notify** and **stop-task** commands.

This table contains the following information: names of tasks, entries, task identification codes, priority of a task, status, program counter, error numbers, and protector domain identification.

ACMEPACKET# **show processes**

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
-----	-----	-----	-----	-----	-----	-----	-----	-----
tJobTask	1934484	6704870	0	PEND	19e33dc	6707ed0	0	0
tExcTask	1933408	26c6458	0	PEND	19e33dc	26ca1f0	0	0
tLogTask	logTask	6704d30	0	PEND	19e0ac8	6711e90	0	0
tNbiloLog	19354e8	670ebc0	0	PEND	19e33dc	671aef0	0	0
tWatchDog	435fc	698b9c0	0	DELAY	19ea2c0	699df68	0	3943
tNpwbTmr	160a690	18793830	0	DELAY	19ea2c0	187c6f40	0	77
ubsec_bh_h>	167b8f0	13155990	1	PEND	19e33dc	13168f40	0	0
tClisSHO	_Z4acl i P11ta	1be38940	1	PEND	19e33dc	1324e820	44	0

tCl i SSH1	_Z4acl i P11ta	1be88cd0	1	PEND	19e33dc 1be9a820	44	0
tCl i SSH2	_Z4acl i P11ta	1be89c70	1	PEND	19e33dc 1bead820	44	0
tCl i SSH3	_Z4acl i P11ta	1be9c010	1	PEND	19e33dc 1bec0820	44	0
tCl i SSH4	_Z4acl i P11ta	1be9cbc0	1	PEND	19e33dc 1bed6820	44	0
tCl i 33837	_ZN12cl i l nte	1bedb940	1	PEND+T	19e33dc 1bf02620	3d0004	
tCl i Tnet1 0	_ZN12cl i l nte	1bef1ce0	1	READY	f94e7c 1bf17050	3d0002	
tCl i Tnet2	_ZN12cl i l nte	1bf07ca0	1	PEND	19e33dc 1bf2f7f0	9	0
tCl i Tnet3	_ZN12cl i l nte	1bf1ec90	1	PEND	19e33dc 1bf457f0	44	0
tCl i Tnet4	_ZN12cl i l nte	1bf4b4c0	1	PEND	19e33dc 1bf5c7f0	44	0
tCl i Tnet5	_ZN12cl i l nte	1bf62090	1	PEND	19e33dc 1bf737f0	44	0
tWdbTask	wdbTask	130c4930	3	PEND	19e33dc 130c7ee0	0	0
tErftTask	183ea10	6979d90	10	PEND	19e3c20 697cf40	0	0
tAi ol oTask>	ai ol oTask	6952960	50	PEND	19e3c20 6967f20	0	0
tAi ol oTask>	ai ol oTask	6952cf0	50	PEND	19e3c20 6974f20	0	0
tNetTask	netTask	6a344f0	50	PEND	19e33dc 6a38f30	0	0
tXbdServi c> 895	192e5c0	130d3a20	50	PEND+T	19e3c20 130e6f40	3d0004	
tXbdServi c> 768	192e5c0	13136f20	50	PEND+T	19e3c20 13139f40	3d0004	
tAi oWai t	ai oWai tTask	69524d0	51	PEND	19e33dc 695aec0	0	0
tPortmapd	portmapd	13046650	54	PEND	19e33dc 1304eec0	16	0
tl dma l nt	i dma5700l ntT	132b2ac0	55	PEND	19e0ac8 1806bf18	0	0
tSSH 289	SSH_startSer	1beaf140	55	PEND+T	19e33dc 1beece50	3d0004	
tTel netd	tel netd	1bf624c0	55	PEND	19e33dc 1bf81e60	0	0
tTel netOut> 0	tel netOutTas	1c17fab0	55	READY	19e3210 1c16dca0	0	
tTel net l n_> 0	tel net l nTask	1c0ecb60	55	PEND	19e33dc 1c0f5ba0	0	
tFtp6d	f78730	13046aa0	56	PEND	19e33dc 13058e30	0	0
tBrokerd 0	_Z7brokerdPc	132635e0	60	PEND	19e0ac8 13274b30	3d0002	
tNpFrmTx	app_send_tas	18774200	60	PEND	19e33dc 1877aea0	0	0
tNpFrmRx	app_frame_rx	187746e0	60	PEND	19e33dc 1878eec0	0	0
tNpCel l Rx	app_cel l _rx_	18774b10	60	PEND	19e33dc 18799ec0	0	0
tNpDmaTx	app_i dma_sen	18788b30	60	PEND	19e0ac8 187afef0	0	0
tNpwbNpmRx 0	npwbNpmRxTas	18793b80	60	PEND	19e0ac8 187d1ee0	0	
tl pFrag	15e73a4	188278e0	60	PEND	19e0ac8 18879e10	0	0
ti fXCheck 12722	i fXUpdate	1bd4d2a0	60	DELAY	19ea2c0 1bd58df0	3d0002	
tAl arm	404fa0	1bd66740	60	DELAY	19ea2c0 1bd71be0	0	868
tNpDmaRx 2713	app_i dma_fra	18788890	61	PEND+T	19e33dc 187a4ed0	3d0004	
tArpMgr	arp_manager_	187e5500	61	PEND	19e0ac8 18822bb0	0	0
tArpTmr 622	arp_manager_	1881cd00	61	DELAY	19ea2c0 1882dee0	0	
tPktCapMgr	pktcpt_mai n	18a27940	61	PEND	19e0ac8 18a38ec0	0	0

tFlowGdTmr 17151	nApp_fg_mai	18873850	62	PEND+T	19e33dc 18a2dec0	0	
tSysmand 32382	sysmand	13155d60	75	PEND+T	19e33dc 13178910	3d0004	
tAtcpd 181	_Z5atcpdPcP9	18ada4d0	75	PEND+T	19e33dc 18aebcd0	3d0004	
tSecured 32374	_Z7manual dPc	1ba472c0	75	PEND+T	19e33dc 1bac1cf0	3d0004	
tMbcd 2371	_Z11mbcd_dae	1b34afe0	78	PEND+T	19e33dc 1b35cac0	3d0004	
tEbmd 32365	_Z11ebmd_dae	1b856ba0	78	PEND+T	19e33dc 1b867820	3d0004	
tLi d 32361	_Z9l i _daemon	1b59db10	80	PEND+T	19e33dc 1b5ae8b0	3d0004	
tAl gd 32359	_Z11al gd_dae	1b69e570	80	PEND+T	19e33dc 1b6afae0	3d0004	
tSi pd 2355	_Z4si pdPcP9s	1b89dfd0	80	PEND+T	19e33dc 1b8b7b80	3d0004	
tLrtd 32350	_Z4l rtdPcP9s	1b938740	80	PEND+T	19e33dc 1b949c80	3d0004	
tH323d 2345	_Z5h323dPcP9	1b990570	80	PEND+T	19e33dc 1b9a1ca0	3d0004	
tH248d 32339	_Z5h248dPcP9	1b9c56c0	80	PEND+T	19e33dc 1b9d6cc0	3d0004	
tRadd 32334	_Z4raddPcP9s	1b6e6790	82	PEND+T	19e33dc 1b6f7d30	3d0004	
tPusher 32333	_Z6pusherPcP	1b824c60	82	PEND+T	19e33dc 1b8357e0	3d0004	
tAndMgr 105	AND_start	132b1f10	95	PEND+T	19e0ac8 132bde60	3d0004	
tCol l ect 2395	_Z7col l ectPc	18aac4f0	97	PEND+T	19e33dc 18abdd20	3d0004	
tSnmpd 32322	snmpd	1bae1760	97	PEND+T	19e33dc 1baf2d40	3d0004	
tLemd 32321	_Z4l emdPcP9s	18a6e400	99	PEND+T	19e33dc 18a7fb80	3d0004	
tAtcpApp 32317	_Z11atcpAppT	18b0c290	99	PEND+T	19e33dc 18b1dd30	3d0004	
tTffsPTask	fl Pol l Task	6982a60	100	READY	19ea2c0 6986f60	0	0
tDumper	tDumperMai n	13229260	100	PEND	19e33dc 1322ef20	0	0
tTaskCheck 37	taskCheckMai	132295f0	100	DELAY	19ea2c0 13238f30	160068	
tCl i Worker 0	_Z13cl i Worke	18a40470	100	PEND	19e33dc 18a51f20	0	
tPanel	26510	6984010	251	PEND	19e0ac8 698ef18	0	0
tl d l e	2e93bc	6984c10	255	READY	2e93c0 6995f90	0	0

Accessing Process Subcommands

Display the help text for the **show processes** command to access the following subcommands:

ACMEPACKET# **show processes ?**

acl i Console	acl i Console process statistics
acl i SSH0	acl i SSH0 process statistics
acl i SSH1	acl i SSH1 process statistics
acl i SSH2	acl i SSH2 process statistics
acl i SSH3	acl i SSH3 process statistics
acl i SSH4	acl i SSH4 process statistics
acl i Tel net0	acl i Tel net0 process statistics
acl i Tel net1	acl i Tel net1 process statistics
acl i Tel net2	acl i Tel net2 process statistics
acl i Tel net3	acl i Tel net3 process statistics
acl i Tel net4	acl i Tel net5 process statistics
al gd	al gd process statistics
all	display statistics for all processes
berpd	berpd process statistics
brokerd	brokerd process statistics
cliWorker	cliWorker process statistics
collect	Collector process statistics
cpu	display CPU Usage
current	current process statistics
ebmd	ebmd process statistics
h323d	h323d process statistics
lcmd	lcmd process statistics
lid	lid process statistics
mbcd	mbcd process statistics
pusher	pusher process statistics
radd	radd process statistics
si pd	si pd process statistics
snmpd	snmpd process statistics
sysmand	sysmand process statistics
total	total process statistics

The following table lists and defines the subcommands and additional capabilities of the **show processes** command.

show processes Subcommand	Description
sysmand	Statistics for the sysmand process, which is related to the system startup tasks. sysmand starts and keeps track of many of the system tasks. All application tasks send their system log messages to the sysmand task and all notify requests go through sysmand.
lcmd	Statistics for the local element management (lcmd) process, which is responsible for maintaining and providing local and remote access to data (including configuration and policy data) stored in the system.
brokerd	Statistics for the brokerd process, which is a log concentrator and sequencer used for forwarding path and hardware monitor tasks.
mbcd	Statistics for the mbcd process, which is the process for the middlebox control daemon. It provides signalling applications with the ability to dynamically manage (create, modify, delete, and receive flow event notifications) NAT entries (pinholes) for media flows via the MIBOCO protocol.

show processes Subcommand	Description
algd	Statistics for the algd process, which is the process for the application layer gateway. It processes the application-specific intelligence and knowledge of its associated middlebox function. It assists in the performance of NAT of the application layer so applications can transparently operate through NATs. algd is responsible for processing MGCP messages. It NATs the Layer 5 signaling content (MGCP message headers for example) and manages the associated media flow via tMBCD.
sipd	Statistics for sipd process statistic, which acts as a SIP server that receives and forwards them on the behalf of the requestor. sipd is responsible for processing SIP (RFC 3261) messages. It NATs the Layer 5 signaling content (for example, SIP message headers) and manages the associated media flows via tMBCD.
current	Current statistics for all processes.
total	Total statistics for all processes.
all	All statistics for all processes.
cpu	Percentage of CPU utilization by all processes.

Viewing Statistics for all Processes

Display the statistics for all processes by using the **show processes all** command.

ACMEPACKET# show processes all

```

12: 05: 39-79
Process Svcs      Rcvd      Sent      Events  Al arm    S log    Pl og    CPU Max
12: 05: 09-150 (sysmand) ID=13155d60
Process Status      -- Period -- ----- Li fetime -----
                Active  High  Total      Total  PerMax    High
Services          29    29    0         29     29      29
Messages           0     1    12        35909  322     3
Transactions       0     0     0          0     0     0
Timed Objects     31    31     0         31     31    31
Total Buffers     10    10     0         10     5     10
Alloc Buffers      5     5     0          95    33     7
Memory Chunks     83    84    12        35947  390    84
TOQ Entries        2     2     1         5326   4      2
Operations                    16        44721  310
Messages Received          12        35853  296
Messages Sent              0         45    15
Partial Message            0          0     0
Partial Msg Expired        0          0     0
Partial Msg Dropped        0          0     0
Timed Events              1         5324   2
Alarms                    0          0     0
System Logs              0          11    11
Process Logs             0          58    55
Load Rate                    0.0          0.4
CPU Usage                  0.0        11.868/531797

```

```

08: 23: 17-37 (acl i SSH0) ID=1be38940
Process Status      -- Period -- ----- Li fetime -----
                Active  High  Total      Total  PerMax    High

```

Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.000/531814		

17: 19: 33-113 (brokerd) ID=132635e0

Process	Status	-- Period --		----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	2	2	0	2	2	2
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	2	2	0	2	2	2
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	11	11	0	11	11	11
TOQ Entries	0	0	0	0	0	0
Operations			8	41	31	
Messages Received			3	20	16	
Messages Sent			0	4	4	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	3	3	
System Logs			0	4	4	
Process Logs			0	4	4	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.006/531829		

09: 32: 34-194 (cliWorker) ID=18a40470

Process	Status	-- Period --		----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	2	2	0	2	2	2
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	2	3	1	6	2	3
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0

Memory Chunks	10	11	1	14	10	11
TOQ Entries	0	1	1	4	1	1
Operations			2	13	2	
Messages Received			0	0	0	
Messages Sent			0	2	1	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	5	4	
Process Logs			0	6	4	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.013/531845		

12:06:39-140 (lcmd) ID=18a6e400

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	5	5	0	5	5	5
Messages	0	0	0	10	5	6
Transactions	0	0	0	3	2	2
Timed Objects	6	6	0	15	9	10
Total Buffers	10	10	0	10	5	10
Alloc Buffers	5	5	0	9	4	7
Memory Chunks	78	78	0	91	62	86
TOQ Entries	0	0	0	6	3	3
Operations			3	8874	5	
Messages Received			0	5	2	
Messages Sent			0	28	21	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	3	2	
Alarms			0	0	0	
System Logs			0	26	18	
Process Logs			0	36	22	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.378/531858		

12:06:54-155 (collect) ID=18aac4f0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	3	3	0	6	6	5
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	12	12	0	14	14	14
TOQ Entries	0	0	0	2	2	1
Operations			35	115198	22	
Messages Received			0	1	1	
Messages Sent			0	6	6	

Partial Message	0	0	0
Partial Msg Expired	0	0	0
Timed Events	0	0	0
Alarms	0	0	0
System Logs	0	8	8
Process Logs	0	8	8
Load Rate	0.0		0.0
CPU Usage	0.0	2.545/531872	

12:07:11-171 (atcpd) ID=18ada4d0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	5	5	0	5	5	5
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	6	6	0	12	12	8
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	41	41	0	59	59	43
TOQ Entries	1	1	342	1059444	201	2
Operations			346	1068224	202	
Messages Received			0	1	1	
Messages Sent			0	8	8	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			342	1059436	201	
Alarms			0	0	0	
System Logs			0	10	10	
Process Logs			0	12	12	
Load Rate			0.0		0.0	
CPU Usage		0.0		35.711/531883		

12:06:39-140 (atcpApp) ID=18b0c290

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	0	4	4	4
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	7	7	6
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	14	14	0	16	16	16
TOQ Entries	0	0	0	2	2	1
Operations			3	8867	4	
Messages Received			0	1	1	
Messages Sent			0	5	5	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	7	7	
Process Logs			0	8	8	

Load Rate	0.0	0.0
CPU Usage	0.0	0.247/531905

12: 07: 39-100 (mbcd) ID=1b34afe0

Process Status	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Servi ces	9	9	0	9	9	9
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	16012	16012	0	16019	16019	16014
Total Buffers	10	10	0	10	10	10
Al loc Buffers	8	8	0	10	10	10
Memory Chunks	54	54	0	86	86	56
T0Q Entries	2	2	5	23060	15	3
Operations			5	21279	6	
Messages Recei ved			0	1	1	
Messages Sent			0	30	30	
Partial Message			0	0	0	
Partial Msg Expi red			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			5	23049	5	
Al arms			0	0	0	
System Logs			0	32	32	
Process Logs			0	38	38	
Load Rate			0.0		0.0	
CPU Usage		0.0		1.144/531917		

12: 07: 39-100 (l id) ID=1b59db10

Process Status	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Servi ces	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	4	4	4
Total Buffers	5	5	0	5	5	5
Al loc Buffers	3	3	0	3	3	3
Memory Chunks	12	12	0	13	13	13
T0Q Entries	0	0	0	1	1	1
Operations			2	8867	3	
Messages Recei ved			0	1	1	
Messages Sent			0	6	6	
Partial Message			0	0	0	
Partial Msg Expi red			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Al arms			0	0	0	
System Logs			0	8	8	
Process Logs			0	8	8	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.206/531930		

12: 07: 39-100 (al gd) ID=1b69e570

Process Status	-- Period --			----- Li fetime -----		
----------------	--------------	--	--	-----------------------	--	--

	Active	High	Total	Total	PerMax	High
Services	5	5	0	6	6	5
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	7	7	0	17	17	10
Total Buffers	10	10	0	10	10	10
Alloc Buffers	5	5	0	7	7	7
Memory Chunks	47	47	0	81	81	49
TOQ Entries	1	1	1	5328	10	2
Operations			3	12415	5	
Messages Received			0	1	1	
Messages Sent			0	9	9	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			1	5320	2	
Alarms			0	0	0	
System Logs			0	11	11	
Process Logs			0	13	13	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.550/531940		

12:07:39-100 (radd) ID=1b6e6790

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	7	7	6
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	14	14	0	18	18	16
TOQ Entries	1	1	1	5328	10	2
Operations			3	12415	5	
Messages Received			0	1	1	
Messages Sent			0	9	9	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			1	5320	2	
Alarms			0	0	0	
System Logs			0	11	11	
Process Logs			0	13	13	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.550/531940		

12:07:39-100 (radd) ID=1b6e6790

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	7	7	6
Total Buffers	5	5	0	5	5	5

Alloc Buffers	2	2	0	4	4	4
Memory Chunks	14	14	0	18	18	16
TOQ Entries	1	1	1	5321	3	2
Operations			3	14185	4	
Messages Received			0	1	1	
Messages Sent			0	9	9	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			1	5318	2	
Alarms			0	0	0	
System Logs			0	11	11	
Process Logs			0	11	11	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.358/531957		

12:07:39-100 (pusher) ID=1b824c60

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	3	3	0	6	6	5
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	11	11	0	13	13	13
TOQ Entries	0	0	0	2	2	1
Operations			2	8868	4	
Messages Received			0	1	1	
Messages Sent			0	6	6	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	8	8	
Process Logs			0	8	8	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.232/531987		

12:08:39-160 (ebmd) ID=1b856ba0

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	5	5	0	5	5	5
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	7	7	0	16	16	9
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	56	56	0	102	102	58
TOQ Entries	2	2	2	10654	18	3
Operations			4	12417	6	
Messages Received			0	1	1	

Messages Sent	0	9	9
Partial Message	0	0	0
Partial Msg Expired	0	0	0
Partial Msg Dropped	0	0	0
Timed Events	2	10640	4
Alarms	0	0	0
System Logs	0	11	11
Process Logs	0	11	11
Load Rate	0.0		0.0
CPU Usage	0.0	0.445/532002	

12: 09: 19-100 (sipd) ID=1b89dfd0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	5	5	0	5	5	5
Messages	0	0	0	6	4	3
Transactions	0	0	0	0	0	0
Timed Objects	7	7	0	14	11	9
Total Buffers	5	5	0	5	5	5
Alloc Buffers	3	3	0	7	4	5
Memory Chunks	48	48	0	82	79	50
TOQ Entries	2	2	11	58529	19	4
Operations			11	53204	12	
Messages Received			0	3	2	
Messages Sent			3	17750	30	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			11	58519	12	
Alarms			0	0	0	
System Logs			3	17750	32	
Process Logs			3	17753	35	
Load Rate			0.0		0.0	
CPU Usage		0.0		8.164/532015		

12: 08: 39-160 (Irted) ID=1b938740

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	0	4	4	4
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	4	4	4
Total Buffers	5	5	0	5	5	5
Alloc Buffers	3	3	0	3	3	3
Memory Chunks	15	15	0	18	18	16
TOQ Entries	0	0	0	1	1	1
Operations			3	8868	3	
Messages Received			0	1	1	
Messages Sent			0	5	5	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	

System Logs	0	7	7
Process Logs	0	10	10
Load Rate	0.0		0.0
CPU Usage	0.0	0.247/532030	

12: 09: 49-130 (h323d) ID=1b990570

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	6	6	0	6	6	6
Messages	0	0	0	3	3	2
Transactions	0	0	0	0	0	0
Timed Objects	9	9	0	19	19	9
Total Buffers	10	10	0	10	10	10
Alloc Buffers	6	6	0	6	6	6
Memory Chunks	133	133	0	170	170	134
TOQ Entries	3	3	19	79815	25	4
Operations			14	53203	10	
Messages Received			0	1	1	
Messages Sent			4	17790	72	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			19	79802	16	
Alarms			0	0	0	
System Logs			4	17792	74	
Process Logs			4	17798	80	
Load Rate			0.0		0.0	
CPU Usage		0.0		8.668/532048		

12: 09: 39-120 (h248d) ID=1b9c56c0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	2	2	0	2	2	2
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	3	3	0	3	3	3
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	11	11	0	49	49	30
TOQ Entries	1	1	1	5322	3	1
Operations			4	12416	3	
Messages Received			0	0	0	
Messages Sent			0	24	24	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			1	5321	2	
Alarms			0	0	0	
System Logs			0	27	27	
Process Logs			0	27	27	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.301/532093		

12: 10: 39-180 (secured) ID=1ba472c0

Process Status		-- Period --		----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	5	5	0	5	5	5
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	5	5	0	11	11	7
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	43	43	0	65	65	45
TOQ Entries	0	0	0	7	7	1
Operations			4	8871	4	
Messages Received			0	1	1	
Messages Sent			0	6	6	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	8	8	
Process Logs			0	10	10	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.258/532104		

12: 10: 39-180 (snmpd) ID=1bae1760

Process Status		-- Period --		----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	0	4	4	4
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	4	4	0	7	7	6
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	16	16	0	22	22	18
TOQ Entries	0	0	0	2	2	1
Operations			4	8871	4	
Messages Received			0	1	1	
Messages Sent			0	7	7	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	9	9	
Process Logs			0	9	9	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.244/532118		

08: 23: 17-37 (acl SSH1) ID=1be88cd0

Process Status		-- Period --		----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5

Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	

CPU Usage 0.0 0.000/532127

08:23:17-37 (accliSSH2) ID=1be89c70

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	

CPU Usage 0.0 0.000/532143

08:23:17-37 (accliSSH3) ID=1be9c010

Process Status	-- Period --			----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	

Partial Msg Expired	0	0	0
Partial Msg Dropped	0	0	0
Timed Events	0	0	0
Alarms	0	0	0
System Logs	6	6	6
Process Logs	6	6	6
Load Rate	0.0		0.0
CPU Usage	0.0		0.000/532143

08:23:17-37 (acl SSH3) ID=1be9c010

Process Status	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Servi ces	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Al loc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Recei ved			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expi red			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	
CPU Usage		0.0			0.000/532170	

08:23:17-37 (acl SSH4) ID=1be9cbc0

Process Status	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Servi ces	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Al loc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Recei ved			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expi red			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	

Process Logs	6	6	6
Load Rate	0.0		0.0
CPU Usage	0.0		0.000/532344

12: 14: 39-120 (acl i Console) ID=1bedb940

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	3	3	0	3	3	3
Messages	0	0	0	2	2	2
Transactions	0	0	0	0	0	0
Timed Objects	5	5	0	8	5	7
Total Buffers	5	5	0	5	5	5
Alloc Buffers	2	2	0	4	4	4
Memory Chunks	15	15	0	18	13	15
TOQ Entries	0	0	0	2	1	1
Operations			3	10517	177	
Messages Received			0	1	1	
Messages Sent			0	16	6	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			0	18	6	
Process Logs			0	18	6	
Load Rate			0.0		0.0	
CPU Usage		0.0			0.450/532357	

12: 05: 39-179 (acl i Telnet0) ID=1bef1ce0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	0	4	4	4
Messages	0	0	0	43	7	5
Transactions	0	0	0	0	0	0
Timed Objects	5	5	0	68	6	7
Total Buffers	10	10	0	10	5	10
Alloc Buffers	5	5	0	37	4	7
Memory Chunks	90	90	0	147	77	92
TOQ Entries	0	0	0	45	6	1
Operations			42	21969	498	
Messages Received			0	22	5	
Messages Sent			0	92	15	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	3	1	
Alarms			0	0	0	
System Logs			0	73	12	
Process Logs			0	73	12	
Load Rate			0.0		0.4	
CPU Usage		0.0			19.778/532371	

14: 04: 54-134 (acl i Telnet1) ID=1bf07ca0

Process Status	-- Period --			----- Li fetime -----		
Active	High	Total	Total	PerMax	High	
Services	4	4	0	4	4	4
Messages	1	1	1	10	5	2
Transactions	0	0	0	0	0	0
Timed Objects	6	7	2	10	5	7
Total Buffers	5	5	0	5	5	5
Alloc Buffers	5	5	0	7	4	5
Memory Chunks	15	15	1	22	13	15
TOQ Entries	1	1	1	3	1	1
Operations			4	662	282	
Messages Received			0	6	4	
Messages Sent			4	20	6	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			3	16	6	
Process Logs			3	16	6	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.129/532384		

08: 23: 17-37 (acl iTel net2) ID=1bf1ec90

Process Status	-- Period --			----- Li fetime -----		
Active	High	Total	Total	PerMax	High	
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.000/532397		

08: 23: 17-37 (acl iTel net3) ID=1bf4b4c0

Process Status	-- Period --			----- Li fetime -----		
Active	High	Total	Total	PerMax	High	
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0

Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.000/532435		

08: 23: 17-37 (acl iTel net4) ID=1bf62090

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	4	4	4	4	4	4
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	5	5	5	5	5	5
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	13	13	13	13	13	13
TOQ Entries	1	1	1	1	1	1
Operations			1	1	1	
Messages Received			0	0	0	
Messages Sent			3	3	3	
Partial Message			0	0	0	
Partial Msg Expired			0	0	0	
Partial Msg Dropped			0	0	0	
Timed Events			0	0	0	
Alarms			0	0	0	
System Logs			6	6	6	
Process Logs			6	6	6	
Load Rate			0.0		0.0	
CPU Usage		0.0		0.000/532454		

08: 24: 43-23 (tTaskCheck) ID=132295f0

Process Status	-- Period --			----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Services	0	0	0	0	0	0
Messages	0	0	0	0	0	0
Transactions	0	0	0	0	0	0
Timed Objects	0	0	0	0	0	0
Total Buffers	0	0	0	0	0	0
Alloc Buffers	0	0	0	0	0	0
Memory Chunks	4	4	4	4	4	4
TOQ Entries	0	0	0	0	0	0
Operations			1	1	1	

Messages Received	0	0	0
Messages Sent	0	0	0
Partial Message	0	0	0
Partial Msg Expired	0	0	0
Partial Msg Dropped	0	0	0
Timed Events	0	0	0
Alarms	0	0	0
System Logs	0	0	0
Process Logs	0	0	0
Load Rate	0.0		0.0
CPU Usage	0.0		0.000/532474

Viewing Totals for all Processes

Display total statistics for all processes by using the **show processes total** command.

ACMEPACKET# **show processes total**

12: 32: 34-94

Process	Svcs	Rcvd	Sent	Events	Al arm	Sl og	Pl og	CPU Max	
sysmand	29	35961	45	5340	0	11	58	0.0	0
acl i SSH0	4	0	3	0	0	6	6	0.0	0
brokerd	2	20	4	0	3	4	4	0.0	0
cli Worke	2	0	2	0	0	5	6	0.0	0
lcmd	5	5	28	3	0	26	36	0.0	0
collect	3	1	6	0	0	8	8	0.0	0
atcpd	5	1	8	1062468	0	10	12	0.0	0
atcpApp	4	1	5	0	0	7	8	0.0	0
mbcd	9	1	30	23112	0	32	38	0.0	0
lid	3	1	6	0	0	8	8	0.0	0
algd	6	1	9	5334	0	11	13	0.0	0
radd	3	1	9	5333	0	11	11	0.0	0
pusher	3	1	6	0	0	8	8	0.0	0
ebmd	5	1	9	10668	0	11	11	0.0	0
sipd	5	3	17796	58671	0	17796	17799	0.0	0
lrtd	4	1	5	0	0	7	10	0.0	0
h323d	6	1	17835	80005	0	17837	17843	0.0	0
h248d	2	0	24	5334	0	27	27	0.0	0
secured	5	1	6	0	0	8	10	0.0	0
snmpd	4	1	7	0	0	9	9	0.0	0
acl i SSH1	4	0	3	0	0	6	6	0.0	0
acl i SSH2	4	0	3	0	0	6	6	0.0	0
acl i SSH3	4	0	3	0	0	6	6	0.0	0
acl i SSH4	4	0	3	0	0	6	6	0.0	0
acl i Cons	3	1	16	0	0	18	18	0.0	0
acl i Tel n	4	22	92	3	0	73	73	0.0	0
acl i Tel n	4	6	20	0	0	16	16	0.0	0
acl i Tel n	4	0	3	0	0	6	6	0.0	0
acl i Tel n	4	0	3	0	0	6	6	0.0	0
acl i Tel n	4	0	3	0	0	6	6	0.0	0
tTaskChe	0	0	0	0	0	0	0	0.0	0

Viewing Current Statistics

Display the current statistics for all processes by using the **show processes current** command.

```
ACMEPACKET# show processes current
12: 35: 12-52
Process   Svcs   T0Q    Ops   Rcvd   Sent  Events  Al rm  SI og  PI og
CPU Now
sysmand   29     2     15    11     0     1     0     0     0  0.0  0
acI i SSH0 4     1      1     0     3     0     0     6     6  0.0  0
brokerd   2     0      8     3     0     0     0     0     0  0.0  0
cl i Worke 2     0      2     0     0     0     0     0     0  0.0  0
l emd      5     0      3     0     0     0     0     0     0  0.0  0
col l ect  3     0     34     0     0     0     0     0     0  0.0  0
atcpd     5     1    307     0     0    304     0     0     0  0.0  0
atcpApp    4     0      3     0     0     0     0     0     0  0.0  0
mbcd      9     2      7     0     0     6     0     0     0  0.0  0
l i d      3     0      3     0     0     0     0     0     0  0.0  0
al gd      6     1      4     0     0     1     0     0     0  0.0  0
radd       3     1      5     0     0     2     0     0     0  0.0  0
pusher     3     0      3     0     0     0     0     0     0  0.0  0
ebmd       5     2      4     0     0     2     0     0     0  0.0  0
si pd      5     2     16     0     5    16     0     5     5  0.0  0
l rtd       4     0      3     0     0     0     0     0     0  0.0  0
h323d      6     3     16     0     5    22     0     5     5  0.0  0
h248d      2     1      4     0     0     1     0     0     0  0.0  0
secured    5     0      3     0     0     0     0     0     0  0.0  0
snmpd      4     0      3     0     0     0     0     0     0  0.0  0
acI i SSH1 4     1      1     0     3     0     0     6     6  0.0  0
acI i SSH2 4     1      1     0     3     0     0     6     6  0.0  0
acI i SSH3 4     1      1     0     3     0     0     6     6  0.0  0
acI i SSH4 4     1      1     0     3     0     0     6     6  0.0  0
acI i Cons 3     0      3     0     0     0     0     0     0  0.0  0
acI i Tel n 4     0     48     0     0     0     0     0     0  0.0  0
acI i Tel n 4     1      4     0     4     0     0     3     3  0.0  0
acI i Tel n 4     1      1     0     3     0     0     6     6  0.0  0
acI i Tel n 4     1      1     0     3     0     0     6     6  0.0  0
acI i Tel n 4     1      1     0     3     0     0     6     6  0.0  0
tTaskChe  0     0      1     0     0     0     0     0     0  0.0  0
```

Checking Remaining Space

Check the amount of storage space is available on the flash file system on the following devices by using the **check-space-remaining** command:

- /boot
- /code
- ramdrv

For example:

```
ACMEPACKET# check-space-remaini ng boot

boot: 20127744/29760512 bytes (67%) remaini ng
ACMEPACKET# check-space-remaini ng code

code: 23214080/29760512 bytes (78%) remaini ng
ACMEPACKET# check-space-remaini ng ramdrv
```

ramdrv: 126768128/132104192 bytes (95%) remaining

Viewing Redundancy Statistics

This section explains how to check the redundancy status for Net-Net High Availability (HA) pairs by using the **show redundancy** command. Viewing the redundancy statistics provides the following information:

- General HA statistics
- Statistics related to HA transactions that have been processed
- Numerical identifier for the last redundant transaction processed (each transaction is numbered)

In an HA architecture that is functioning properly, the number for the last redundant transaction processed on a standby Net-Net SBC peer should not be far behind (if not exactly the same as) the one shown for the active Net-Net SBC peer.

The **show redundancy** command's output displays a time stamp showing when the current period began, the statistics and transactions for high availability and the numerical identifier for the last redundant transaction processed.

Accessing Redundancy Subcommands

The following example shows the **show redundancy** subcommands. You can display the redundancy statistics for the Middlebox Control (MBC), MGCP, SIP and for the configuration.

```
ACMEPACKET# show redundancy ?
```

algd	MGCP Redundancy Statistics
collect	Collect Redundancy Statistics
config	Configuration Redundancy Statistics
link	Shows Link Redundancy Configuration
mbcd	MBC Redundancy Statistics
radius-cdr	Radius CDR Redundancy Statistics
rotated-cdr	Rotated Radius CDR Redundancy Statistics
sipd	SIP Redundancy Statistics

Configuration Checkpoint Example

The following example shows the configuration checkpointing statistics you can display by using the **show redundancy config** subcommand.

```
ACMEPACKET# show redundancy config
```

```
18: 35: 05-105
```

Redundancy Statistics	Active	High	Total	Total	PerMax	High
Queued Entries	0	0	0	5	2	1
Red Records	0	0	0	5	2	2
Records Dropped	-	-	0	0	0	
Server Trans	1	1	44	593	78	27
Client Trans	0	0	0	0	0	0
Redundancy Transactions						
	Recent		Total	PerMax		
Requests received		44	593	78		

```

Duplicate requests          0          2          1
Success responses          44         593         78
Error responses             0           0           0
Request sent                0           0           0
Retransmissions sent       0           0           0
Success received            0           0           0
Errors received             0           0           0
Transaction timeouts        0           0           0
Avg Latency=0.000 for 0
Max Latency=0.000
Last redundant transaction processed: 5
ACMEPACKET#

```

About High Availability Transactions

The following table lists the redundancy statistics for the HA transactions for the Lifetime monitoring span. A standby Net-Net SBC always acts as the client side in a client-server relationship with an active Net-Net-SD peer and an active Net-Net SBC acts as the server. The standby Net-Net SBC peer always sends HA requests to its active Net-Net SBC peer, which always acts as receiver of HA transactions from the standby peer.

Statistic	Description
Queued entries	Number of transactions the active Net-Net SBC has not yet sent to its standby Net-Net SBC peer.
Red Records	Total number of HA transactions created. This set of statistics should be the same as those for <code>Queued entries</code> .
Records Dropped	Number of HA transaction records that were lost (i.e., dropped) because the standby Net-Net SBC fell behind in synchronization.
Server Trans	This statistic shows the number of HA transactions in which the Net-Net SBC acted as the server side in the client-server relationship. The active HA Net-Net SBC peer is the server.
Client Trans	This statistic shows the number of HA transactions in which the Net-Net SBC acted as the client side in the client-server relationship. The standby HA Net-Net SBC peer is the client.

Viewing Border Element Redundancy Protocol Information

You can view Border Element Redundancy Protocol statistics by using the `show berpd` command.

The border element redundancy protocol responds to alarms, advertisements, and checkpointing. This protocol manages switchovers between active and standby Net-Net SBCs and checkpoints health, media flow, and signaling state information. Using the border element redundancy protocol, HA Net-Net SBC peers communicate through their configured interfaces with User Datagram Protocol (UDP) messages.

In HA operation, each HA Net-Net SBC peer in an HA Net-Net SBC pair uses the border element redundancy protocol to advertise its current state and health so that an active peer can be elected. Using the border element redundancy protocol, HA Net-Net SBC peers communicate with UDP (advertisement or checkpoint)

messages which are sent out on one or more rear interfaces (destinations). These checkpoint messages are sent by both HA Net-Net SBC peers in the HA Net-Net SBC pair on a regular basis.

The border element redundancy protocol is sometimes referred to as “BERP” (e.g., the berpd task/process) by the internal Net-Net system components

Viewing Redundancy Health

In HA architectures, the **show health** command displays the following information:

- Health score

The health score of a Net-Net SBC is used to determine the active/standby roles of the Net-Net SBCs participating in an HA Net-Net pair architecture. The healthiest Net-Net SBC peer (the Net-Net SBC peer with the highest health score) is the active Net-Net SBC peer. The Net-Net SBC peer with the lower health score is the standby Net-Net SBC peer.

The health score is based on a 100-point scoring system. When all system components are functioning properly, the health score of the system is 100.

If the health score of an active Net-Net SBC peer drops below a configurable threshold, the standby Net-Net SBC peer takes control and initiates an automatic switchover (assumes the active role). The standby Net-Net SBC peer only takes over the active role if its own health score is greater than that of the active Net-Net SBC peer. In the case where an active Net-Net SBC's health score has reached an unsatisfactory level and therefore the standby Net-Net SBC has taken over, the Net-Net SBC that was originally active assumes the role of the standby system.

- Whether the current HA Net-Net SBC is active, standby, or out of service
- The last 20 switchover events in the switchover log

HA States

Refer to the following table for information about each potential HA state.

State	Description
Initial	HA Net-Net SBC is booting and looking for its configured peers.
BecomingActive	HA Net-Net SBC has negotiated to become the active system, but it is waiting for the length of time equal to its configured becoming-active-time to become fully active. It is important to note that packets cannot be processed in this state. An HA Net-Net SBC must be in the Active state before packet processing can occur.
Active	HA Net-Net SBC has waited for the length of time set in the becoming-active-time field and is healthy enough. This HA Net-Net SBC is handling all media flow and signaling processing.
RelinquishingActive	HA Net-Net SBC has been in the Active state, but has begun the switchover process to the Standby state. This state is very brief (i.e., the HA Net-Net SBC quickly transitions from the Active state through the RelinquishingActive state to the BecomingStandby state).
BecomingStandby	HA Net-Net SBC has negotiated to become the standby system, but is waiting to become synchronized and fully standby. It remains in this state for the length of time equal to its configured becoming-standby-time.

State	Description
Standby	HA Net-Net SBC is fully synchronized with an active peer.
OutOfService	HA Net-Net SBC is not able to synchronize with its peer within the length of time set in the becoming-standby-time field. The HA Net-Net SBC can only transition to this state from the BecomingStandby state. An active Net-Net SBC will consider its HA Net-Net SBC peer to be in this state if the peer has timed out and not sent a checkpoint message to the active peer within a time period (equal to the percent-drift value multiplied by the advertisement-time value).

Command Examples

Display information about redundancy health by using the **show health** command.
(available in User Mode)

Active

The following example shows a currently active Net-Net SBC.

```
ACMEPACKET# show health
```

```
Media Synchroni zed      enabl ed
SIP Synchroni zed        enabl ed
MGCP Synchroni zed       enabl ed
H248 Synchroni zed       enabl ed
Config Synchroni zed     enabl ed
Collect Synchroni zed    enabl ed
Radius CDR Synchroni zed enabl ed
Rotated CDRs Synchroni zed enabl ed
Active Peer Address      163. 4. 12. 2
```

```
Redundancy Protocol Process (v2):
```

```
State      Active
Health     100
Lowest Local Address  11. 0. 0. 1: 9090
```

```
1 peer(s) on 1 socket(s):
```

```
systest3B: v2, Standby, health=100, max silence=1050
last received from 11. 0. 0. 2 on wancom1: 0
```

```
Switchover Log:
```

```
Jul 11 14: 18: 21. 442: Active to RelinquishingActive
```

```
Jul 11 14: 24: 00. 872: Standby to BecomingActive, active peer
systest3B has timed out. The following example that follows shows a
currently standby Net-Net SBC.
```

Standby

The following example shows a becoming standby Net-Net SBC.

```
ACMEPACKET# show health
```

```
Media Synchroni zed      true
SIP Synchroni zed        di sabl ed
MGCP Synchroni zed       true
Config Synchroni zed     true
Active Peer Address      0. 0. 0. 0
```


Redundancy Protocol Process (v2):

```

State                               Active
Health                              100
Lowest Local Address                11.0.0.1:9090
1 peer(s) on 1 socket(s):
systest3B: v2, Standby, health=100, max silence=1050
      last received from 11.0.0.2 on wancom1:0

```

Switchover Log:

```

Jul 11 14:18:21.442: Active to RelinquishingActive
Jul 11 14:24:00.872: Standby to BecomingActive, active peer systest3B
has timed out
ACMEPACKET2#

```

The following table lists the health statistics along with a brief description.

Statistic	Description
Media Synchronized	Whether or not the media flow is synchronized for all supported protocols: SIP, H.323, and MGCP (true/false). If media flow information is not available, the Media Synchronized disabled message is displayed in the show health output.
SIP Synchronized	Whether or not SIP signaling information is synchronized (true/false). If SIP signaling is not available, the SIP Synchronized disabled message is displayed in the show health output.
MGCP Synchronized	Whether or not MGCP signaling information is synchronized (true/false). If configuration checkpointing is not available, the Config Synchronized disabled message is displayed in the show health output.
Config Synchronized	Whether or not configuration information is synchronized (true/false). If MGCP signaling is not available, the MGCP Synchronized disabled message is displayed in the show health output.
Active Peer Address	IPv4 address of the current HA Net-Net SBC's active peer (an HA Net-Net SBC that is currently active does not have an active Net-Net SBC peer and will show 0.0.0.0)

Viewing Routing Statistics

This section explains how to view the routing statistics.

Viewing Routing Table Entries

Display entries in the routing table by using the **show routes** command. The routing table displays IP layer information about the destination, mask, TOS, gateway, flags, reference count, use, interface, and protocol information.

```
ACMEPACKET# show routes
Desti nation/Pfx      Gateway           Fl ags    RefCnt Use      Proto Tos I/f

0. 0. 0. 0/0          172. 30. 0. 1    2010003  0      0        1  0 wancom0
10. 0. 0. 0/16        172. 30. 0. 1    2010003  1      0        1  0 wancom0
10. 0. 200. 164       172. 30. 0. 1    2020007  1     13801     2  0 wancom0
127. 0. 0. 1          127. 0. 0. 1     2200005  82     36220     2  0 lo0
172. 30. 0. 0/16      172. 30. 55. 127 2000101  2      0        2  0 wancom0
```

Viewing Routing Stats

Display statistics for the application layer routes shown in the routing table by using the **show route-stats** command.

```
ACMEPACKET# show route-stats
routi ng:
    0 bad routing redi rect
    3 dynami cally created route
    1 new gateway due to redi rects
    9 desti nation s found unreachable
    2 use of a wil dcard route
```

```
ACMEPACKET#
```

Testing Routing Policies

Use the **test policy** command to test application layer routes from the ACLI by specifying a *from* and *to* address. You can also specify a source realm, time of day, and carriers.

The **test-policy** command works similarly to the way a configuration element does. This command allows you to test and display local policy routes from the ACLI by specifying From and To addresses. After you have entered these addresses, use the **show** command to perform the actual lookup.

```
ACMEPACKET# test-policy ?

carriers                sets list of permitted carriers
from-address            From address list
media-profi les        list of media profiles
show                   shows local policy test results
source-realm           Source realm
time-of-day            enables/di sables time of day
to-address             To address
exit                  end test
```

The following table lists the test-policy specification formats.

Specification	Format
source-realm	A string that indicates the name set in the source-realm field of a configured local-policy element. If you enter a "*" in this specification, any configured source realms will be matched. An empty source-realm value indicates that only the "global" realm will be tested
time-of-day	A Boolean value that can be set to either enabled or disabled that indicates whether or not to use the time of day value set in the start-time and end-time fields set in configured local-policy elements
carriers	A list of comma-separated text strings enclosed in quotation marks of the names of permitted carriers set in the carriers fields set in configured local-policy elements.

Test Policy Subcommands

The following table lists and describes the **test-policy** subcommands.

test-policy Subcommand	Description
from-address	Set the From address of the local policy you want to look up/test. From addresses should be entered as SIP-URLs (e.g., sip:19785551212@netnetsystem.com).
to-address	Set the To address of the local policy you want to look up/test. To addresses should be entered as SIP-URLs (for example, sip:19785551212@netnetsystem.com).
show	Performs the actual policy lookup and shows the next hop and the associated carrier information for all routes matching the From and To addresses entered.
exit	Exits the test-policy session.

Testing Address Translations

Net-Net SBC number translation is used to change a Layer-5 endpoint name according to prescribed rules. Number translations can be performed on both the inbound and the outbound call legs independently, before and after routing occurs. Number translation is used for SIP, H.323, and SIP/H.323 interworking configurations.

ACMEPACKET# **test-translation**

called-address	called address
calling-address	calling address
show	shows local translation test results
translation-id	Translation Id
exit	end test

Viewing QoS Based Routing Statistics

You can view statistics about QoS based routing for realms, and see what realms are in service or whether a call load reduction has been applied. In the ACLI **show realms** display, the following values show you QoS based routing information:

- QoS Major Exceeded

- QoS Critical Exceeded
- QoS R-Factor Avg.

You can see these statistics in the following example of a **show realm** display:

```

ACMEPACKET# show realm
13: 34: 24-167   Realm Statistics
-- Period -- ----- Li fetime -----
Real m          Active Rate  High Total      Total PerMax  Hi gh
external      [Reduction In Call Load]
    Inbound      0  0.0    0    0          0    0    0
    Outbound     0  0.0    2    1          2    2    1
Internal     [In Service]
    Inbound      0  0.0    3    1          3    3    1
    Outbound     0  0.0    0    0          0    0    0

ACMEPACKET# show realm external
13: 33: 00-82
Realm external () [Reduction In Call Load]
-- Period -- ----- Li fetime -----
                Active   High   Total      Total  PerMax  Hi gh
Inbound Sessions    0     0     0          0     0     0
  Rate Exceeded     -     -     0          0     0     -
  Num Exceeded      -     -     0          0     0     -
  Burst Rate        0     0     0          0     0     0
  Reg Rate Exceeded -     -     0          0     0     -
  Reg Burst Rate    0     0     0          0     0     0
Outbound Sessions   0     1     2          2     2     1
  Rate Exceeded     -     -     0          0     0     -
  Num Exceeded      -     -     0          0     0     -
  Burst Rate        0     2     0          0     0     2
  Reg Rate Exceeded -     -     0          0     0     -
Out of Service      -     -     0          0     0     -
Trans Timeout       0     0     0          0     0     0
Requests Sent       -     -     0          0     0     -
Requests Complete  -     -     0          0     0     -
Sei zure            -     -     4          4     4     -
Answer              -     -     4          4     4     -
  ASR Exceeded      -     -     0          0     0     -
Requests Recei ved -     -     0          0     0     -
QoS Major Exceeded -     -     2          2     2     -
QoS Cri ti cal Exceeded -     -     0          0     0     -
Latency=0.000; max=0.000
QoS R-Factor Avg=82.39; max=93.21

```

Local Route Table Statistics and Management

This section ACLI commands that have been added so that you can troubleshooting this feature, and view monitoring statistics and other information about it.

Setting the Log Level

Log files for the local routing system task are `log.lrt` and `lrt.log`. The `lrt.log` file contains the DNS request and response communication between the system's SIP and local routing tasks.

Using the new ACLI **notify lrt** command, you can set the local routing task's log level to any of the following:

- log
- nolog
- debug
- nodebug

To set the log level for the local routing task:

1. In Superuser mode, type **notify lrt**, followed by the log level you want to set. Then press <Enter>.

```
ACMEPACKET# notify lrt log
```

Updating the Local Cache

When you want to update the cache file with new entries, delete old ones, or edit existing entries, you can refresh the local cache for a specific local routing policy.

To update the cache file for a local routing policy:

1. In Superuser mode, type **notify lrt refresh**, followed by the name of the local routing policy you want updated.

```
ACMEPACKET# notify lrt refresh lookup
```

Testing a Lookup in the Local Cache

To test a lookup in the local cache:

1. In User or Superuser mode, enter the **show enum lookup lrt=** command. After the equal sign (=), type the name of the local routing configuration you want to test followed by a <Space>. Then type in the E.164 number you want to look up, and press <Enter>.

```
ACMEPACKET# show enum lookup lrt=lookup +123
Enum Lookup Result:
Query Name -->
+123
Answers -->
sip: 123@192.168.1.191 ttl= 60
```

Displaying a Route Entry in the Local Cache

To see a route entry in the local cache:

1. In User or Superuser mode, enter the **show lrt route-entry** command. Then type in the name of the local routing configuration, a <Space>, the key you want to use, and then press <Enter>.

```
ACMEPACKET# show lrt route-entry lookup 123
```

```

UserName <123>
User Type= E164
NextHop= !^.*$! si p: 123@192. 168. 1. 191!
NextHop Type= regexp

```

Displaying Statistics for a Local Route Tables

There are two ways to see statistics for local route tables:

- Collectively—Viewing all of the statistics for all of the local route tables at once (using the **show lrt stats** command)
- Individually—Viewing the statistics for a local route table that you specify (using the **show lrt stats** command with the name of a specific local routing configuration)

The Net-Net SBC shows you the following information:

- Queries—Number of queries from the application includes those that resulted in a cache hit, and those that caused an actual query to be sent
- Success—Number of successful results; includes cache hits and queries sent
- NotFound—Number of not found results; includes cache hits and queries sent
- Number of Valid Entries—Total number of valid entries in the cache
- Number of Invalid Entries—Total number of invalid entries in the cache
- Last Modified—Date and time the cache was last modified

Resetting ENUM Statistic Counters

To clear statistics for ENUM, you can use the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the show command—by typing, for example, **show enum stats**.

The **reset** command takes the ENUM arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

You can **reset all** system statistics using the reset all command.

The ENUM example confirms successful completion of the command.

To clear ENUM statistics:

1. At the command line, type **reset enum** and then press <Enter>.

```

ACMEPACKET# reset enum
Successful reset of the ENUM Agent stats

```

Viewing SIP Protocol Performance Statistics

This section contains the commands you use to access SIP protocol statistics. These statistics provide information about the SIP protocol performance.

Accessing SIP Statistics

You can access SIP statistics for both client and server SIP transactions by using the **show sipd** command. You can then use additional subcommands to display more specific information, including specific types of SIP messages.

Example

The following example shows the output of the **show sipd** command.

```

ACMEPACKET# show sipd
14: 10: 32-178
SIP Status
-- Period -- ----- Li fetime -----
Active High Total Total PerMax High
Sessi ons 0 0 0 0 0 0
Subscri ptions 0 0 0 0 0 0
Di a l o g s 0 0 0 0 0 0
Ca l l I D Map 0 0 0 0 0 0
Rej ecti ons - - 0 0 0
Re l N V I T E s - - 0 0 0
Medi a Sessi ons 0 0 0 0 0 0
Medi a Pendi ng 0 0 0 0 0 0
Cl i e n t Trans 0 0 0 0 0 0
Se r v e r Trans 0 0 0 0 0 0
Res p Contexts 0 0 0 0 0 0
Sav e d Contexts 0 0 0 0 0 0
Soc k e t s 0 0 0 0 0 0
Req Dropped - - 0 0 0
DNS Trans 0 0 0 0 0 0
DNS Sock e t s 0 0 0 0 0 0
DNS Resul t s 0 0 0 0 0 0

Session Rate = 0.0
Load Rate = 0.0

```

The display organizes the SIP transaction statistics for the Net-Net system into two categories: Client Trans(actions) and Server Trans(actions). The remainder of the display provides information regarding dialogs, sessions, sockets, and DNS transactions.

Viewing SIP Status Information

The following example shows the output of the **show sipd status** command.

```

ACMEPACKET# show sipd status
14: 11: 15-121
SIP Status
-- Period -- ----- Li fetime -----
Active High Total Total PerMax High
Sessi ons 0 0 0 0 0 0
Subscri ptions 0 0 0 0 0 0
Di a l o g s 0 0 0 0 0 0
Ca l l I D Map 0 0 0 0 0 0
Rej ecti ons - - 0 0 0
Re l N V I T E s - - 0 0 0
Medi a Sessi ons 0 0 0 0 0 0
Medi a Pendi ng 0 0 0 0 0 0
Cl i e n t Trans 0 0 0 0 0 0
Se r v e r Trans 0 0 0 0 0 0
Res p Contexts 0 0 0 0 0 0
Sav e d Contexts 0 0 0 0 0 0
Soc k e t s 0 0 0 0 0 0
Req Dropped - - 0 0 0
DNS Trans 0 0 0 0 0 0
DNS Sock e t s 0 0 0 0 0 0
DNS Resul t s 0 0 0 0 0 0

```

Session Rate = 0.0

Load Rate = 0.0

The following table lists the SIP status statistics.

Statistic	Description
Dialogs	Number of SIP signaling connections between the Net-Net SBC and a SIP UA (for example, a call leg)
Sessions	Number of sessions established by an INVITE request. A session consists of all dialogs created by one INVITE transaction.
Sockets	Number of active SIP communication ports (the number of open UDP and TCP sockets)
DNS Transactions	Number of outstanding DNS requests

Viewing SIP Performance Statistics

The following example shows the subcommands available for the **show sipd** command.

All

Display information for many of the subcommands by using the **show sipd** command. The following information is returned:

- SIP status
- SIP media events
- SIP server transactions
- SIP client transactions
- SIP messages and events, including: INVITEs, REGISTERs, OPTIONS, CANCELs, BYEs, ACKs, INFOs, PRACKs (provisional ACKs), SUBSCRIBEs, NOTIFYs, REFERs, and UPDATEs

Note: Only statistics for those SIP messages and events that have traversed the Net-Net system will be displayed.

ACMEPACKET# **show sipd all**

15: 10: 31-138

```

State
Active High Total Total PerMax High
MGCP Sessions 24000 24000 0 24000 12935 24000
CA Endpoints 71976 71976 0 71976 38792 71976
GW Endpoints 71976 71976 0 71976 38793 71976
Media Sessions 907 1161 2351 2351 1897 1161
Client Trans 23567 23567 24121 24350 20309 23567
Server Trans 18203 18204 24993 25356 20828 18204
Pending MBCD 0 3 2351 2351 1897 3
MGCP ALGs 19 19 0 19 19 19

----- Gateway ----- Call Agent -----
MGCP Transactions ----- Lifetime ----- Lifetime -----
Recent Total PerMax Recent Total PerMax
Requests received 5718 5718 5033 19275 19638 15795
Responses sent 5716 5716 5031 19271 19633 15793
Duplicates received 23 23 20 47 48 27
Requests sent 18769 18998 15642 5352 5352 4667
Responses received 18767 18995 15640 5350 5350 4665
Retransmissions sent 47 48 27 0 0 0
15: 10: 31-138
MGCP Media Events ----- Lifetime -----
Recent Total PerMax
Calling SDP Errors 0 0 0
Called SDP Errors 0 0 0
Drop Media Errors 0 0 0
Transaction Errors 0 0 0
Application Errors 0 0 0
Media Exp Events 0 0 0
Early Media Exps 0 0 0
Exp Media Drops 0 0 0
15: 10: 31-138
MGCP ACL Status -- Period -- ----- Lifetime -----

```

	Active	High	Total	Total	PerMax	High
Total Entries	3475	3475	3247	3475	2390	3475
Trusted	2351	2351	2351	2351	1897	2351
Blocked	0	0	0	0	0	0

ACL Operations ----- Lifetime -----

	Recent	Total	PerMax
ACL Requests	2351	2351	1897
Bad Messages	0	0	0
Promotions	2351	2351	1897
Demotions	0	0	0

---< NO DATA AVAILABLE >----(RSIP)

15: 10: 31-138

----- Lifetime -----

	Recent	Total	PerMax
RQNT incoming:			
Requests received	9904	9924	8252
Replies sent	9653	9653	8156
Errors sent	232	252	154
RQNT outgoing:			
Requests sent	9672	9672	8174
Replies received	9653	9653	8156
Errors received	0	0	0

15: 10: 31-138

----- Lifetime -----

	Recent	Total	PerMax
NTFY incoming:			
Requests received	5741	5741	5053
Replies sent	5350	5350	4665
Errors sent	366	366	366
Overload 403 sent	366	366	366
NTFY outgoing:			
Requests sent	5352	5352	4667
Replies received	5350	5350	4665
Errors received	0	0	0

15: 10: 31-138

----- Lifetime -----

	Recent	Total	PerMax
CRCX incoming:			
Requests received	2356	2356	1902
Replies sent	2351	2351	1897
Errors sent	0	0	0
CRCX outgoing:			
Requests sent	2356	2356	1902
Replies received	2351	2351	1897
Errors received	0	0	0

15: 10: 31-138

----- Lifetime -----

	Recent	Total	PerMax
MDCX incoming:			
Requests received	4761	4761	3987

Replies sent	4759	4759	3985
Errors sent	0	0	0
MDCX outgoing:			
Requests sent	4761	4761	3987
Replies received	4759	4759	3985
Errors received	0	0	0

15: 10: 31-138

	Recent	Total	PerMax
----- Lifetime -----			
DLCX incoming:			
Requests received	1450	1450	1450
Replies sent	1447	1447	1447
Errors sent	0	0	0
DLCX outgoing:			
Requests sent	1450	1450	1450
Replies received	1447	1447	1447
Errors received	0	0	0

15: 10: 31-138

	Recent	Total	PerMax
----- Lifetime -----			
AUEP incoming:			
Requests received	851	1195	620
Replies sent	555	783	400
Errors sent	274	388	199
AUEP outgoing:			
Requests sent	577	807	421
Replies received	555	783	400
Errors received	0	0	0

15: 10: 31-138

	Recent	Total	PerMax
----- Lifetime -----			
Other incoming:			
Requests received	0	0	0
Replies sent	0	0	0
Errors sent	0	0	0
Other outgoing:			
Requests sent	0	0	0
Replies received	2	2	2
Errors received	0	0	0

The **show sipd** command, when issued with the appropriate message name, lets you view information about individual types of SIP messages including: INVITEs, REGISTERs, OPTIONS, CANCELs, BYEs, ACKs, INFOs, PRACKs (provisional ACKs), SUBSCRIBEs, NOTIFYs, REFERs, and UPDATEs.

- **show sipd invite**
- **show sipd ack**
- **show sipd bye**
- **show sipd register**
- **show sipd cancel**

- show sipd prack
- show sipd options
- show sipd info
- show sipd notify
- show sipd refer
- show sipd subscribe
- show sipd update
- show sipd other

Note: For each type of SIP message, only those transactions for which there are statistics will be shown.

Example

ACMEPACKET# show sipd invite

INVI TE (15: 53: 43-122)

Message/Event	Server			Client		
	Recent	Total	PerMax	Recent	Total	PerMax
INVI TE Requests	469	11132	428	469	11132	428
Retransmi ssi ons	0	0	0	0	0	0
100 Tryi ng	469	11132	428	468	10965	428
180 Ri ngi ng	467	10964	429	467	10964	429
200 OK	468	10975	430	468	11007	430
486 Busy Here	0	156	156	0	156	156
Response Retrans	0	0	0	0	0	0
Transacti on Ti meouts	-	-	-	0	0	0

Avg Latency=0.057 for 469

Max Latency=0.110

Note: If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

About the Information

The information is divided in two sections: Server and Client and includes information for recent, total, and period maximum messages or events.

- **Recent:** number of specific SIP messages and/or events that occurred within the number of seconds defined by the figure that appears directly after the time. In the example below, the Recent period of time is 76 seconds.
- **Total:** current number of SIP messages and/or events that occurred since the system was last rebooted.
- **PerMax:** maximum number of SIP messages and/or events that occurred during a single time period since the system was last rebooted.

This display also shows information regarding the average and maximum latency.

Viewing Statistics for Other SIP Methods

Display statistics for other SIP methods by using the **show sipd other** command.

SIP Monitoring by Transaction Type

You can view statistics about SIP monitoring by transaction type.

SIP Server Transactions

Display statistics SIP server transactions by using the **show sipd server** command.

ACMEPACKET# **show sipd server**

15: 40: 05-65

SIP Server Trans	Active	High	Total	Total	PerMax	High
All States	0	346	2213	67975	3729	365
<Initial>	0	1	2213	67975	3729	1
<Trying>	0	48	1504	44773	2431	63
<Proceeding>	0	9	709	23202	1310	9
<Cancelled>	0	2	75	1370	182	4
<Established>	0	2	545	20201	971	3
<Completed>	0	148	959	24572	1489	149
<Confirmed>	0	157	716	23202	1309	161
<Terminated>	0	1	545	20201	972	1

ACMEPACKET#

The following table lists the specifics along with a brief description.

Statistic	Description
All States	Total number of all server transactions.
Initial	State when the server transaction is created after a request is received.
Trying	Number of times the 100 Trying message has been sent, meaning that a request has been received and action is being taken.
Proceeding	Number of times a server transaction has been constructed for a request.
Cancelled	Number of INVITE transactions for which the Net-Net system receives a CANCEL.
Established	Situation in which the server sends a 2xx response to an INVITE.
Completed	Number of times that the server has received a 300 to 699 status code and therefore entered the completed state.
Confirmed	Number of times that an ACK was received while the server was in the completed state and therefore transitioned to the confirmed state.
Terminated	Number of times that the server has received a 2xx response or has never received an ACK while in the completed state, and has therefore transitioned to the "terminated" state.

SIP Client Transactions

Display statistics for SIP client transactions by using the **show sipd client** command.

ACMEPACKET# **show sipd client**

15: 40: 09-69

SIP Client Trans	Active	High	Total	Total	PerMax	High
All States	0	382	2042	64973	3371	387
<Initial>	0	1	2042	64973	3371	2
<Trying>	0	128	1333	41771	2073	128
<Calling>	0	2	709	23202	1310	2
<Proceeding>	0	8	613	21570	1130	9
<Cancelled>	0	2	75	1370	182	4
<EarlyMedia>	0	0	0	0	0	0
<Completed>	0	146	959	24571	1489	167
<SetMedia>	0	2	545	20201	972	2
<Established>	0	127	545	20201	971	127
<Terminated>	0	0	0	0	0	0

ACMEPACKET#

The following table lists the statistics along with a brief description.

Statistic	Description
All States	Total number of all client transactions.
Initial	State before a request is sent out.
Trying	Number of times the <i>trying</i> state was entered due to the receipt of a request.
Calling	Number of times that the <i>calling</i> state was entered due to the receipt of an INVITE request.
Proceeding	Number of times that the <i>proceeding</i> state was entered due to the receipt of a provisional response while in the <i>calling</i> state.
Early Media	Number of times that the <i>proceeding</i> state was entered due to the receipt of a provisional response that contained SDP while in the <i>calling</i> state.
Completed	Number of times that the <i>completed</i> state was entered due to the receipt of a 300 to 699 status code when either in the <i>calling</i> or <i>proceeding</i> state.
SetMedia	Number of transactions in which the Net-Net system is setting up NAT and steering ports (setting up the steering of the RTP flow).
Established	Number of situations in which the client receives a 2xx response to an INVITE, but can not forward it on because it requires NAT and steering port information.
Terminated	Number of times that the <i>terminated</i> state was entered due to the receipt of a 2xx message.

Viewing SIP Media Event Errors

Display statistics for SIP media event errors by using the **show sipd errors** command.

ACMEPACKET# **show sipd errors**

13: 06: 59-159

SIP Errors/Events	---- Lifetime ----		
	Recent	Total	PerMax
SDP Offer Errors	0	0	0
SDP Answer Errors	0	0	0
Drop Media Errors	0	0	0
Transaction Errors	0	0	0
Application Errors	0	0	0
Media Exp Events	0	0	0
Early Media Exps	0	0	0
Exp Media Drops	0	0	0
Expired Sessions	0	0	0
Multiple OK Drops	0	0	0
Multiple OK Terms	0	0	0
Media Failure Drops	0	0	0
Non-ACK 2xx Drops	0	0	0
Invalid Requests	0	0	0
Invalid Responses	0	0	0
Invalid Messages	0	0	0
CAC Session Drop	0	0	0
CAC BW Drop	0	0	0

The information displayed is divided into the following categories:

- **Recent:** number of errors that occurred within the number of seconds defined by the figure that appears directly after the time. In the example above, the Recent period of time is 60 seconds.
- **Total:** number of errors that occurred since the system was last rebooted.
- **PerMax:** period maximum number of errors that occurred since the system was last rebooted. This value identifies the highest individual Period Total value calculated over the lifetime of the monitoring.

These statistics record exceptional events encountered by the SIP application in processing SIP media sessions, dialogs, and sessions descriptions (SDP). Serious errors will be accompanied by a log message in log.sipd and acmelog (depending of the current log level setting) of the appropriate severity which will indicate the nature of the error.

Statistic	Description
SDP Offer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model defined in RFC 3264. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in one of the show mbcd errors.
SDP Answer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264). This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in the show mbcd errors.

Statistic	Description
Drop Media Errors	Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog/session; or c) a BYE initiated by the Net-Net SBC due to a timeout notification from MBCD. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in the show mbc errors.
Transaction Errors	Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session.
Missing Dialog	Number of requests received by the SIP application for which a matching dialog count not be found. Usually, this event will also be counted as a 481 (Does Not Exist) server response for the method of the SIP request. This event will occur quite often particularly when both endpoints send a BYE request at approximately the same time.
Application Errors	Number of miscellaneous errors that occur in the SIP application that are otherwise uncategorized.
Media Exp Events	Number of flow timer expiration notifications received from MBCD. These may be fairly common particularly if endpoints stop sending media (or do not start sending media) without sending the appropriate signaling message (BYE) to terminate the dialog/session. These events may also be counted in the show mbc errors.
Early Media Exps	Number of flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or still pending INVITE transaction (e.g., 200 OK response to the INVITE has not been received yet). This can occur if an INVITE transaction takes longer than the initial-guard-timer or subseq-guard-timer fields defined in the media-manager-config element. This event does not result in the dialog/session being terminated if the INVITE is still pending. Note that this statistic is a subset of the Media Exp Events above.
Exp Media Drops	Number of flow timer expiration notifications from MBCD which resulted in the SIP application terminating the dialog/session.
Multiple OK Drops	Number of dialogs that were terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction which was forked by a downstream proxy. When multiple UASs accept an INVITE with a 200 OK responses, only the first one is passed on by the Net-Net SBC. If the subsequent 200 OK were processed and passed on the media session established by the first 200 OK would be disrupted. The Net-Net SBC will ACK the 200 OK response and then send a BYE request to terminate the dialog for the subsequent 200 OK response. The proscribed behavior for the proxy is to cancel outstanding branches of the fork when a 200 OK is received. However, there is a race condition where a subsequent 200 OK is generated by a UAS before the CANCEL reaches the UAS.

Statistic	Description
Multiple OK Terms	Number of dialogs that were terminated upon reception of a 200 OK response which conflicts with an existing established dialog on the Net-Net SBC. This is similar to the Multiple OK Drops statistic. The difference is that an upstream proxy forked the INVITE resulting in multiple INVITE transactions which have the same Call-ID and session description (SDP). The Net-Net SBC will accept only the first 200 OK received. If the subsequent 200 OK were processed, the media session established by the initial 200 OK would be disrupted. The Net-Net SBC will ACK the 200 OK response and then send a BYE request to terminate the dialog for the subsequent 200 OK response. The Net-Net SBC will send a 487 (Terminated) response upstream in order to complete the client transaction which conflicted with an established dialog. The prescribed behavior for the proxy is to cancel outstanding branches of the fork when a 200 OK is received. However, there is a race condition where a subsequent 200 OK is generated by a UAS before the CANCEL reaches the UAS.
Media Failure Drops	Number of dialogs that had to be terminated due to a failure in setting up the media session. This situation occurs when an SDP offer is sent downstream in a request, but the SDP answer in a response to that request encounters a failure. Rather than passing the successful response upstream to the User Agent Client (UAC), the Net-Net SBC terminates the session. For an INVITE transaction, the Net-Net SBC sends an ACK for the 200 OK response and then sends a BYE request. The Net-Net SBC then sends an error response to the UAC.
Expired Sessions	Number of sessions that were terminated due to the session timer expiring. When the media for a dialog/session does not traverse the Net-Net SBC, the SIP application sets a session timer (equal to the <code>flow-time-limit</code> defined in the <code>media-manager-config</code>). This to ensure that the session is properly cleaned up in the event that the endpoints do not send the appropriate signaling to terminate the session (e.g., BYE). Note that when the media session does traverse the Net-Net SBC, the flow timers are used by MBCD and the SIP application does not set a session timer.

Viewing SIP Session Agent Statistics

Display SIP session agent information by using the **show sipd agents** command. With this command, the Net-Net SBC ascertains whether a session agent is in service. When the session agent stops responding to SIP requests, it transitions to the out-of-service state. You can configure the Net-Net SBC to periodically *ping* the session agent if it has gone out-of-service, or if no requests have been sent to it.

The **show sipd agents** command shows information about the number of active sessions, the average rate of session invitations, and the number of times that the constraints established in the session-agent element have been exceeded for sessions inbound to and outbound from each session agent, as well as the average and maximum latency and the maximum burst rate related to each session agent.

For example:

```
ACMEPACKET# show sipd agents
19: 39: 34-95
----- Inbound -----
Session Agent  Active  Rate  ConEx  Active  Rate  ConEx  Avg  Max  Burst  InBurst  OutBurst
192.168.200.131  1      0    0.0    0      0    0.0    0  0.000  0.000  0      0      0
```

Inbound statistics:

- Active: number of active sessions sent to each session agent listed
- Rate: average rate of session invitations (per second) sent to each session agent listed

- ConEx: number of times the constraints have been exceeded

Outbound statistics:

- Active: number of active sessions sent from each session agent
- Rate: average rate of session invitations (per second) sent from each session agent listed
- ConEx: number of times the constraints have been exceeded

Latency statistics:

- Avg: average latency for packets traveling to and from each session agent listed
- Max: maximum latency for packets traveling to and from each session agent listed
- Max Burst: total number of session invitations sent to or received from the session agent within the amount of time configured for the burst rate window of the session agent

The second column, which is not labeled, of the **show sipd agents** output shows the service state of each session agent identified in the first column. In the service state column, an *I* indicates that the particular session agent is in service and an *O* indicates that the particular session agent is out of service. An *S* indicates that the session agent is in transition from the out-of-service state to the in-service state; it remains in this transitional state for a period of time that is equal to its configured in-service period, or 100 milliseconds (whichever is greater). A *D* indicates that the session agent is disabled.

Viewing SIP Session Agent Group Statistics

Display session information for the session agent groups on the Net-Net system by using the **show sipd groups** command. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the **show sipd groups** command accesses the subcommands that are described in this section, the main **show sipd groups** command (when executed with no arguments) displays a list of all session agent groups for the Net-Net system.

If you carry out this command, but you do not specify the name of an existing session agent group, the Net-Net system informs you that the group statistics are not available.

Viewing Session and Dialog States

Display session and dialog states by using the **show sipd sessions** command. For example:

SIP Session Status		-- Period --		----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Sessi ons	0	0	0	0	0	0
Ini ti al	0	0	0	0	0	0
Ear ly	0	0	0	0	0	0
Establ i shed	0	0	0	0	0	0
Termi nated	0	0	0	0	0	0
Di al ogs	0	0	0	0	0	0
Ear ly	0	0	0	0	0	0
Confi rmed	0	0	0	0	0	0
Termi nated	0	0	0	0	0	0

Sessions

- Initial—state of a new session for which an INVITE or SUBSCRIBE is being forwarded.
- Early—state the session enters when it receives the first provisional response (1xx other than 100).
- Established—state the session enters when it receives a success (2xx) response.
- Terminated—state the session enters when the session is ended by receiving or sending a BYE for an Established session or forwarding an error response for an Initial or Early session. The session remains in the Terminated state until all the resources for the session are freed.

Dialogs

A dialog is created when a dialog establishing method (INVITE or SUBSCRIBE) receives a provisional (1xx other than 100) or success (2xx) response.

- Early—dialog is created by a provisional response.
- Confirmed—dialog is created by a success response; an Early dialog transitions to Confirmed when it receives a success response.
- Terminated—dialog enters this state when the session is ended by receiving/sending a BYE for an Established session, or by receiving/sending error response Early dialog. The dialog remains in the Terminated state until all the resources for the session are freed.

Viewing SIP Endpoint

The **show sipd sip-endpoint-ip** command supports the look-up and display of registration information for a designated endpoint. This command uses the following syntax: **show sipd endpoint-ip <phone number>**. For the phone number value, you can enter as many components of the particular phone number about which you would like information—including information about adaptive HNT.

This command must be entered with the numerical value representing the endpoint to look up. The ACLI help menu prompts you for this information.

```
ACMEPACKET# show sipd endpoint-ip ?
```

```
----- ACLI v1.0 -----
```

```
<phone number> enter phone number to look up endpoint
```

There is no support for wildcard matches or lists of users. The first entry that matches the phone number given as an argument will be returned. The following examples show a range of matching values.

```
ACMEPACKET# show sipd endpoint-ip 1781
Reg[sip: 17815551111@69. 69. 69. 10]
RegEntry[sip: 17815551111@69. 69. 69. 10] ID=4 exp=28
UA-
contact='sip: 17815551111@69. 69. 69. 69: 5062; acme_nat=192. 168. 201. 50: 5060'
SD-contact='sip: 17815551111-1ke1g79h75pu8@69. 69. 69. 10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
```

```
ACMEPACKET# show sipd endpoint-ip 17815551111
Reg[sip: 17815551111@69. 69. 69. 10]
RegEntry[sip: 17815551111@69. 69. 69. 10] ID=4 exp=20
UA-
contact='sip: 17815551111@69. 69. 69. 69: 5062; acme_nat=192. 168. 201. 50: 5060'
SD-contact='sip: 17815551111-1ke1g79h75pu8@69. 69. 69. 10'
hnt-test-status='COMPLETED'
successful-test-time='40 secs'
```

```
ACMEPACKET# show sipd endpoint-ip 17815559999
Reg[sip: 17815559999@69.69.69.80]
RegEntry[sip: 17815559999@69.69.69.80] ID=5 exp=29
UA-
contact='sip: 17815559999@69.69.69.69:5063; acme_nat=192.168.201.155:5060'
SD-contact='sip: 17815559999-2se308dh8lp29@69.69.69.10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
```

```
ACMEPACKET# show sipd endpoint-ip 1781555
Reg[sip: 17815551111@69.69.69.10]
RegEntry[sip: 17815551111@69.69.69.10] ID=4 exp=17
UA-
contact='sip: 17815551111@69.69.69.69:5062; acme_nat=192.168.201.50:5060'
SD-contact='sip: 17815551111-1ke1g79h75pu8@69.69.69.10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
```

```
ACMEPACKET# show sipd endpoint-ip 1781555555
Reg[sip: 17815555555@69.69.69.80]
RegEntry[sip: 17815555555@69.69.69.80] ID=3 exp=19
UA-contact='sip: 17815555555@69.69.69.69:5060; user=phone'
SD-contact='sip: 17815555555-v3etv61h55om8@69.69.69.10'
hnt-test-status='COMPLETED'
successful-test-time='40 secs'
```

Viewing SIP Per User CAC Statistics

The commands in this section allow you to view information about SIP per user CAC.

IP-Based CAC Information

If you want to see information about the operation of SIP per user CAC for the IP address mode, you can use the new CLI **show sipd ip-cac** command. You enter this command with the IP address for which you want to view data.

The Net-Net SBC will display the number of configured sessions allowed, number of active sessions, amount of configured bandwidth allowed, and the amount of bandwidth used.

To view information about SIP per user CAC using the IP address mode:

1. In either User or Superuser mode, type **show sipd ip-cac**, a <Space>, and the IP address for which you want to view data. Then press <Enter>.

```
ACMEPACKET# show sipd ip-cac 192.168.200.191
CAC Parameters for IP <192.168.200.191>
Allowed Sessions=2
Active-sessions=0
Allowed Bandwidth=3000000
used-bandwidth=0
```

AoR-Based CAC Information

If you want to see information about the operation of SIP per user CAC for the AoR mode, you can use the **show sipd endpoint-ip** command. You enter this command with the AoR for which you want to view data.

1. In either User or Superuser mode, type **show sipd endpoint-ip**, a <Space>, and the AoR for which you want to view data. Then press <Enter>.

```
ACMEPACKET# show sipd endpoint-ip 123
User <sip: 123@192.168.200.191>
Contact local-exp=47 exp=97
UA-Contact: <sip: 123@192.168.200.191:5061>
SD-Contact: <sip: 123-rrbgdlubs3e66@192.168.1.190:5060>
Call-ID: 00078555-47260002-3dde9eea-259763e2@10.10.10.16
Allowed Sessions=2
Active-sessions=0
Allowed Bandwidth=3000000
used-bandwidth=0
```

Number of Calls Dropped because of Per User CAC Limits

The **show sipd errors** command allows you to view how many calls were dropped:

- Because the per user CAC session limit was exceeded
- Because the per user CAC bandwidth limit was exceeded

Viewing Statistics for SIP Per User Subscribe Dialog Limit

You can display the number of subscription dialogs per SUBSCRIBE event type using the ACLI **show registration sipd subscriptions-by-user** command. You can display this information per event type, or you can show data for all event types by wildcarding the event type argument.

The following example shows you how to use this command with a wildcard.

```
ACMEPACKET# show registration sipd subscriptions-by-user *
Registration Cache          FRI NOV 21 2008 13:40:14
User: sip: 7815550001@192.168.1.206
AOC: <sip: 7815550001@192.168.1.206:5060; transport=udp>
Event-Type: dialog --> Subscriptions: 2
-----
```

Viewing IMS-AKA Statistics

The ACLI **show sipd endpoint-ip** command is updated to show the IMS-AKA parameters corresponding to each endpoint. The display shows the algorithms used, the ports used, and the security parameter indexes (SPIs) used.

In addition, the **show sa stats** command now shows the security associations information for IMS-AKA.

```
ACMEPACKET# show sa stats
05:28:32-107
SA Statistics
```

	Recent	Total	PerMax
IKE Statistics			
ADD-SA Req Rcvd	0	0	0
ADD-SA Success Resp Sent	0	0	0
ADD-SA Fail Resp Sent	0	0	0
DEL-SA Req Rcvd	0	0	0
DEL-SA Success Resp Sent	0	0	0
DEL-SA Fail Resp Sent	0	0	0
ACQUIRE-SA Req Sent	0	0	0
ACQUIRE-SA Success Resp	0	0	0
ACQUIRE-SA Fail Resp Rcv	0	0	0

ACQUIRE-SA Trans Timeout	0	0	0
SA Added	0	0	0
SA Add Failed	0	0	0
SA Deleted	0	0	0
SA Delete Failed	0	0	0
IMS-AKA Statistics			
ADD-SA Req Rcvd	0	0	0
ADD-SA Success Resp Sent	0	0	0
ADD-SA Fail Resp Sent	0	0	0
DEL-SA Req Rcvd	0	0	0
DEL-SA Success Resp Sent	0	0	0
DEL-SA Fail Resp Sent	0	0	0
SA Added	0	0	0
SA Add Failed	0	0	0
SA Deleted	0	0	0
SA Delete Failed	0	0	0

STUN Server Statistics and Protocol Tracing

This section describes how you can monitor STUN server statistics and perform STUN protocol tracing.

STUN Server Statistics

You can display statistics for the STUN server using the ACLI **show mbcn stun** command when the STUN server has been enabled. However, if the STUN server has not been enabled since the last system reboot, the command does not appear and no statistics will be displayed.

```
ACMEPACKET# show mbcn stun
09: 05: 21-193
STUN Statistics
-- Period -- ----- Lifetime -----
Active High Total Total PerMax High
Servers 1 1 0 2 1 1
Server Ports 4 4 0 8 4 4
Binding Requests - - 4 861 4
Binding Responses - - 4 861 4
Binding Errors - - 0 0 0
Messages Dropped - - 0 0 0
```

The table below defines display's categories.

STUN Server Display Category	Description
Servers	The number of STUN servers (the same as the number of realms configured with a STUN server).
Server Ports	Number of ports per STUN server; there will be four ports per STUN server.
Binding Requests	Number of STUN Binding Request messages received by all STUN servers.
Binding Responses	Number of STUN Binding Response messages sent by all STUN servers.

STUN Server Display Category	Description
Binding Errors	Number of STUN Binding Error messages sent by all STUN servers.
Messages Dropped	Number of messages dropped by all STUN servers.

STUN Protocol Tracing

You can enable STUN protocol tracing two ways: by configuration or on demand.

- By configuration—The Net-Net SBC's STUN protocol trace file is called `stun.log`, which is classified as a call trace. This means that when the system configuration's call-trace parameter is set to enabled, you will obtain STUN protocol information for the system. As with other call protocol traces, tracing data is controlled by the log-filter in the system configuration.

On demand—Using the ACLI **notify mbc d log** or **notify mbc d debug** commands, you enable protocol tracing for STUN. Using **notify mbc d debug** sets the STUN log level to TRACE. You can turn off tracing using the **notify mbc d nolog** or **notify mbc d nodebug** commands. Using **notify mbc d nodebug** returns the STUN log level back to its configured setting.

H.323 Protocol Performance

This section describes the different statistics you can access for monitoring H.323 protocol performance.

Viewing the H.323 Performance Statistics

Display the H.323 performance statistics by using the **show h323d** command. The main **show h323d** command executed without arguments indicates the date and time the current period began and displays session statistics, status statistics, and stack statistics for functioning H.323 processes.

For example:

```
acmepacket# show h323d
```

```
18: 22: 24-84
```

Session Stats		-- Period --		----- Li fetime -----		
	Active	High	Total	Total	PerMax	High
Incoming Calls	135	176	1001	77258	785	196
Outgoing Calls	135	176	1001	77258	785	196
Connected Calls	135	172	977	74390	727	196
Incoming Channels	251	319	1953	148780	1454	358
Outgoing Channels	251	319	1953	148780	1454	358
Contexts	135	179	1001	77258	785	197

H323D Status	Current	Li fetime
Queued Messages	238	16000
TPKT Channels	542	4004
UDP Channels	0	0

Stack	State	Type Mode	Registered Gatekeeper
-------	-------	-----------	-----------------------

external enabled H323 Gateway No

internal enabled H323 Gateway No

The following table lists the session statistics along with a brief description.

Statistic	Description
Incoming Calls	Number of H.323 calls coming into the Net-Net SBC.
Outgoing Calls	Number of H.323 calls going out of the Net-Net SBC.
Connected Calls	Number of H.323 calls that are currently connected via the Net-Net SBC.
Incoming Channels	Number of incoming channels that have been established on the Net-Net SBC.
Outgoing Channels	Number of outgoing channels that have been established on the Net-Net SBC.
Contexts	Number of contexts (i.e., the number of calls traversing the Net-Net SBC) that have been established on the Net-Net SBC.

About Status Statistics

The following table lists the current H.323 process status statistics along with a brief description:

Statistic	Description
Queued Messages	Number of messages queued.
TPKT Channels	Number of Transport Packet (TPKT) channels open(ed).
UDP Channels	Number of User Datagram Protocol (UDP) channels open(ed).

Note: The show h323d status command shows the same information available when the show h323d command is executed without any arguments.

About Stack Statistics

The stack statistics provide a summary of information about the H.323 stacks configured on the Net-Net SBC via the h323 stack. This information includes the following facts about each stack: its name, whether or not it is enabled, its type, its mode (either Gateway or Gatekeeper), and whether or not it is registered with a Gatekeeper.

Viewing Current Configuration

Display statistics for the H.323 configuration currently running on the Net-Net SBC by using the **show h323d config** command. Only information about the main configuration element is shown, not for any subelements.

```
ACMEPACKET# show h323d config
h323-config
    state                enabled
    log-level             INFO
    response-tmo          4
    connect-tmo           32
    rfc2833-payload       101
    alternate-routing     proxy
```


codec-fall back
last-modified-date

disabled
2006-07-07 07:49:57

Viewing Stack Information

You can view statistics about the configured H.323 stacks.

Viewing a List of Stacks

Display the list of H.323 stacks (for example, configured instances of the h323 stack) that are currently configured by using the **show h323d stacklist** command.

ACMEPACKET# **show h323d stacklist**

H323-Stack List

name	internal
name	external

ACMEPACKET#

Viewing Stack Details

Display detailed information about the configured instances of H.323 stacks by using the **show h323d stackconfig** command.

ACMEPACKET# **show h323d stackconfig**

h323-stack

name	tester
state	disabled
isgateway	enabled
realm-id	test
assoc-stack	acme
local-ip	172.30.1.150
max-calls	100
max-channels	10
registration-ttl	15
terminal-alias	e164=17823484839
prefixes	url=http://www.acmepacket.com
ras-port	1030
auto-gk-discovery	enabled
multicast	172.30.1.150:11
gatekeeper	170.30.1.150:57
gk-identifier	RS
q931-port	1720
alternate-transport	173.30.1.150:15
q931-max-calls	200
h245-tunneling	disabled
fs-in-first-msg	disabled
call-start-fast	enabled
call-start-slow	disabled
media-profiles	acme
process-registration	disabled
allow-anonymous	all
proxy-mode	H225
h245-stage	connect

```

q931-start-port          0
q931-number-ports        0
dynamic-start-port        0
dynamic-number-ports      0
rfc2833-mode              transparent
filename                  packet11
tcp-keepalive             disabled
last-modified-date        2006-07-07 08:39:01
ACMEPACKET#

```

Viewing Specific Stacks

Display detailed information about the configured H.323 stack specified in the <stack name> argument by using the **show h323d stackconfig <stack name>** command.

```

ACMEPACKET# show h323d stackconfig internal
h323-stack
  name                  internal
  state                 enabled
  isgateway             enabled
  realm-id              acme
  assoc-stack           packet
  local-ip              0.0.0.0
  max-calls             200
  max-channels          6
  registration-ttl      120
  terminal-alias
                        url=http://www.acmepacket.com

  prefixes
                        ipAddress=63.67.143.4:2000

  ras-port              1719
  auto-gk-discovery     disabled
  multicast             0.0.0.0:0
  gatekeeper            0.0.0.0:0
  gk-identifier         rs
  q931-port             1720
  alternate-transport
  q931-max-calls        200
  h245-tunneling        disabled
  fs-in-first-msg       disabled
  call-start-fast       enabled
  call-start-slow       disabled
  media-profiles
                        sip
  process-registration  disabled
  allow-anonymous       all
  proxy-mode            H225
  h245-stage            connect
  q931-start-port       0
  q931-number-ports     0
  dynamic-start-port    0
  dynamic-number-ports  0
  rfc2833-mode          transparent
  filename              ps
  tcp-keepalive         disabled

```

Last-modified-date
ACMEPACKET#

2006-07-10 11:48:13

Viewing Session Agent Stats

You can view statistics about the session agents.

Viewing a List of Session Agents

Display a list of session agents by using the **show h323d agentlist** command. For example:

```
ACMEPACKET# show h323d agentlist
H323-Session Agent List
  hostname 192.168.200.20
  hostname 192.168.200.30
  hostname 10.10.10.3
```

Viewing Session Agent Stats

Display statistics about the session agent by using the **show h323d agentstats** command. For example:

```
ACMEPACKET# show h323d agentstats 172.16.0.13
19:57:21-51
Session Agent 172.16.0.13(h323172) [In Service]

-- Period -- ----- Lifetime -----
Active High Total Total PerMax High
Inbound Sessions      0      0      0      0      0      0
Rate Exceeded         -      -      0      0      0      -
Num Exceeded          -      -      0      0      0      -
Reg Rate Exceeded     -      -      0      0      0      -
Outbound Sessions    199     245     196    23583     164    256
Rate Exceeded         -      -      0      0      0      -
Num Exceeded          -      -      0      0      0      -
Reg Rate Exceeded     -      -      0      0      0      -
Out of Service        -      -      0      0      0      -
Trans Timeout         0      0      0      19      2      1
Requests Sent         -      -    2092    234608    1569      -
Requests Complete     -      -     196    23563     164      -
Seizure               -      -     196    23583     164      -
Answer                -      -     199    23563     164      -
ASR Exceeded          -      -      0      0      0      -
Messages Received     -      -    2267    258308    1675      -
Latency=0.011; max=0.045
```

The following table lists the statistics along with a brief description of each.

Statistic	Description
Inbound	
Active	Number of active sessions sent to each session agent listed in the Session Agent column of this command's output.
Rate	Average rate of session invitations (per second) sent to each session agent listed in the Session Agent column of this command's output.

Statistic	Description
ConEx	Number of times that the constraints established in the constraints fields of the session-agent element have been exceeded. The constraints fields of the session-agent element include the following: max-sessions, max-outbound-sessions, max-burst-rate, max-sustain-rate, burst-rate-window, and sustain-rate-window.
Outbound	
Active	Number of active sessions sent from each session agent listed in the Session Agent column of this command's output.
Rate	Average rate of session invitations (per second) sent from each session agent listed in the Session Agent column of this command's output.
ConEx	Number of times that the constraints established in the constraints fields of the session-agent element have been exceeded.
Latency	
Avg	Average latency for packets traveling to and from each session agent listed in the Session Agent column of this command's output.
Max	Maximum latency for packets traveling to and from each session agent listed in the Session Agent column of this command's output.
Max Burst	Total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field of the session-agent element.

Viewing Specific Session Agent Statistics

Display the activity for the particular H.323 session agent specified in the <agent> argument by using the **show h323d agents <agent>** command.

ACMEPACKET# **show h323d agentstats 172.16.0.13**

19:57:21-51

Session Agent 172.16.0.13(h323172) [In Service]

	Active	High	Total	Total	PerMax	High
Inbound Sessions	0	0	0	0	0	0
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Reg Rate Exceeded	-	-	0	0	0	-
Outbound Sessions	199	245	196	23583	164	256
Rate Exceeded	-	-	0	0	0	-
Num Exceeded	-	-	0	0	0	-
Reg Rate Exceeded	-	-	0	0	0	-
Out of Service	-	-	0	0	0	-
Trans Timeout	0	0	0	19	2	1
Requests Sent	-	-	2092	234608	1569	-
Requests Complete	-	-	196	23563	164	-
Seizure	-	-	196	23583	164	-
Answer	-	-	199	23563	164	-
ASR Exceeded	-	-	0	0	0	-

Messages Received - - 2267 258308 1675 -
 Latency=0.011; max=0.045

The following table lists the statistics and a brief description.

Statistic	Description
Inbound Sessions	
Rate Exceeded	Number of times the session or burst rate was exceeded for inbound sessions.
Num Exceeded	Number of times the time constraints were exceeded for inbound sessions.
Outbound Sessions	
Rate Exceeded	Number of times the session or burst rate was exceeded for outbound sessions.
Num Exceeded	Number of times the time constraints were exceeded for outbound sessions.
Burst	Number of times the burst rate was exceeded for this session agent.
Out of Service	Number of times this session agent went out of service.
Trans Timeout	Number of transactions that timed out for this session agent.
Requests Sent	Number of messages sent via the session agent.
Requests Complete	Number of requests that have been completed for this session agent.
Messages Received	Number of messages received by this session agent.

Viewing Session Agent Configurations

Display the configuration for all configured H.323 session agents by using the **show h323d agentconfig** command.

```
ACMEPACKET(sessi on-agent)# show h323 agentconfi g
sessi on-agent
  hostname                testhostname.com
  ip-address              192.168.200.13
  port                    5060
  state                   enabl ed
  app-protocol             SIP
  app-type                 H323-GW
  transport-method        UDP
  real m-i d              h323192
  descri pti on
  carri ers
  al low-next-hop-l p      enabl ed
  constrai nts             di sabl ed
  max-sessi ons            0
  max-i nbound-sessi ons   4
  max-outbound-sessi ons   5
  max-burst-rate           0
  max-i nbound-burst-rate  10
  max-outbound-burst-rate  1
  max-sustai n-rate        0
```

```

max-inbound-sustain-rate      0
max-outbound-sustain-rate     0
min-seizures                   5
min-asr                       0
time-to-resume                0
ttr-no-response               0
in-service-period             0
burst-rate-window             0
sustain-rate-window           0
req-uri-carrier-mode           None
proxy-mode                     Rect
rect-action                   enabled
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method
ping-interval                  0
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translated
out-translated
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulated
out-manipulated
p-asserted-id
trunk-group

tgname1: tgcontext1
tgname2: tgcontext2

max-register-sustain-rate     0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
last-modified-date             2007-03-29 17:15:50
task done

```

Viewing Session Agent by Hostname

The **show h323d agentconfig <hostname>** command displays detailed information about the configured session agent specified by its hostname in the **<hostname>** argument.

When displaying individual H.323 session agent configurations, remember that H.323 does not support DNS and therefore the hostname field values for H.323 session agents are IPv4 addresses.

```

ACMEPACKET(session-agent)# show h323d agentconfig
session-agent
hostname                               testhostname.com

```

ip-address	192. 168. 200. 13
port	5060
state	enabl ed
app-protocol	SI P
app-type	H323-GW
transport-method	UDP
real m-i d	h323192
descri pti on	
carri ers	
al low-next-hop-l p	enabl ed
constrai nts	di sabl ed
max-sessi ons	0
max-i nbound-sessi ons	4
max-outbound-sessi ons	5
max-burst-rate	0
max-i nbound-burst-rate	10
max-outbound-burst-rate	1
max-sustai n-rate	0
max-i nbound-sustai n-rate	0
max-outbound-sustai n-rate	0
mi n-sei zures	5
mi n-asr	0
ti me-to-resume	0
ttr-no-response	0
i n-servi ce-peri od	0
burst-rate-wi ndow	0
sustai n-rate-wi ndow	0
req-uri -carri er-mode	None
proxy-mode	Redi rect
redi rect-acti on	
l oose-routi ng	enabl ed
send-medi a-sessi on	enabl ed
response-map	
pi ng-method	
pi ng-i nterval	0
pi ng-i n-servi ce-response-codes	
out-servi ce-response-codes	
medi a-profi les	
i n-transl ati oni d	
out-transl ati oni d	
trust-me	di sabl ed
request-uri -headers	
stop-recurse	
l ocal -response-map	
pi ng-to-user-part	
pi ng-from-user-part	
l i -trust-me	di sabl ed
i n-mani pul ati oni d	
out-mani pul ati oni d	
p-asserted-i d	
trunk-group	
	tgname1: tgcontext1
	tgname2: tgcontext2
max-regi ster-sustai n-rate	0

```

early-media-allow
invalid-registrations      disabled
rfc2833-mode               none
rfc2833-payload            0
codec-policy
last-modified-date         2007-03-29 17:15:50
task done

```

Viewing Session Agent Group Stats

You can view statistics for session agent groups.

Listing Session Agent Groups

Display a list of the H.323 session agent groups by using the **show h323d grouplist** command.

```

ACMEPACKET# show h323d grouplist
H323-Session Agent Group List
      group-name                sag1
ACMEPACKET#

```

Viewing Session Agent Group Stats

Display session information for the session agent groups by using the **show h323d groupstats** command. Session information is compiled by totalling the session agent statistics for all session agents that make up a particular session agent group.

While the **show h323d groupstats** command accesses the subcommands that are described in this section, the main **show h323d groupstats** command (when executed without arguments) displays a list of all session agent groups for the Net-Net SBC.

All of the categories for these statistics are the same as those used in the displays produced by the **show h323d agent** command.

```

ACMEPACKET# show h323d groupstats
19:38:59-30
      ----- Inbound -----      Outbound -----      Latency --      Max -----
SAG      Active Rate ConEx Active Rate ConEx Avg Max Burst InBurst OutBurst
H323Group I 0 0.0 0 0 0.0 0 0.000 0.000 0 0 0

```

Viewing Session Agent Details

You can list and show the statistics for the session agents that make up the session agent groups that are being reported. The **-v** (meaning “verbose”) executed with this command must be included to provide this level of detail.

```

ACMEPACKET# show h323d groups -v
SAG:      SGTest
19:38:59-30
      ----- Inbound -----      Outbound -----      Latency --      Max -----
SAG      Active Rate ConEx Active Rate ConEx Avg Max Burst InBurst OutBurst
H323Group I 0 0.0 0 0 0.0 0 0.000 0.000 0 0 0
SAG:      SGTest
192.168.200.61 I 120 0.0 0 359 0.0 0 0.000 0.000 5 0 0 0

Total s:
SGTest    D 120 0.0 0 359 0.0 0 0.000 0.000 5 0 0 0
ACMEPACKET#

```


Viewing Specific Session Group Statistics

Display statistics for the designated session agent group by using the **show h323d groups <group name>** command with the name of a specific session agent group.

```
ACMEPACKET# show h323d groups testgroup
```

```
16: 35: 18-18
```

SAG	----- Inbound -----			----- Outbound -----			-- Latency --		Max Burst
	Active	Rate	ConEx	Active	Rate	ConEx	Avg	Max	
testgroup	0	0.0	0	0	0.0	0	0.000	0.000	0

```
ACMEPACKET#
```

If this command is carried out, but the name of an existing session agent group is not available, the Net-Net system will display a messaging saying that the group statistics are not available.

```
ACMEPACKET# show h323d groups test
```

```
group statistics not available
```

```
ACMEPACKET#
```

Viewing all Configurations

Display the configuration for all configured H.323 session agent groups by using the **show h323d groupconfig** command.

```
acmepacket# show h323d groupconfig
```

```
session-group
```

```
group-name h323
```

```
description
```

```
state enabled
```

```
app-protocol H323
```

```
strategy Hunt
```

```
dest
```

```
172.16.0.13
```

```
1.1.1.1
```

```
trunk-group
```

```
last-modified-date
```

```
2006-07-11 19:12:22
```

Viewing Specific Session Agent Group Statistics

Display detailed information about the configured session agent group specified by its group name by using the **show h323d agentconfig <group name>** command. The group name is configured in the `group-name` field of the session-agent-group element in the `<group name>` argument.

```
ACMEPACKET# show h323d groupconfig h323
```

```
session-group
```

```
group-name h323
```

```
description
```

```
state enabled
```

```
app-protocol H323
```

```
strategy Hunt
```

```
dest
```

```
172.16.0.13
```

```
1.1.1.1
```

```
trunk-group
```

```
last-modified-date
```

```
2006-07-11 19:12:22
```

Viewing Stats for Each Configured Stack

Display information for each of the configured H.323 stacks by using the **show h323d h323stats** command.

```
ACMEPACKET# show h323d h323stats
```

```
STACK : h323172
```

```
H. 225 : Sent      585622  Recd      764844  maxCPU  0
H245   : Msg       976289  Ack       1171626  Rej      0      Rel      0
RAS    : Req        0      Ack        0      Rej      0      maxCPU  0
```

```
STACK : h323192
```

```
H. 225 : Sent      586040  Recd      585622  maxCPU  0
H245   : Msg       976087  Ack       1171626  Rej      0      Rel      0
RAS    : Req        0      Ack        0      Rej      0      maxCPU  0
```

The display identifies the H.323 stack by its name and then provides the data described in the following table.

Statistic	Description
H.225	Number of H.225 messages sent and received by this H.323 stack
H245	Number of H.245 requests, acknowledgements, rejections, and releases sent and received by this H.323 stack
RAS	Number of RAS requests, acks, and rejects sent and received by this H.323 stack

Viewing Statistics for Specific Stacks

Display detailed statistics for the H.323 stack specified in the <stack name> argument by using the **show h323d h323stats <stack name>** command. This information is displayed according to the following categories: H.225, H.245, and RAS.

```
acmepacket# show h323d h323stats h323172
```

```
STACK : h323172
```

```
H. 225 STATISTICS
```

MESSAGE TYPE	SENT	RECD
Setup	200118	0
Call Proceeding	0	0
Alerting	0	200112
Connect	0	200109
Progress	0	0
Facility	0	0
Release Complete	199906	191628
Status	0	0
Status Inquiry	0	0
Notify	0	0
Info	0	0

```
H. 245 STATISTICS (Total)
```

MESSAGE TYPE	MSG	ACK	REJ	REL
Master Slave	200110	400218	0	0
Terminal Capability	400218	400218	0	0
OpenLogical Channel	0	0	0	0
CloseLogical Channel	399812	399812	0	0

RAS STATISTICS FOR MESSAGES SENT

MESSAGE TYPE	REQ	CON	REJ
GK Discovery	0	0	0
Registration	0	0	0
Unregistration	0	0	0
Admission	0	0	0
Location	0	0	0
Bandwidth	0	0	0
Dialing	0	0	0
Info	0	0	0

RAS STATISTICS FOR MESSAGES RECD

MESSAGE TYPE	REQ	CON	REJ
GK Discovery	0	0	0
Registration	0	0	0
Unregistration	0	0	0
Admission	0	0	0
Location	0	0	0
Bandwidth	0	0	0
Dialing	0	0	0
Info	0	0	0

ACMEPACKET#

The following table lists the statistics along with its type and a brief description.

Statistic	Type	Description
H.225 STATISTICS		Statistics about the H.225.
	MESSAGE TYPE	Type of messages sent and received by this H.323 stack.
	SENT	For each type of message specified in the MESSAGE TYPE column, how many of the message types were sent by this H.323 stack.
	RECD	For each type of message specified in the MESSAGE TYPE column, this statistic shows how many of the message types were received by this H.323 stack.
H.245 STATISTICS Total		Statistics about the H.245
	MESSAGE TYPE	Type of H.245 messages sent and received by this H.323 stack.
	MSG	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many message requests were sent and received by this H.323 stack.
	ACK	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many acknowledgements were sent and received by this H.323 stack.
	REJ	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many rejections were sent and received by this H.323 stack.

Statistic	Type	Description
	REL	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many releases were sent and received by this H.323 stack.
RAS STATISTICS FOR MESSAGES		There are two sections of RAS statistics: one for SENT (or issued) and one for RECD (or received).
	MESSAGE TYPE	Type of RAS messages sent and received by this H.323 stack.
	REQ	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many requests were issued/received by this H.323 stack.
	CON	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many confirmations were issued/received by this H.323 stack.
	REJ	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many rejections were issued/received by this H.323 stack.

Viewing H.323 Registrations

Display the total number of H.323 endpoint registrations by using the **show h323d reg** command.

```
acmepacket# show h323d reg
```

```
Stack: external      Number of registrations: 256
```

```
Total Number of Registrations : 256
```

Viewing MGCP Performance Statistics

This section explains how to display performance statistics for MGCP.

Listing the MGCP Performance Subcommands

You can display a list of the **show algd** subcommands.

```
ACMEPACKET# show algd ?
```

acl s	MGCP ACL statistics
al l	display all ALG Statistics
aucx	AUCX command statistics
au ep	AUEP command statistics
crcx	CRCX command statistics
dl cx	DLCX command statistics
epcf	EPCF command statistics
errors	MGCP error statistics
mdcx	MDCX command statistics
ntfy	NTFY command statistics
other	Other MGCP command statistics
redundancy	MGCP Redundancy Statistics
rqnt	RQNT command statistics

rsip
statistics

RSIP command statistics
ALG MGCP statistics

Viewing MGCP Status Statistics

Display MGCP state and transaction status statistics by using the **show algd statistics** command.

ACMEPACKET# **show algd statistics**

14: 14: 19-105

```

State
-----
Active    High    Total    Total    PerMax    High
MGCP Sessions      0      0      0      0      0      0
CA Endpoints      0      0      0      0      0      0
GW Endpoints      0      0      0      0      0      0
Media Sessions     0      0      0      0      0      0
Client Trans       0      0      0      0      0      0
Server Trans       0      0      0      0      0      0
Pending MBCD       0      0      0      0      0      0
MGCP ALGs          0      0      0      0      0      0

----- Gateway ----- Call Agent -----
MGCP Transactions
----- Li fetime ----- Li fetime -----
Recent    Total    PerMax    Recent    Total    PerMax
Requests received      0      0      0      0      0      0
Responses sent         0      0      0      0      0      0
Duplicates received    0      0      0      0      0      0
Requests sent          0      0      0      0      0      0
Responses received     0      0      0      0      0      0
Retransmissions sent   0      0      0      0      0      0
ACMEPACKET#

```

About State Statistics

The State section displays information about MGCP sessions, connections, and transactions, which are defined in the following table.

Statistic	Description
MGCP Sessions	Number of MGCP signaling sessions established through the MGCP ALG. For each gateway that registers with the call agent with an Restart in Progress (RSIP) command, an MGCP signaling session is established. It contains the information to map endpoint names and signaling addresses on either side of the Net-Net SBC so that requests from the call agent can be routed to the gateway.
Media Sessions	Number of media sessions for MGCP connections established through the Net-Net SBC. A media session is created when a connection is created (CRCX), and deleted when the connection is deleted (DLCX).
Client Trans	Number of client transactions where the Net-Net SBC is sending a request to a gateway or the call agent. Unless the transaction was originated by the Net-Net SBC. For example an Audit Endpoint (AUEP) for NAT traversal, there will be a corresponding server transaction on the other side of the Net-Net SBC.
Server Trans	Number of server transactions where the Net-Net SBC received a request from a gateway or the call agent. There will be a corresponding client transaction on the other side of the Net-Net SBC.

Statistic	Description
Pending MBCD	Number of requests or responses that were held while waiting for an MBC transaction to complete. When an MGCP request or response requires media setup or teardown (e.g., when the message contains SDP), the request or response can not be forwarded on until the MBC transaction is complete. New requests for the connection are pending until the MBC transaction completes. This statistic counts the case where a new request is received before previous one was sent on.
MGCP ALGs	This statistic shows the number of MGCP ALGs in the Net-Net SBC. It corresponds to the number of <code>mgcp-config</code> elements defined in the Net-Net SBC.

About MGCP Transactions

These statistics show information about MGCP transactions (requests and responses). The `Gateway` columns show information about MGCP messages between the gateway and the Net-Net SBC. The `Call Agent` columns show information about MGCP messages between the Net-Net SBC and the call agent.

Statistic	Description
Requests received	Number of requests received by the Net-Net SBC from the gateway and call agent.
Responses sent	Number of responses sent back by the Net-Net SBC to the gateway and call agent in response to the requests received.
Duplicates Received	Number of request retransmissions received by the Net-Net SBC from the gateway and call agent. Since MGCP is sent over UDP, elements must retransmit requests if they do not receive a response.
Requests Sent	Number of requests sent by the Net-Net SBC to the gateway and call agent.
Responses Received	Number of responses received from the gateway and call agent in response to the requests sent by the Net-Net SBC.
Retransmissions Sent	Number of request retransmissions sent by the Net-Net SBC to the gateway and call agent. Since MGCP is sent over UDP, elements must retransmit requests if a response is not received.

- **CurPer:** an abbreviated form of *current period*. Displays the total number of transactions during the current monitoring period.
- **Total:** displays the total number of transactions since the Net-Net system was last rebooted.
- **PerMax:** displays the period maximum number of transactions during a single period in the time since the Net-Net system was last rebooted. This statistic identifies the highest individual `CurPer` value achieved over the lifetime of the monitoring.

All Available Information

Displays information about many of the `show algd` subcommands by using the `show algd all` command. You can see all of the information for the following:

- MGCP status
- MGCP transactions

- MGCP errors
- MGCP commands, including: RSIPs, RQNTs, NTFYs, CRCXs, MDCXs, DLCXs, and AUEPs

ACMEPACKET# **show al gd al l**

14: 15: 22-168

State	-- Period --			----- Li fetime -----		
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
MGCP Sessi ons	0	0	0	0	0	0
CA Endpoi nts	0	0	0	0	0	0
GW Endpoi nts	0	0	0	0	0	0
Medi a Sessi ons	0	0	0	0	0	0
Cl ient Trans	0	0	0	0	0	0
Server Trans	0	0	0	0	0	0
Pendi ng MBCD	0	0	0	0	0	0
MGCP ALGs	0	0	0	0	0	0

----- Gateway -----				----- Cal l Agent -----		
MGCP Transacti ons		----- Li fetime -----		----- Li fetime -----		
	Recent	Total	PerMax	Recent	Total	PerMax
Requests recei ved	0	0	0	0	0	0
Responses sent	0	0	0	0	0	0
Dupl i cates recei ved	0	0	0	0	0	0
Requests sent	0	0	0	0	0	0
Responses recei ved	0	0	0	0	0	0
Retransmi ssi ons sent	0	0	0	0	0	0

14: 15: 22-168

MGCP Medi a Events		----- Li fetime -----		
	Recent	Total	PerMax	
Call i ng SDP Errors	0	0	0	
Call ed SDP Errors	0	0	0	
Drop Medi a Errors	0	0	0	
Transacti on Errors	0	0	0	
Appl i cation Errors	0	0	0	
Medi a Exp Events	0	0	0	
Early Medi a Exps	0	0	0	
Exp Medi a Drops	0	0	0	

14: 15: 22-168

MGCP ACL Status		-- Period --			----- Li fetime -----	
	Acti ve	Hi gh	Total	Total	PerMax	Hi gh
Total Entries	0	0	0	0	0	0
Trusted	0	0	0	0	0	0
Blocked	0	0	0	0	0	0

ACL Operati ons		----- Li fetime -----		
	Recent	Total	PerMax	
ACL Requests	0	0	0	
Bad Messages	0	0	0	
Promoti ons	0	0	0	
Demoti ons	0	0	0	

----< NO DATA AVAI LABLE >----(RSIP)

----< NO DATA AVAI LABLE >----(RQNT)

----< NO DATA AVAI LABLE >----(NTFY)

----< NO DATA AVAI LABLE >----(CRCX)

----< NO DATA AVAI LABLE >----(MDCX)

```

----< NO DATA AVAILABLE >----(DLCX)
----< NO DATA AVAILABLE >----(AUEP)
----< NO DATA AVAILABLE >----(Other)

```

Viewing MGCP Error Statistics

These statistics record exceptional events encountered by the MGCP ALG application in processing media sessions, connections, and sessions descriptions (SDP). Serious errors are accompanied by a log message in log.algd and acmelog (depending of the current log level setting) of the appropriate severity which will indicate the nature of the error.

ACMEPACKET# **show alg errors**

11:51:16-176

MGCP Media Events	---- Lifetime ----		
	Recent	Total	PerMax
Calling SDP Errors	0	0	0
Called SDP Errors	0	0	0
Drop Media Errors	0	0	0
Transaction Errors	0	0	0
Application Errors	0	0	0
Media Exp Events	2	2	2
Early Media Exps	0	0	0
Exp Media Drops	2	2	2

ACMEPACKET#

The following table lists the statistics along with a brief description.

Statistics	Description
Calling SDP Errors	Number of errors encountered in setting up the media session for a session description (SDP) in an MGCP request. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in one of the show mbcd errors.
Called SDP Errors	Number of errors encountered in setting up the media session for a session description (SDP) in an MGCP response. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in one of the show mbcd errors.
Drop Media Errors	Number of errors encountered in tearing down the media for an MGCP connection that is being terminated due to: a) non-successful response to an MGCP transaction; or b) a Delete Connection (DLCX) transaction received from the call agent. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in the show mbcd errors.
Transaction Errors	Number of errors in continuing the processing of the MGCP transaction associated with setting up or tearing down of the media session.
Application Errors	Number of miscellaneous errors that occur in the MGCP ALG application that are otherwise uncategorized.

Statistics	Description
Media Exp Events	Number of flow timer expiration notifications received from MBCD. These may be fairly common, particularly if endpoints stop sending media (or do not start sending media) without sending the appropriate signaling message to terminate the MGCP connection. These events may also be counted in the show mbcdr errors display.
Early Media Exps	Number of flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or still pending MGCP call setup. This can occur if an MGCP call setup takes longer than the initial-guard-timer or subseq-guard-timer fields defined in the media-manager-config element. This event does not result in the connection being terminated if the transaction is still pending. Note that this statistic is a subset of the Media Exp Events above.
Exp Media Drops	Number of flow timer expiration notifications from MBCD which resulted in the MGCP ALG application terminating the connection.

MGCP Message Monitoring

Display information about individual types of MGCP commands by using the `show algd` command with the appropriate message name. You can view information about the following messages: RSIPs, Notification Requests (RQNTs), Notifys (NFTYs), Create Connections (CRCXs), Modify Connections (MDCXs), DLCXs, and AUEPs.

- `show algd rsip`
- `show algd rqnt`
- `show algd ntfy`
- `show algd crcx`
- `show algd mdcx`
- `show algd dlcx`
- `show algd auep`

```
ACMEPACKET# show algd rsi p
20: 43: 05-195
```

```

Recent      Total      PerMax
----- Li fetime -----
RSIP incomi ng:
  Requests recei ved      0      1736      1228
  Replies sent            0      1532      1024
  Errors sent             0         0         0
RSIP outgoi ng:
  Requests sent           0      1532      1024
  Replies recei ved       0      1532      1024
  Errors recei ved        0         0         0
ACMEPACKET#
```

Note: If there is no data available for a certain MGCP message, the system displays the fact that there is none and specifies the message about which you inquired.

Other MGCP Stats

Display statistics for other MGCP methods by using the `show algd other` command.

Viewing Accounting Data and Statistics

This section explains how to view accounting data and statistics. See *Admission Control and Quality of Service Reporting* in the *Net-Net 4000 ACLI Configuration Guide* for additional details about Quality of Service (QoS). See the *Net-Net RADIUS Guide* for additional details about Remote Authentication Dial-in User Service (RADIUS).

QoS Reporting

If you are using for the QoS functionality in collecting and calculating the jitter, latency, and loss statistics. QoS reporting provides you with real-time evaluation of network and route performance. It lets you contrast internal domain and external domain performance and facilitates SLA verification and traffic engineering.

QoS metrics are collected and reported on a per-session basis, per call-leg basis for completed calls. These metrics are reported through real-time RADIUS records along with call accounting data. These metrics are the result of the monitoring of the Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) traffic for each flow that has QoS enabled.

The following statistics:

- lost packets for RTP and RTCP that indicates the count of packets lost based on comparing the sequence numbers since the beginning of the call or the last context memory flow
- jitter count for RTP and RTCP that indicates the incremental number of packets that have been used to generate total and max jitter since the beginning of the call or the last context memory poll
- jitter total for RTP and RTCP indicates the incremental accumulated jitter (ms) over all the packets received since the beginning of the call or the last context memory poll
- jitter max for RTP and RTCP that indicates the maximum single jitter value (ms) from all the packets since the beginning of the call or the last context memory poll
- latency count for RTCP only indicates the number of RTCP frames over which latency statistics have been accumulated since the beginning of the call or the last context memory poll
- latency total for RTCP only indicates the incremental total of latency values reported since the beginning of the call or the last context memory poll
- latency max for RTCP only indicates the highest single latency value measured since the beginning of the call or the last context memory poll

From these flow context statistics the QoS daemon derives the following statistics that are kept in host memory while the call is active:

- lost packets indicates the total number of RTP and RTCP lost packets for the call
- jitter count indicates the number of RTP and RTCP packets that make up a call
- jitter total indicated the accumulated jitter over all the packets received during the call
- jitter average indicates the total accumulated jitter divided by the total jitter count for the call
- jitter max indicates the maximum single jitter value from all the packets during the call

- latency count for RTCP indicates the number of RTCP frames of which latency statistics have been accumulated during the call
- latency total for RTCP only indicates the incremental total of latency values reported
- latency max for RTCP only indicates the highest latency value reported during the call
- latency average for RTCP only indicates the RTCP latency total divided by the latency count

You can access QoS statistics that provide information about four areas of call performance.

Viewing Network Management Control Statistics

You can use the new ACLI **show net-management-control** command to see the statistics that the Net-Net SBC collects. When you use the command, you specify the name of the network management control rule for which you want to display data or you can enter **all** to see the statistics for all control rules.

For each network management control rule, the Net-Net SBC gathers statistics for the number of:

- Incoming calls—Incoming calls that match the destination identifier
- Rejected calls—Calls that were rejected as a result of the control rule being applied
- Diverted calls—Incoming that were diverted as a result of the control rule being applied

The display you see when you execute this command shows statistics for the current period, lifetime, and maximum value in a period.

Displaying Network Management Control Statistics

To display network management control statistics:

1. In either User or Superuser mode, type the **show net-management-control** command, a <Space>, and then the name of the control rule for which you want to see data. You can enter **all** if you want to see the data for all control rules. Then press <Enter>.

```
ACMEPACKET# show net-management-control nmcpercent
14: 45: 15-63
Name: nmcpercent
Type: gap-percent
----- Li f e t i m e -----
Current      Total      PerMax
Incoming Cal l s      0          0          0
Rejected Cal l s      0          0          0
Diverted Cal l s      0          0          0
```

Resetting Network Management Control Statistics

To reset network management control statistics, you use the ACLI **reset net-management-control** command followed by the name of the control rule for which you want to reset statistics. This command resets the counters to zero (0).

To reset network management control statistics:

1. In Superuser mode, type the ACLI **reset net-management-control** command, a <Space>, and then the name of the control rule for which you want to see data. Then press <Enter>.

```
ACMEPACKET# reset net-management-control nmcpercent
```

Monitoring Your Net-Net System in Real-Time

This section explains how to monitor your Net-Net system in real-time by using the **monitor media** and **monitor sessions** commands.

- **monitor media:** real-time media statistics
- **monitor sessions:** real-time SIP statistics

Note: The ACLI statistics displays use standard VT100 escape sequences to format the display. Therefore, your terminal emulator or terminal itself must support VT100.

Displaying the Statistics

The following information explains how to work with the statistics display.

Changing the Refresh Rate

At any point, you can press any numerical digit (0-9) to change the number of seconds for the refresh rate (the rate at which the display is updated). By default, the statistics refresh every second. For example, while viewing the statistics, you can press <6> to cause the Net-Net system statistics to refresh every 6 seconds. While viewing the statistics via the ACLI, you can press any key to automatically refresh the statistics upon keypress.

Quitting the Display

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt (for example, ACMEPACKET#). From that point, you can continue with any other task you choose.

Viewing Real-Time Media Statistics

Display real-time media statistics for your running Net-Net system by using the **monitor media** command.

```
acmepacket# monitor media
```

```
17: 31: 00-160
```

MBCD Status		-- Period --		----- Lifetime -----		
	Active	High	Total	Total	PerMax	High
Client Sessions	143	182	1930	1218332	4225	683
Client Trans	0	18	5744	2500196	8439	625
Contexts	144	182	1930	834745	2783	2001
Flows	296	372	3860	1669498	5566	3689
Flow-Port	286	362	3860	1669488	5566	3679
Flow-NAT	294	365	3788	1658668	5563	2051
Flow-RTCP	0	0	0	0	0	0
Flow-Hairpin	0	0	0	0	0	0
Flow-Released	0	0	0	0	0	0
MSM-Release	0	0	0	0	0	0
NAT Entries	295	365	3791	1658671	5563	2051

Free Ports	7430	7518	7828	3346410	11604	8002
Used Ports	572	724	7724	3338980	11132	8000
Port Sorts	-	-	0	14796	4156	
MBC Trans	1141	1234	5748	2503147	8440	2974
MBC Ignored	-	-	0	0	0	
ARP Trans	0	0	0	8	8	1

Real-time statistics for the following categories appear on the screen:

- Client Sessions
- Client Trans
- Contexts
- Flows
- Flow-Port
- Flow-NAT
- Flow-RTCP
- Flow-Hairpin
- Flow-Release
- MSM-Release
- NAT Entries
- Free Ports
- Used Ports
- Port Sorts
- MBC Trans
- MBC Ignored
- ARP Trans

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the Net-Net system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Viewing Real-Time SIP Session Statistics

If you have Superuser access, display real-time monitoring of your running Net-Net system for sessions. This table displays information similar to that which is displayed for the **show sipd** command, except that the information in the **monitor sessions** table is real-time and updates automatically.

```

ACMEPACKET# show sipd
14: 16: 43-149
SIP Status
-- Period -- ----- Li fetime -----
Active High Total Total PerMax High
Sessi ons 0 0 0 0 0 0
Subscri ptions 0 0 0 0 0 0
Di a l o g s 0 0 0 0 0 0
Ca l l I D Map 0 0 0 0 0 0
Rej ect i o n s - - 0 0 0
Re I N V I T E s - - 0 0 0
Medi a Sessi ons 0 0 0 0 0 0
Medi a Pendi ng 0 0 0 0 0 0
Cl i e n t Trans 0 0 0 0 0 0
Ser v e r Trans 0 0 0 0 0 0
Res p Contexts 0 0 0 0 0 0
S a v e d Contexts 0 0 0 0 0 0
S o c k e t s 0 0 0 0 0 0
Req Dropped - - 0 0 0
D N S Trans 0 0 0 0 0 0
D N S S o c k e t s 0 0 0 0 0 0
D N S Resul ts 0 0 0 0 0 0

Session Rate = 0.0
Load Rate = 0.0

```

Real-time statistics for the following categories appear on the screen:

- Dialogs
- Sessions
- CallID Map
- Rejections
- ReINVITES
- Media Sessions
- Media Pending
- Client Trans
- Server Trans
- Resp Contexts
- Sockets
- Reqs Dropped
- DNS Trans
- DNS Sockets
- DNS Results

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the Net-Net system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Viewing TLS Information

You can use the commands described in this section to obtain information about TLS and its associated Net-Net SSM hardware module.

Clearing the Entire TLS Session Cache

To clear the entire TLS session cache:

1. Enter the ACLI **clear-cache tls** command.

```
ACMEPACKET# clear-cache tls
```

Viewing TLS Session Cache State and Statistics

To see whether TLS session caching is enabled on your system and how many entries there are in the cache:

1. Enter the ACLI **show security tls session-cache** command.

```
ACMEPACKET# show security tls session-cache
```

```
TLS Session Caching enabled.
```

```
Current TLS Session Cache Entries: 3
```

```
ACMEPACKET#
```

Viewing Certificates in PEM Form

The ACLI **show certificates** command has been enhanced to provide a **pem** argument that you can use to retrieve the Privacy Enhanced Mail Security Certificate (PEM) portion of the certificate after it the Net-Net SBC has imported it.

You enter this command with the name of the certificate you want to see in PEM form.

To see a certificate in PEM form:

1. Enter the command **show security certificates pem** followed by a <Space>, the name of the certificate, and then press <Enter>.

```
ACMEPACKET# show security certificates pem client1a
```

```
certificate-record: client1a
```

```
-----BEGIN PKCS7-----
```

```
MIIDRWYJKoZIhvcNAQcCoIIDDCCAzaQCAQExADADBgEAoIIDDJCCAYAwggKJoAMCAQI
CCAI TAI AAhACeMAOGCSqGSI b3DQEBBQUAMHAXCzAJBgNVBAYTAI VTRMRmweEQYD
VQI EwpDYWxpZm9ybml hMREwDwYDVQQHEwhTYW4gSm9zZTEOMAwGA1UEChMFc2Iw
aXQxKTAnBgNVBAsTIFNpcGFI OI FRI c3QgQ2VydGI maWNhdGUgQXV0aG9yaXR5MB4X
DTA2MDgxMDE1NDQ0OVoxDTA5MDgwOTE1NDQ0OVowVzELMAkGA1UEBhMCMVVMxGZAJ
BgNVBAGTAk1BMRMwEQYDVQQHEwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVI
cmI uZzEQMA4GA1UEAxMHcnI hbmVuZDCBnzANBgkqhki G9w0BAQEFAA0Bj QAwgYkC
gYEAshgHLBsue6HhyxDsv+6hB53a7rTWRNj u10Qk0hi tAEhVswgyj 3wCHnd5o62
LVAI 3esKJfnRJI /gl eHZ7uhVI L3j uMhDTcF/XT+Dzb+ZBMmgJQzrkokseRgL2aLI
```

```

FBbnnG3DoUugyk/Jp3J6CBz+ZGUF85WQri 1JuDREJ9fVCMOCaWEAAa0B2zCB2DAP
BgNVHREECDAggRyeWfUMAKGA1UdEwQCMAAwHQYDVRO0BBYEFaphhPV97obtLI CT
9mn1y0VU2yduMI GaBgNVHSMegZI wgY+AFGtGFxTqI HYI gFRuE1TaoeNUFKG2oXSk
cj BwMQswCQYDVQOGEwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pYTERMA8GA1UEBxMI
U2FuI Epvc2UxDj AMBgNVBAoTBXNpcGI OMSkwJwYDVQOLEyBTaXBpdCBUZXRNOI ENI
cnRpZml j YXRRI EF1dGhvcml OeYI BADANBgkqhki G9w0BAQUFAA0BgQAzSuW+sYI 2
I /K/8Fo8Pj 6T8qDWh3qcEoqJkPyI FXHSWCdQPdKrOi i YAgNV3wE8dhRRZWWrb30T
yl Qzfc2YTJStJ/XveX/Hwt4X1yRwcBL32Rr4Xj i DpeUWWrfwwqAH5Rfj S4X/kHw4
agrTDzKbE03+kSr2dPb42ko+Tai SDoLI 8j EA
-----END PKCS7-----

```

ACMEPACKET#

Viewing Net-Net SSM Status

For TLS support, you must have a Net-Net SSM hardware module installed in the system chassis. Without this module, TLS functions will not work.

The Net-Net SBC tells you whether or not the SSM installed on boot-up, but now you can check the module's status from the command line.

To view the status of the Net-Net SSM installed in your Net-Net SBC chassis:

1. Enter the command **show security ssm-accelerator**, and press <Enter>. The system will tell you if an SSM is installed.

```

ACMEPACKET# show security ssm-accelerator
SSM (Security Service Module) present.
ACMEPACKET#

```

Viewing IPsec Statistics

The following section explains the commands used to obtain IPsec statistics which can be helpful for debugging purposes.

Security Association Entries

The CLI **show security ipsec sad** command displays the security association database entries which are programmed into the security processor. In the case of manual keying, the entries should match that of the running configuration. Network-interface is entered as a network interface configuration element name, selectors are entered as the selector term, a <space>, and a search term for that selector. You can enter multiple selector in one command. The command's syntax follows:

```

show security ipsec sad [network-interface] <bri ef | deta il >
[sel ectors]

```

Entering no selectors returns all entries for that network interface. Valid values for the selectors argument are as follows:

- direction—Direction (IN | OUT | BOTH), Default: BOTH
- dst-addr-prefix—Destination address prefix, Default: match any
- dst-port—Destination port, Default: match any
- ipsec-protocol—IPsec protocol (AH | ESP | ALL), Default: ALL
- spi—security-policy-index, Default: match any
- src-addr-prefix—Source address prefix, Default: match any

- src-port—Source port, Default: match any
- trans-proto—Transport protocol (UDP | TCP | ICMP | ALL), Default: ALL

Security Policy Entries

The **show security ipsec spd** command shows the security policy database entries which are programmed into the security processor. Network-interface is entered as a network interface configuration element name. The command's syntax follows:

```
show security ipsec spd [network-interface]
```

IPSec Statistics

The ACLI **show** commands for IPSec statistics are used to display statistical values as reported directly from the IPSec hardware. There are two versions of this command:

- The **show security ipsec statistics sad** command queries a selected IPSec processor for statistics about the SAs configured on it, as located in the security association database (SAD).
- The **show security ipsec statistics gmac** command queries the GMAC side of the security processor for Ethernet statistics.

Viewing Statistics for a Specific SA

The **show security ipsec statistics sad** command shows statistical values for a particular SA entry on the IPSec security processor. You enter a network interface configuration name, selectors by the selector term, a <Space>, and a search term for that selector. You can enter multiple selector in one command. The command's syntax follows:

```
show security ipsec statistics [network-interface] sad <selectors>
```

Entering no selectors returns all entries for that network interface. Valid values for the selectors argument are as follows:

- direction—Direction (IN | OUT | BOTH), Default: BOTH
- dst-addr-prefix—Destination address prefix, Default: match any
- dst-port—Destination port, Default: match any
- ipsec-protocol—IPSec protocol (AH | ESP | ALL), Default: ALL
- spi—security-policy-index, Default: match any
- src-addr-prefix—Source address prefix, Default: match any
- src-port—Source port, Default: match any
- trans-proto—Transport protocol (UDP | TCP | ICMP | ALL), Default: ALL

Viewing Statistic for Traffic to/from the GMAC Interface and the Security Processor

The **show security ipsec statistics gmac** command displays statistics on traffic that moves between the GMAC interface and the security processor on a specified network interface. Network-interface is entered as a network interface configuration element name. You can display either errors, transmit statistics, receive statistics, or all statistics per HW accelerator / gmac interface . The command's syntax follows:

```
show security ipsec statistics [network-interface] gmac <enter | error  
| rx | tx>
```

Viewing IPSec Interface Status

The **show security ipsec status** command displays whether a particular interface on Net-Net SBC is IPSec enabled, and the hardware status of the security processor.

Network-interface is entered as a network interface configuration element name.
The **show security ipsec status** command usage is as follows:

```
show security ipsec status [network-interface]
```

Viewing SSH Security Information

The following section explains the commands used to obtain SSH statistics which can be helpful for debugging purposes.

Viewing SSH Statistics

The **show security ssh** command displays public key record information. You can include the brief argument to view a brief display which includes login name, fingerprint, and fingerprint raw, or you can view a detailed display which, along with the information displayed in the brief output, also includes comment, and public key.

Viewing a Brief SSH Statistics Output

The following is an example of a **show security ssh brief** command:

```
ACMEPACKET# show security ssh-pub-key brief
Login-name:
SEtest
fingerprint:
31: b1: 5d: 16: ed: 01: a7: 97: 52: e3: 92: 72: f2: ee: 00: 74
fingerprint-raw:
66: 81: 95: 8b: 05: 1b: fc: cd: a4: f9: 01: 39: 44: 42: f1: 87
```

Viewing a Detailed SSH Statistics Output

The following is an example of a **show security ssh detailed** command:

```
ACMEPACKET# show security ssh-pub-key detail
Login-name:
SEtest
comment:
"2048-bit RSA, converted from OpenSSH by test1@tac-
linux.acmepacket.com"
fingerprint:
31: b1: 5d: 16: ed: 01: a7: 97: 52: e3: 92: 72: f2: ee: 00: 74
fingerprint-raw:
66: 81: 95: 8b: 05: 1b: fc: cd: a4: f9: 01: 39: 44: 42: f1: 87
pub-key:

AAAAB3NzaC1yc2EAAAABIwAAAQEAxPy5GYj KBI 52URsdw0LrKtALvDNzyK3HFgtqHsVwh
WZcEMDqTGcKqr+AAYd/72j ug+QtJTp8xzI SZZcsL2Fbi 0S6W4d3I HGdt8I QCHsNpNLdUj
3YfXxbi eQy++EI Pi BAgi fEzj Y7swCCnUdcgsUDA27/HzSP/tbl dvEAwtfe+Yu5uBo7vpm
SGI vzNHkpWhkZ4EyHVXQzafbvXpNnl 06j dUHVci i yPy242zl L9tnzhm+yKmpZS7NUNkqX
pmC3VDEVqi vdOGvzrBNJ2RJJI JUqMq9ZkFnj XgEKL1YTKP3zTP/fArUn4cRDRkzkKPF17
0+oapo5ki hDkk3UDhWJVBeI SQ==

Modulus (2048 bit):
00: c4: fc: b9: 19: 88: ca: 06: 2e: 76: 51: 1b: 1d: c0: e2:
eb: 2a: d0: 0b: bc: 33: 73: c8: ad: c7: 16: 0b: 6a: 1e: c5:
70: 85: 66: 5c: 10: c0: ea: 4c: 67: 0a: aa: bf: 80: 01: 87:
7f: ef: 68: ee: 83: e4: 2d: 25: 3a: 7c: c7: 39: 52: 65: 97:
2c: 2f: 61: 5b: 8b: 44: ba: 5b: 87: 77: 20: 71: 9d: b7: c9:
50: 08: 7b: 0d: a4: d2: dd: 52: 3d: d8: 7d: 7c: 5b: 89: e4:
32: fb: e1: 08: 3e: 20: 40: 82: 27: c4: ce: 36: 3b: b3: 00:
82: 9d: 47: 5c: 82: c5: 03: 03: 6e: ff: 1f: 34: 8f: fe: d6:
```

c8: 76: f1: 00: c2: d7: de: f9: 8b: b9: b8: 1a: 3b: be: 99:
92: 18: 8b: f3: 34: 79: 29: 5a: 19: 19: e0: 4c: 87: 55: 74:
33: 69: f6: ef: 5e: 93: 67: 23: 4e: a3: 75: 41: d5: 72: 28:
b2: 3f: 2d: b8: db: 39: 4b: f6: d9: f3: 86: 6f: b2: 28: ca:
59: 4b: b3: 54: 36: 4a: 97: a6: 60: b7: 54: 31: 15: aa: 2b:
dd: d0: 6b: f3: ac: 13: 49: d9: 12: 4a: 94: 95: 2a: 32: af:
59: 90: 59: e3: 5e: 01: 0a: 2f: 56: 13: 28: fd: f3: 4c: ff:
df: 02: b5: 27: e1: c4: 43: ae: 4c: e4: 28: f1: 75: ec: ef:
a8: 6a: 9a: 39: 92: 28: 43: 92: 4d: d4: 0e: 15: 89: 54: 17:
a5: 49
Exponent: 35 (0x23)

User Privilege Levels and Passwords: Without Data Storage Security

User and Superuser Modes

There are two modes available in the ACLI: User mode and Superuser mode. User mode provides only limited system access and allows no system configuration. It simply enables you to view configuration files, logs, and all show commands. Superuser mode provides more complete system access and it allows you to configure your Net-Net SBC.

When you log in to a Net-Net SBC you are initially in User mode. To indicate this, the system uses a ">" (close-angle-bracket) as the final character of the ACLI prompt. To enter Superuser mode, you type **enable** followed by <Enter> at the ACLI prompt. The system prompts you to enter the Superuser password. After you enter the correct password, the prompt changes to a "#" (pound sign) to indicate Superuser mode.

```
User Access Verification
```

```
Password:
```

```
ACMEPACKET> enable
```

```
Password:
```

```
ACMEPACKET#
```

To exit to User mode from Superuser mode, type **exit** at the top-level ACLI prompt.

```
ACMEPACKET# exit
```

```
ACMEPACKET>
```

Setting Passwords

Acme Packet recommends that you change the preset passwords for ACLI User and Superuser modes. You can change the passwords from Superuser mode only.

To set new ACLI passwords:

1. Use the **secret** command to change passwords.

Type **secret login** and press <Enter> to set the User password. The Net-Net SBC asks for a new password, which must be between six and eight characters with at least one non-alphabetic character. For example:

```
ACMEPACKET# secret login
```

```
Enter new password :
```

If you do not enter a password in the required format, the following error message appears:

```
% Password must be 6-8 characters with at least one non-alpha
```

2. Type **secret enable** to set the Superuser password. Again, the Net-Net SBC asks for a new password that must be between six and eight characters with at least one non-alphabetic character. For example:

```
ACMEPACKET# secret enable
Enter new password :
```

3. Use your new passwords when prompted for them.

SSH Remote Connections

For increased security, you can also connect to your Net-Net system using SSH (secure shell). SSH requires that you have an SSH client. The Net-Net system supports three concurrent SSH and/or SFTP sessions.

To initiate an SSH connection to the Net-Net system without specifying users and SSH user passwords:

1. Open your SSH client (Windows, an open source client, etc.).
2. At the prompt in the SSH client, type the **ssh** command, a <Space>, the IPv4 address or hostname of your Net-Net system, and then press <Enter>. You will be prompted for a password. Enter the Net-Net system's User mode password. After it is authenticated, an SSH session is initiated and you can continue with tasks in User mode or enable Superuser mode.

```
ssh sd. acme. com
Password:
ACMEPACKET>
```

You can explicitly use the default username and password pair (user/packet) by specifying you are logging in with the user account.

```
ssh -l user sd. user acme. com
Password: <ACLI -user-password>
ACMEPACKET>
```

To create an SSH user and password pair on your Net-Net system:

1. In the ACLI at the Superuser prompt, use the **ssh-password** command and press <Enter>. Enter the name of the user you want to establish. Then enter a password for that user when prompted. Passwords are not displayed on the screen.

```
ACMEPACKET# ssh-password
SSH username [saved]: MJones
Enter new password:
```

If you do not enter a password in the required format, the following error message appears:

```
% Password must be 6-8 characters with at least one non-alpha
Enter new password again:
```

Once you have entered a valid password, you must enter your password a second time for confirmation.

After your SSH username and password is set, you can SSH into your Net-Net SBC. Once you provide a valid username and password pair, you need to log in to the ACLI with the previously configured ACLI username and password.

You can SSH into the Net-Net SBC for the first time with the default username and superuser password.

```
ssh -l user net-net-sd. company. com
```

SSH RADIUS Authentication VSA Support

The Net-Net SBC supports the use of the Cisco Systems Inc.TM “Cisco-AVPair” vendor specific attribute (VSA). This attribute allows for successful administrator login to servers that do not support the Acme Packet authorization VSA. While using RADIUS-based authentication, the Net-Net SBC authorizes you to enter Superuser mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA.

For this VSA, the Vendor-ID is 1 and the Vendor-Type is 9. The list below shows the values this attribute can return, and the result of each:

- `shell : pri v-l vl =15`—User automatically logged in as an administrator
- `shell : pri v-l vl =1`—User logged in at the “user” level, and not allowed to become an administrator
- Any other value—User rejected

SSHv2 Public Key Authentication

The Net-Net SBC supports viewing, importing, and deleting public keys used for authentication of SSHv2 sessions from administrative remote users.

ACLI Instructions and Examples: Viewing SSH Public Key Data

This section explains how to use the ACLI **show security ssh-pub-key** commands that show you the following information in either brief or detailed displays:

- Login name
- Fingerprint
- Fingerprint raw
- Comment (detailed view only)
- Public key (detailed view only)

You use the login name information from these displays to import or delete SSHv2 public keys.

To view information for public keys in brief format:

1. In Superuser mode, type **show security ssh-pub-key brief**, and the log-in name for the public key you want to see. Then press <Enter>.

```
ACMEPACKET# show security ssh-pub-key brief j doe
```

Your display will resemble the following example:

```

Login-name:
  j doe
fi nger-pri nt:
  c4: a0: eb: 79: 5b: 19: 01: f1: 9c: 50: b3: 6a: 6a: 7c: 63: d5
fi nger-pri nt-raw:
  ac: 27: 58: 14: a9: 7e: 83: fd: 61: c0: 5c: c8: ef: 78: e0: 9c
```

1. In Superuser mode, type **show security pub-key detail**, and the log-in name for the public key you want to see. Then press <Enter>.

```
ACMEPACKET# show security ssh-pub-key detail msml th
```

```

Login-name:
  msml th
comment:
```

```

1024-bit rsa, created by me@example.com Mon Jan 15 08:31:24 2001
finger-print:
61: f8: 12: 27: 13: 51: ef: c2: 3e: b3: 29: 32: d7: 3a: f2: fc
finger-print-raw:
3f: a2: ee: de: b5: de: 53: c3: aa: 2f: 9c: 45: 24: 4c: 47: 7b
pub-key:
AAAAB3NzaC1yc2EAAAABJQAAAIEAi PWx6WM4I hHNedGfBpPJNPPz7yKu+dnn1SJeg t45
96k6Yj zGGphH2TUxwKzxcKDKKezwkpfnxPkSMkuEspGRt/aZZ9wa++0i 7Qkr8prgHc4so
W6NUI fDzpvZK2H5E7eQaSeP3SAwGmQKUFHCddNaPOL+hM7zhFNzj FvpaMgJw0=

Modulus (1024 bit):
00: 88: f5: b1: e9: 63: 38: 96: 11: cd: 79: d1: 9f: 06: 93:
c9: 34: fa: 59: ef: 22: ae: f9: d9: e7: d5: 22: 5e: 8e: 0b:
78: e7: de: a4: e9: 88: f3: 18: 6a: 61: 1f: 64: d4: c7: 02:
b3: c5: c2: 83: 28: a7: b3: c2: 4a: 5f: 9f: 13: e4: 48: c9:
2e: 12: ca: 46: 46: df: da: 65: 9f: 70: 6b: ef: 8e: 8b: b4:
24: af: ca: 6b: 80: 77: 38: b2: 85: ba: 35: 49: 5f: 0f: 3a:
6f: 64: ad: 87: e4: 4e: de: 41: a4: 9e: 3f: 74: 80: c0: 69:
90: 29: 41: 47: 09: d7: 4d: 68: fd: 0b: fa: 13: 3b: ce: 11:
4d: ce: 31: 6f: a5: a3: 20: 27: 0d
Exponent: 37 (0x25)

```

Importing a Public Key Record

This section shows you how to import a public key record. Note that the processes requires you to save and activate your configuration for changes to take effect.

To import an SSHv2 public key record:

1. In Superuser mode, type the command **ssh-public-key import**, then a <Space> and the login-name (found in both brief and detail **show security public-key** commands) corresponding to the public key you want to import.

The Net-Net SBC confirms you have successfully imported the key, and then reminds you to save your configuration.

After you complete this procedure, you can confirm the public key has been imported by using either of the show security **ssh-pub-key** commands.

```
ACMEPACKET# ssh-pub-key import J doe
```

IMPORTANT:

Please paste ssh public key in the format defined in rfc4617.
Terminate the certificate with ";" to exit.....

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted from OpenSSH by jdoe@acme54"
AAAAB3NzaC1yc2EAAAABI wAAQEA70Bf08J Je7MSMgerj DTgZpbPbl rX4n17LQJgPC7cl
L
cDGEtKSi Vt5Mj cSav3v6AEN2pYZi h0xd2Zzi smpoo019kkJ56s/Ij GstEzqXMKHKUr9mB
V
qvqI E0TqbowEi 5sz2AP31GUj QTCKZRF1X0Qx8A44vHZCum93/j fNRsnWQ1mhHmaZMmt2L
S
h0r4J/NI p+vpsvpdroI V6Ftz5ei VfgoxrDrj NcVtsAMyLBpDdL6e9XebQzGSS92TPuKP
/
yqzLJ2G5NVFhxdw5i +FvdHz1vBdvB505y2QPj /i z1u3TA/307tyntB0b7beDyl rg64Azc
8
G7E3AGi H49LnBtI Qf/aw==
---- END SSH2 PUBLIC KEY ----
;

```



```
SSH public key imported successfully....
```

```
WARNING: Configuration changed, run "save-config" command to save it
and run "activate-config" to activate the changes.
```

2. Save and activate your configuration.

To delete an SSHv2 public key record:

1. In Superuser mode, type the command **ssh-public-key delete**, then a <Space> and the login-name (found in both brief and detail **show security public-key** commands) corresponding to the public key you want to import.

The Net-Net SBC confirms you have successfully imported the key, and then reminds you to save your configuration.

After you complete this procedure, you can confirm the public key has been imported by using either of the show security **ssh-pub-key** commands.

```
ACMEPACKET# ssh-pub-key del ete J doe
```

```
SSH public key deleted successfully....
```

```
WARNING: Configuration changed, run "save-config" command.
```

```
ACMEPACKET# ssh-pub-key del ete J doe
```

```
record (j doe) does not exist
```

2. Save and activate your configuration.

Expanded Privileges

Commands available to the User level user now include:

- All show commands
- All display commands
- All monitor commands

See the Net-Net ACLI Reference Guide Command Summary Chapter for a list of privileges for each ACLI command.

User Sessions

The Net-Net SBC provides a way to manually terminate an existing Telnet session on your system. Sessions are terminated by issuing the kill command to a specifically chosen session. You first identify the session you wish to “kill” and then issue the command.

1. At the User or Superuser prompt, type **show users** followed by <enter>. This will display the current sessions on the Net-Net SBC.

```
ACMEPACKET# show users
```

Index	task-id	remote-address	IdNum	duration	type	state
0	0x0225c400		0	00:00:44	console	priv
1	0x0225e260	10.0.200.40:4922	1	00:00:26	telnet	priv
2	0x0219c720	10.0.200.40:4938	100	00:00:08	ssh	priv *

```
ACMEPACKET#
```

The current session is noted by the asterisk to the right of the entry in the state column. In the above example, the current session has an IdNum of 2.

Identify the session you wish to kill by the IPv4 address listed in the remote-address column of the show users display.

- Issue the **kill** command followed by the IdNum of the session you wish to kill. The IdNum is listed when you issue the **show users** command.

```
ACMEPACKET# kill 2
```

```
Killing ssh session at Index 2
```

```
ACMEPACKET# show users
```

Index	task-id	remote-address	IdNum	duration	on type	state
0	0x0225c400		0	00: 03: 42	consol e	pri v
1	0x0225e260	10. 0. 200. 40: 4922	1	00: 03: 24	tel net	pri v *

```
ACMEPACKET#
```

Note: You must be in Superuser mode to issue the kill command, but you only need to be in User mode to issue the **show users** command.

Concurrent Sessions

The Net-Net SBC allows a maximum number of 5 concurrent Telnet sessions and 5 concurrent SSH sessions. The SSH allowance is shared between SSH and SFTP sessions.

Data Storage Security

In Net-Net Release C5.0, the Net-Net SBC supports more secure storage of the various passwords used for system functions and using certain system features. These include: administration, certificate private key information, and manual IPSec security association key information. In addition, the Net-Net SBC now stores passwords in a more secure manner when you enable password-secure mode.

Warning: Before enabling the features described in this section, you should be certain that you want to upgrade to Net-Net OS Release C5.0.

Considerations When Enabling Data Storage Security

The features in this group make your system more secure, and in doing so they correspondingly make it difficult for an outsider to tamper both with sensitive information used for IPSec, TLS, and HDR and with your passwords in secure-password mode.

If you use these security measures, you should be careful to:

- Guard against losing your secure data password.
- Enable secure-password mode in Upgrade to Net-Net Release C5.0 and when you are certain you will not need to fall back to an earlier software image.

Note that the password-secure mode feature does not default to enabled on your system. This is for backward compatibility, so you need to enable password-secure mode if you want to use it and you should exercise caution when you enable it.

About Net-Net SBC Password Features

This section describes the multiple ways that password support has been expanded and improved to provide your system with a greater degree of security. It contains information about password-secure mode, new password support for

configurations, configuration migration, new password requirements, and backwards compatibility.

Password Secure Mode

When you enable password secure mode, the Net-Net SBC asks you to set and confirm the following new passwords:

- **Login**—Password to use when logging on to the Net-Net SBC in user mode; in this mode you have monitoring and some maintenance functions enabled, but you cannot perform certain key maintenance tasks (like changing the system image) or perform configuration tasks.
- **Privileged**—Password to use when entering Superuser mode to access and use the full range of system tasks and configuration.
- **LI**—Password to use when accessing lawful intercept (LI) configuration tasks and related functions. If you do not have authorization to change passwords for LI functions, the Net-Net SBC will show an error if you try to set a new password for password-secure mode.

In Superuser mode, you can enter the new ACLI **password-secure-mode status** command to see the status for password-secure mode. It is either enabled or disabled, and is disabled by default for backward compatibility.

Once you enable password secure mode, you will not be able to change passwords back to the factory defaults. Password secure mode has different requirements for passwords even from ones you set for non-secure mode. Your new password-secure mode passwords must be: at least eight characters in length, contain numeric and alphabetical characters, and contain both upper and lower case letters.

Protected Configuration Password for TLS, IPSec, and HDR

You can now set a password for your configuration to guard sensitive information for TLS, IPSec, and HDR configurations.

Once you set the protected configuration password, the older configuration can become unusable unless you set the password back to the old value when creating the backup configuration. During the verification and activation of a configuration, the Net-Net SBC checks these values. If there is a conflict and the Net-Net SBC cannot access encrypted data using the password information you set, it displays a message notifying you of the fact.

Note that for HA nodes, the Net-Net SBC requires you to update the new password manually both on the active and on the standby systems.

Configuration Migration

If you want to move a configuration file from one Net-Net SBC to another, the Net-Net SBC checks passwords during the verification and activation processes. If there is a conflict and the Net-Net SBC cannot access encrypted data using the password information you set, it displays a message notifying you of the fact.

However, you can still reuse this configuration. Simply enter the correct protected configuration password information, and then verify and activate the configuration again.

Password Requirements

Since we are inclined to select passwords that are easy for us to remember, the Net-Net SBC has several requirements for passwords that make them more difficult to tamper with. The passwords you enter on the Net-Net SBC must be:

- Between 8 and 20 characters in length

- Comprised of both alphabetical and numeric characters, where your password must have at least one non-alphabetical character
- Comprised of both upper and lower case letters, where your password must have at least one upper case character and one lower case character
- Void of any of the passwords commonly used as default on the Net-Net SBC: default, password, acme, packet, user, admin

Note on Backwards Compatibility

Since the password requirements for previous releases of the Net-Net OS clearly do not meet with the new criteria that have been defined for Net-Net Release C5.0, the password-secure mode is disabled by default. Once you are certain that you want to run Net-Net Release C5.0, you can enable the new password feature.

When you enable the password-secure mode, all old passwords become invalid. These old passwords are rendered useless in order to close any possible holes in security.

Password Reset and Recovery

The enhancements to password protection on the Net-Net SBC have been intentionally implemented so that password recovery and reset are not accessible through the ACLI. Acme Packet strongly recommends that you treat this password information with care and take all precautions against losing it.

For both password secure mode and the protected configuration password, the process for recovery and reset involves loading a diagnostics image on your system. For information about loading and running diagnostics, contact Acme Packet Customer Support.

Password Policy

When you use password secure mode on your Net-Net SBC, you can now configure the minimum acceptable length for a secure password if you have Superuser (administrative) privileges. The maximum password length is 64 characters.

In password secure mode, your password requires three out of four of the following:

- Upper case letters
- Lower case letters
- Numbers
- Punctuation marks

However, secure mode password cannot contain any of the following strings in any variations of case: default, password, acme, user, admin, packet.

Any change you make to the password length requirement does not go into effect until you configure a new password (and are in password secure mode). Pre-existing passwords can continue to be used until you go to change them.

Upgrade to ACP

Another measure Net-Net Release C5.0 takes to provide enhanced security is upgrading the version of the Acme Control Protocol (ACP) from version 1.0 to version 1.1. Version 1.0 uses normal digest authentication, but version 1.1 uses advanced digest authentication. Advanced digest authentication does not require that credentials be stored using reversible format; it uses a pre-calculated hash to construct the digest value. In ACP version 1.1, there is an additional directive (user

credentials hash algorithm) in the Authentication header so that the server (such as the Net-Net EMS) can calculate the proper digest.

SSH Password Considerations

Your existing SSH password will still work after you upgrade to Net-Net Release C5.0. However, because this password is no longer stored in the `/code/ssh` directory, a warning will appear every time the SSH server accesses the file for user authentication:

```
ACMEPACKET# Cannot check the integrity of SSH password storage.
Should consider re-set the SSH password.
```

As of Net-Net Release C5.0, the hash of the password is saved. The file with the password also contains information that guards integrity to prevent tampering.

Resetting your password will prevent the warning messages and make your SSH sessions more secure. The procedure for setting your SSH password is the same as in prior releases.

ACLI Instructions and Examples

This section shows you how to enable password-secure mode, and how to set protected configuration passwords (with special instructions for manually setting the protected configuration password on the standby system in an HA node). You can also see how to set a password policy.

Enabling Password-Secure Mode for the First Time

This feature is disabled by default for the reasons noted in the [Note on Backwards Compatibility \(244\)](#) section.

When you enable password-secure mode, you must set password from within the password-secure mode process. Once in secure mode, you can change login (User), privileged (Superuser), and LI passwords using the ACLI **secret** command.

Note that when you enable the password-secure mode, all old passwords become invalid. Old passwords are rendered useless in order to close any possible holes in security. This is especially important because releases prior to Net-Net Release C5.0 and Net-Net Release C5.0 have different password requirements, and you will not necessarily be able to reinstate the passwords you use for prior releases.

To enable password-secure mode:

1. In Superuser mode, type **password-secure-mode enabled** at the system prompt and press <Enter>.


```
ACMEPACKET# password-secure-mode enable
```
2. After you press <Enter>, the Net-Net SBC reminds you of the consequences of enabling password-secure mode. It informs you that you need to set new login (User) and privileged (Superuser) passwords, and asks you to confirm the change.

Type a **y** (for yes) and press <Enter> to proceed, or abort the process by typing an **n** (for no).

By enabling password secure mode, you will need to set at least 'login' and 'privileged' passwords

WARNING:

Once password secure mode enabled, you will need to

follow the documented procedures in order to use image older than 5.0

Are you sure [y/n]?: **y**

3. Then the Net-Net SBC prompts you to set a new login (User) password. Your entry must confirm to the <Link>Password Requirements (243) for Net-Net Release C5.0.

1. Enter the new login (User) password and press <Enter>.

Set login password

Enter new password : *[your entry will not echo]*

2. Confirm the new login (User) password and press <Enter>.

Enter password again: *[your entry will not echo]*

4. Next, change the password for the privileged (Superuser) level. Again, your entry must confirm to the <Link>Password Requirements (243) for Net-Net Release C5.0.

1. Enter the new privileged (Superuser) password and press <Enter>.

Set privileged password

Enter new password : *[your entry will not echo]*

2. Confirm the new privileged (Superuser) password and press <Enter>.

Enter password again: *[your entry will not echo]*

5. Finally, the Net-Net SBC asks if you want to set new password for LI features. If you want to set the password and have the authority to do so, type a **y** and press <Enter>. If you do not have LI features licensed on your system or do not have authority to change the password, press **n**.

In the following example, the user went forward with changing the LI password, but the system refused the request based on lack of privilege.

Set li password now [y/n]?: **y**

Set li password

Error: This user does not have privilege to change "li-admin" password change it later

If the user had requisite authority, the Net-Net SBC would have asked for and confirmed a password entered according to the <Link>Password Requirements (243).

Setting a Protected Configuration Password: Matching Configurations

You set a protected configuration password using the ACLI **secret** command. As the system warning indicates when you start this process, changing the password makes backup and archived configurations unusable and requires you to change the password on the standby system in an HA node (if applicable).

When your saved and active configurations match, the process will proceed as in the sample below. However, when the saved and active configuration are out of sync, the Net-Net SBC requires you to correct the condition by activating the configuration (using the ACLI **activate-config** command).

To set a protected configuration password when configuration data is in synch:

1. In Superuser mode, type **secret config** at the system prompt and press <Enter>.

ACMEPACKET# **secret config**

2. The Net-Net SBC issues a warning for the change you are about to make, and asks you to confirm whether or not you want to proceed. Type a y and press <Enter> to continue; type an n and press <Enter> to abort the process.

 WARNING:

Proceed with caution!

Changing the configuration password will result in any previous backup/archive configuration unusable.

You also need to change the password on any stand-by SDs when you have changed the password successfully

 Are you sure [y/n]?: y

3. Then the system asks for the old configuration password.

Enter old password : *[your entry will not echo]*

If your entry does not match the old password, the system displays an error message: % Password mismatch - aborted.

If your entry matches, you will be asked for the new password.

4. Enter the new configuration password. Your entry must conform to the <Link>Password Requirements (243) for Net-Net Release C5.0.

Enter new password : *[your entry will not echo]*

5. Confirm the new configuration password and press <Enter>. The Net-Net SBC first displays a message letting you know that it is changing the password, and then another message confirming the change. It also prompts you to save and activate your configuration.

Enter password again: *[your entry will not echo]*

Changing the configuration password...

Be patient. It might take a while...

Preparing backup...

Creating backup...

Done

Removing backup...

Done

Configuration password changed

ACMEPACKET#

Setting a Protected Configuration Password: Mismatched Configurations

When the saved and active configuration are out of sync, the Net-Net SBC requires you to correct the condition by activating the configuration (using the ACLI **activate-config** command). Once this is complete, you can carry out the process for setting a protected configuration password.

To set a protected configuration password when the saved and active configurations are different:

1. In Superuser mode, type **secret config** at the system prompt and press <Enter>.
 ACMEPACKET# **secret config**

- The Net-Net SBC issues a warning for the change you are about to make, and asks you to confirm whether or not you want to proceed. Type a y and press <Enter> to continue; type an n and press <Enter> to abort the process.

WARNING:

Proceed with caution!

Changing the configuration password will result in any previous backup/archive configuration unusable.

You also need to change the password on any stand-by SDs when you have changed the password successfully

Are you sure [y/n]?: y

Currently active (137) and saved configurations (138) do not match!

To sync & activate, run 'activate-config' or 'reboot activate'.

ACMEPACKET#

- Use the **activate-config** command to synchronize the saved and active configurations.

*ACMEPACKET# **activate-config**

Activate-Config received, processing.

waiting 120000 for request to finish

Request to 'ACTIVATE-CONFIG' has Finished,

Activate Complete

- Continue with the process described in the <Link>Setting a Protected Configuration Password: Matching Configurations (246).

Setting a Protected Configuration Password: Committing Changes

This section describes the process of committing the changes you have made by saving and activating configurations when both the configuration data and password have been updated. Committing the changes means saving and activating your configuration.

To commit your protected configuration password changes:

- Carry out the process described in the <Link>Setting a Protected Configuration Password: Matching Configurations (246).
- After you have finished and the system is done creating a backup, the system reminds you that you need to save and activate.

Preparing backup...

Creating backup...

Done

updating cert-record name: end

updating cert-record name: ca

updating security-association name: sa1

Removing backup...

Done

WARNING:

Configuration changed, run 'save-config' and

'activate-config' commands to commit the changes.

3. Save your configuration using the save-config command.

```
ACMEPACKET# save-config
Save-Config received, processing.
waiting 1200 for request to finish
Copy OK: 8516 bytes copied
Copy OK: 8517 bytes copied
Request to 'SAVE-CONFIG' has Finished,
Save complete
```
4. Activate your configuration using the activate-config command.

```
*ACMEPACKET# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

Changing Protected Configuration Password on a Standby System in an HA Node

When changing the protected configuration password for an HA node, you carry out the <Link>Setting a Protected Configuration Password: Matching Configurations (246) process (or one of the related processes) on the active system, and then must manually change it on the standby. However, changing the protected configuration password on the standby is an abbreviated process.

To change the protected configuration password on a standby system in an HA node:

1. On the stand-by system, delete the configuration using the delete-config command.

```
ACMEPACKET2# delete-config
```
2. On the active system, update the configuration password.

```
ACMEPACKET1# secret config
```

Carry out all of the subsequent confirmations, paying close attention to the warnings.
3. On the stand-by system, update the configuration password. Ensure that the password you set on the stand-by matches the password you set on the active system

```
ACMEPACKET2# secret config
```

Carry out all of the subsequent confirmations, paying close attention to the warnings.
4. On the stand-by system, acquire the configuration from the activate system using the **acquire-config** command.

```
ACMEPACKET2# acquire-config
```
5. Reboot the stand-by system.

```
ACMEPACKET2# reboot
```

Confirming Synchronous Protected Configuration Password and Configuration

To confirm that your protected configuration password and configuration are synchronized:

1. In Superuser mode, type **verify-config** at the system prompt and press <Enter>.


```
ACMEPACKET2# veri fy-confi g
Checking confi gurati on data. . .
OK: confi gurati on password is in sync wi th the confi gurati on data
```

Configuration Migration

This section provides with instructions for how to move your configuration file from one Net-Net SBC to another. Additional checking has been added to the verification and activation processes. To describe how to migrate a configuration, this section uses the designations Net-Net SBC1 and Net-Net SBC2, where:

- Net-Net SBC1 has the configuration you want to copy and move
- Net-Net SBC2 is the system to which you want to migrate the configuration from Net-Net SBC1

Note: For Net-Net OS Release C5.0, the protected configuration password only applies if you are using TLS, IPSec, and/or HDR. The coverage (range of Net-Net SBC configurations) offered by the protected configuration password might expand in the future.

To migrate a configuration from Net-Net SBC1 (where the password configuration has been set) to Net-Net SBC2:

1. Ensure that the protected configuration password on Net-Net SBC1 and Net-Net SBC 2 are the same.
2. On Net-Net SBC1, back up a well-working configuration that you also want to use on Net-Net SBC2. Use the **backup-config** command. The ACLI tells you when the back up has been saved.

```
ACMEPACKET1# back-up confi g copyConfi g1
task done
```

3. On Net-Net SBC2, update the protected configuration password if necessary.
4. On Net-Net SBC2, delete the configuration using the **delete-config** command.

```
ACMEPACKET2# del ete-confi g
```

5. On Net-Net SBC2, use the **restore-backup-config** command with the appropriate file name for the backup from Net-Net SBC1. Save the configuration once the backup is restored.

```
ACMEPACKET2# restore-backup-confi g copyConfi g1
Need to perform save-config and activate/reboot activate for changes
to take effect. . .
task done
```

```
ACMEPACKET2# save-confi g
```

```
Save-Conf i g recei ved, processi ng.
wai ting 1200 for request to fi ni sh
Request to 'SAVE-CONFIG' has Fi ni shed,
Save complete
Currentl y active and saved confi gurati ons do not match!
To sync & activate, run 'acti vate-confi g' or 'reboot acti vate'.
```

6. Before activating the configuration, verify it.

```
ACMEPACKET2# veri fy-confi g
```

...

```

Checking configuration password...
OK: configuration password is in sync with the configuration data
...

```

7. Activate the configuration on Net-Net SBC2.

```

ACMEPACKET2# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete

```

Setting the Password Policy

In the security ACLI path, you will find the **password-policy** configuration. It contains the **min-secure-pwd-len** parameter where you set the length requirement—between 8 and 64 characters—to use for passwords when password secure mode is enabled. For example, if you set this value to 15, then your password must be a minimum of 15 characters in length.

To set the minimum password length to use for password secure mode:

1. In Superuser mode, type **configure terminal** and press <Enter>.


```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```
2. Type **security** and press <Enter>.


```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```
3. Type **password-policy** and press <Enter>.


```
ACMEPACKET(system-config)# password-policy
ACMEPACKET(password-policy)#
```
4. **min-secure-pwd-len**—Enter a value between 8 and 64 characters that defines the minimum password length to use when in password secure mode. This parameter defaults to 8.

Save and activate your configuration.

System Time

There are several reasons why your Net-Net SBC needs to keep an accurate reference to the system time. These include, but are not limited to, the need for accurate billing, logging, and the need to stay synchronized with other network equipment.

Setting Time

To manually set the system-time on your Net-Net SBC:

1. In the ACLI at the superuser prompt, enter the **sys time-set** command and press <Enter>. Enter the Date and Time in the exact format shown on the screen. Remember to use 24-hour time when entering the time. You will be given a chance to confirm your change. Type Y followed by <enter> to confirm.


```

ACMEPACKET# sys time-set
Date YYYY MM DD: 2005 01 26
Time HH MM: 16 05

```

WARNING: Changing the time can have an adverse effect on session processing

Do you want to continue [y/n]?: y

Setting time to: WED JAN 26 16:05:00 2000
ACMEPACKET#

Setting Timezone

You can set the timezone and daylight savings time schedule from the ACLI. This action requires superuser access. The timezone has to be set yearly, if the timezone that you are in uses daylight savings time and the day and/or time when daylight savings starts or ends is different from year to year. You don't have change the timezone-set parameter if your timezone does not use daylight savings time.

1. In the ACLI at the superuser prompt, enter the timezone-set command and press <enter>. Enter the timezone parameters in the exact format as shown on the screen. You need to enter all of the required information to set up the timezone and daylight savings schedule.

```
ACMEPACKET# timezone-set
Timezone name: EST
Minutes from UTC (negative if past UTC): -300
Date and hour daylight saving time begins (mm dd HH): 04 03 02
Date and hour daylight saving time ends (mm dd HH): 10 30 02
ACMEPACKET#
```

Displaying the System Timezone

You can display the timezone configured for your Net-Net SBC using the ACLI show timezone command. It displays the information you set with the timezone-set command.

The following is an example of the displayed information, including the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time:

```
ACMEPACKET# show timezone
Timezone name: EST
Minutes from UTC (negative if past UTC): -300
Date and hour daylight saving time begins (mm dd HH): 04 03 02
Date and hour daylight saving time ends (mm dd HH): 10 30 02
ACMEPACKET#
```

NTP Synchronization

This section provides information about how to set and monitor NTP on your Net-Net SBC.

When an NTP server is unreachable or when NTP service goes down, the Net-Net SBC generates traps for those conditions. Likewise, the Net-Net SBC clears those traps when the conditions have been rectified. The Net-Net SBC considers a configured NTP server to be unreachable when its reach number (whether or not the NTP server could be reached at the last polling interval; successful completion augments the number) is 0. You can see this value for a server when you use the ACLI **show ntp servers** command.

- The traps for when a server is unreachable and then again reachable are:
apSysMgmtNTPServerUnreachabl eTrap and
apSysMgmtNTPServerUnreachabl eClearTrap

- The traps for when NTP service goes down and then again returns are:
apSysMgmtNTPServiceDownTrap and apSysMgmtNTPServiceDownClearTrap

Setting NTP Synchronization

If your Net-Net SBC requires time-critical processing, you can use NTP for time synchronization. Setting NTP synchronizes both hardware and software clocks with the reference time from an NTP server that you specify. NTP is most useful for synchronizing multiple devices located on one network or across many networks to a reference time standard.

To guard against NTP server failure, NTP is restarted periodically to support the dynamic recovery of an NTP server.

You can only set NTP synchronization from the ACLI, but you can view it from the EMS. NTP is RTC-supported as of Net-Net OS Release C5.1.

To set NTP synchronization:

1. In the ACLI's configure terminal section, type **ntp-sync** and press <Enter> to access the NTP configuration. For example:

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# ntp-sync
ACMEPACKET(ntp-config)#
```

2. To add an NTP server, type **add-server**, a <Space>, the IPv4 address of the server, and then press <Enter>.

For example, this entry adds the NTP server at the Massachusetts Institute of Technology in Cambridge, MA:

```
ACMEPACKET(ntp-config)# add-server 18.26.4.105
```

3. To delete an NTP server, type **delete-server** and the IPv4 address of the server you want to delete, and then press <Enter>.

```
ACMEPACKET(ntp-config)# delete-server 18.26.4.105
```

Monitoring NTP from the ACLI

NTP server information that you can view with the new **show ntp servers** command tell you about the quality of the time being used in terms of offset and delays measurements. You can also see the maximum error bounds.

When you use this command, information for all configured servers is displayed. Data appears in columns that are defined in the table below:

Display Column	Definition
server	Lists the NTP servers configured on the Net-Net SBC by IP address. Entries are accompanied by characters: <ul style="list-style-type: none"> • Plus sign (+)—Symmetric active server • Dash (—)—Symmetric passive server • Equal sign (=)—Remote server being polled in client mode • Caret (^)—Server is broadcasting to this address • Tilde (~)—Remote peer is sending broadcast to * • Asterisk (*)—The peer to which the server is synchronizing
st	Stratum level—Calculated from the number of computers in the NTP hierarchy to the time reference. The time reference has a fixed value of 0, and all subsequent computers in the hierarchy are n+1.
poll	Maximum interval between successive polling messages sent to the remote host, measured in seconds.

Display Column	Definition
reach	Measurement of successful queries to this server; the value is an 8-bit shift register. A new server starts at 0, and its reach augments for every successful query by shifting one in from the right: 0, 1, 3, 7, 17, 37, 77, 177, 377. A value of 377 means that there have been eight successful queries.
delay	Amount of time a reply packet takes to return to the server (in milliseconds) in response.
offset	Time difference (in milliseconds) between the client's clock and the server's.
disp	Difference between two offset samples; error-bound estimate for measuring service quality.

To view statistics for NTP servers:

- At the command line, type **show ntp servers** and press <Enter>.

```
ACMEPACKET# show ntp servers
NTP Status                                FRI APR 11: 09: 50 UTC 2007

server                st  poll  reach  delay  offset  disp
-----
*64. 46. 24. 66       3   64   377  0.00018 0.000329 0.00255
=61. 26. 45. 88       3   64   377  0.00017 0.002122 0.00342
```

You can see the status of NTP on your system by using the **show ntp status** command. Depending on the status of NTP on your system, one of the following messages will appear:

- NTP not configured
- NTP Daemon synchronized to server at [the IP address of the specific server]
- NTP synchronization in process
- NTP down, all configured servers are unreachable

To view the status of NTP on your Net-Net SBC:

- At the command line, type **show ntp status** and press <Enter>.

```
ACMEPACKET# show ntp status
```

System Task Management

It is useful to directly control the tasks and processes that are running on your Net-Net system. For example, you might need to terminate a hung task.

The Net-Net SBC also offers several debugging features such as: listing the stack contents, viewing stack traces and task control blocks, and configuring task-specific logs.

Viewing Tasks

There are many tasks or processes running in the background on your Net-Net SBC. You can view information about the currently running tasks from the ACLI.

1. In the ACLI at the superuser prompt, enter the **check-stack** command and press <Enter>. The stacks for all tasks are printed to the screen so that you can view information about current processes running on the Net-Net SBC.

ACMEPACKET# check-stack							
NAME	ENTRY	TID	SIZE	CUR	HIGH	MARGIN	
tMgrTask	mgrTask	0x212ed90	12240	392	440	11800	
tExcTask	excTask	0x2130ba0	8144	280	752	7392	
tLogTask	logTask	0x2134c80	8144	312	360	7784	
tNpwbTmr	0x0000776828	0x219e9c0	20432	168	5016	15416	
tCli	cliInterface	0x2186870	65488	3136	11920	53568	
tCliTelnet	cliInterface	0x22c2ad0	65488	1992	10680	54808	

This command displays a summary of stack usage for a specified task, or for all tasks if no argument is entered. The command output includes task name (NAME), the entry (ENTRY), the task identification (TID), the total stack size (SIZE), the current number of stack bytes used (CUR), the maximum number of stack bytes used (HIGH), and the number of bytes never used at the top of the stack (MARGIN).

Setting Task Log Levels

Logging tasks is essential for debugging problem configurations on your Net-Net SBC.

The log setting changes made via the ACLI's **log-level** commands are not persistent after a Net-Net system reboot. Upon reboot, you need to change the log settings in the system-config element in order for them to be persistent. See the Net-Net ACLI Reference Guide for the default log levels associated with each configuration element.

You can set log levels globally for all tasks or on a task-by-task basis.

To set log levels globally:

1. In the ACLI at the Superuser prompt, enter the **log-level all** command, followed by the Acme Packet logging severity level the system should set all processes to. Refer to the following table for an explanation of logging levels, which can be entered in either numerical or English format.

```
ACMEPACKET# log-level all 4
```

To set log levels for a specified task:

1. In the ACLI at the superuser prompt, enter the **log-level** command followed by a specific task name and then the Acme Packet logging severity level to set this process to. Refer to the following table for an explanation of logging levels. Log levels can be entered in either numerical or English format.

```
ACMEPACKET# log-level mbcld minor
```

The following table defines the syslog levels by severity and number against the Acme Packet log enumeration. For more information regarding the syslog severities, refer to IETF RFC 3164, "The BSD syslog Protocol."

Acme Packet syslog Level (numerical code)	syslog Severity Level (number) From RFC 3164	Acme Packet Code Description
Emergency (1)	Emergency (0)	The EMERGENCY syslog level signifies the utmost severity. These situations require immediate attention. If you do not attend to these types of conditions immediately, there will be physical, permanent, and irreparable damage to your Net-Net system.
Critical (2)	Alert (1)	The CRITICAL syslog level signifies a serious condition within the Net-Net system. These situations require attention as soon as they are noted. If you do not attend to these conditions immediately, there may be physical, permanent, and irreparable damage to your Net-Net system.
Major (3)	Critical (2)	The MAJOR syslog level signifies that functionality has been seriously compromised. As a result, these situations may cause loss of functionality, hanging applications, and dropped packets. If you do not attend to these situations, your Net-Net system will suffer no physical harm, but it will cease to function.
Minor (4)	Error (3)	The MINOR syslog level signifies that functionality has been impaired to a certain degree. As a result, you may experience compromised functionality. There will be no physical harm to your Net-Net system. However, you should attend to these types of conditions as soon as possible in order to keep your Net-Net system operating properly.
Warning (5)	Warning (4)	The WARNING syslog level signifies those conditions that signal that the system has noted some irregularities in performance. This condition is used to describe situations that are noteworthy. However, you should attend to these conditions in order to keep your Net-Net system operating properly.
Notice (6)	Notice (5)	These log levels are used for Acme Packet customer support purposes.
Info (7)	Informational (6)	These log levels are used for Acme Packet customer support purposes.
Trace (8) Debug (9)	Debug (7)	These log levels are used for Acme Packet customer support purposes.

Stopping a Task

The stop-task command shuts down a specified task. You can obtain the identification number of the task you wish to end by using the tcb command. Follow the procedure below to stop a task.

To stop a task:

1. In the ACLI at the superuser prompt, enter the **stop-task** command followed by the name or ID of the task you wish to terminate.

```
ACMEPACKET# stop-task tRadd
ACMEPACKET#
```

Notifying Tasks

The notify command sends a notification to a specific task. Notify commands have different applications and are used as a general method of telling tasks to perform a given action. Several notify applications are presented below. The generalized syntax for using the notify command is:

```
noti fy <task_name> <acti on> [<arguments>...]
```

Tracing Sockets

The notify command is used for runtime protocol tracing for UDP/TCP sockets. This use of the command provides for all protocol messages for ServiceSocket sockets to be written in a log file or sent out of the Net-Net system to a UDP port. This mechanism allows for tracing to be enabled for any socket, provided that the class has a "logit" method for displaying and formatting the protocol message. All ACP classes support this, as do SIP and MGCP. Tracing can be enabled for all processes, specific sockets, all sockets, or specific processes. Tracing for specific sockets is specified by the local IPv4 address and port on which the socket is connected.

```
noti fy all |<process-name> trace all |<socket-address><file-name>
[<outudp-port>]
noti fy all |<process-name> notrace all |<socket-address>
```

The <socket-address> is the IPv4 address and the port on which the socket is connected. The <out-udp-port> is the UDP IPv4 address and port to which the log messages are sent. If the <out-udp-port> is not specified, the logs are written to the <filename>.

Notify Subcommands

The table below lists and defines the subcommands and additional capabilities that are included in the notify command.

notify Subcommand	Description
ALGD	
notify algd nolog	This command disables the logging of MIBOCO messages exchanged with MBCD and MGCP messages processed by the algd task (i.e., these messages appear to originate from and be sent to the loopback interface).
notify algd log	This command enables the logging of MIBOCO and MGCP messages in the alg.log.
notify algd mgcp-endpoint:<endpoint id>	This command deletes the session and the corresponding gateway entries for a specific gateway. The "endpointid" value is the endpoint name the Net-Net SBC receives in the Audit Name field of the RSIP. If a gateway has multiple endpoints, then the last endpoint that sent the RSIP should be used as the endpoint ID.
BERPD	

notify Subcommand	Description
notify berpd force	This command is used to perform a manual switchover between Net-Net systems in HA architectures, regardless of the Net-Net system on which the command is executed (active or standby). This command forces the active Net-Net system into the Standby state and forces the standby Net-Net system into the Active state.
MBCD	
notify mbcd nolog	This command disables MIBOCO logging.
notify mbcd log	This command enables MIBOCO logging in the miboco.log.
notify mbcd debug	This command sets the log level for MBCD for debugging purposes. Unless a specific log type is specified, this command will use its defaults: FLOW and MEDIA.
notify mbcd nodebug	This command disables setting the log level for MBCD. This command is used for debugging purposes.
RADD	
notify radd reload	This command changes the configurations for RADIUS dynamically by reloading the configuration data in the account-config.
SIPD	
notify sipd reload	This command allows you to reload SIPd and thereby update its running state with the latest configuration changes. This command cannot tear down any in-progress sessions, and it cannot tear down any listening sockets. For example, if the previously configured SIP port is 5060 and you edit the configuration and change the port to 5061, both 5060 and 5061 will be listening ports. This command only adds the new listening port to the SIP functionality and does not overwrite the previous one. Calls in progress remain up.
notify sipd nosiplog	This command disables logging SIP and MIBOCO messages, including SIP messages as seen from the Net-Net system SIP proxy's perspective (i.e., all messages are seen coming from and going to home realm addresses) and MIBOCO messages exchanged with the MBCD to manage flows.
notify sipd siplog	This command enables the logging of SIP and MIBOCO messages in the sipmsg.log.
notify sipd report	This command writes all SIP process statistics to the log file.
notify sipd dump limit	This command writes CPU limit information to the log file.
notify sipd debug	This command sets the log level for the SIP protocol for some SIP activity. This command is used for debugging purposes. Unless a specific log type is specified, this command uses its defaults: SIP, SESSION, TRANS, SIPNAT, and MEDIA.
notify sipd nodebug	This command disables setting the log level for the SIP protocol for some SIP activity. This command is used for debugging purposes.

Viewing Power Supply and RAMdrive Status

The **show power** command allows you to view Net-Net SBC power supply information including the state of the power supply and the installation position.

```
ACMEPACKET# show power
Power Supply A (left): ON
Power Supply B (right): OFF or Not Present
```

Displays RAMdrive usage, including the log cleaner threshold values and the size of the most recently saved configuration.

ACMEPACKET# **show ramdrv**

Directory	#Files	Bytes	Clusters	Percent
logs	39	4447497	8712	3
H323CfgFile	1	454	1	0
running	0	0	0	0
data	0	0	0	0
collect	21	10752	21	0
./	4	33114	67	0
Total	70	4494377	8806	3
Free		127587328	-	96

log-min-free=39631230(30%)

log-min-check=66052050(50%)

log-max-usage=66052050(50%)

Rebooting the Net-Net SBC

The **reboot** command is used to reboot the Net-Net SBC system. There are three modes you can use to reboot your Net-Net SBC. Different modes determine which configurations are used to boot your system.

reboot activate

The **reboot activate** command reboots the Net-Net system with the last saved current configuration. This command is useful if changes have been made and saved to the Net-Net system configuration but that configuration has not yet been activated and the Net-Net system goes out of service.

In terms of making the current configuration into the running configuration, using this command is the same as using the **activate-config** command.

reboot force

The **reboot force** command reboots the Net-Net system using the last running configuration. This command does not require you confirm the reboot directive. The boot sequence begins immediately after issuing this command.

reboot force activate

The **reboot force activate** command reboots the Net-Net system using the last saved current configuration. This command does not require you confirm the reboot directive. The boot sequence begins immediately after issuing this command.

Like the **reboot activate** command, **reboot force activate** allows you to activate the current configuration that has been saved but not previously activated. Reboot **force**

activate is the same as issuing the **activate-config** command and then a **reboot force**.

reboot Subcommand	Description
reboot activate	This subcommand reboots the Net-Net SBC and activates the newly saved configuration.
reboot force	This subcommand reboots the Net-Net SBC and loads the last running configuration without confirmation.
reboot force activate	This subcommand reboots the Net-Net SBC and activates the newly saved configuration without confirmation.

Reboot Safeguards

The ACLI's reboot command has safeguards to prevent it from being executed in one ACLI session when certain key processes are in progress in another ACLI session.

Attempting to reboot the Net-Net SBC while a key process is in progress in another ACLI session will result in a warning and notification message that appears on the console. The message informs you that another ACLI session is manipulating the system configuration if any of the following commands/processes are executed:

- save-config
- backup-config
- restore-backup-config
- delete-backup-config
- delete-config

Reboot Status File

The **delete-status-file** command removes the taskcheckdump.dat and statsDump.dat files on the Net-Net SBC. These files contain information from Net-Net SBC system failures.

The Net-Net system writes status information to the statsDump.dat file before the system reboots itself. Acme Packet uses the status file to gather information about why a system rebooted itself for debugging and/or customer service purposes. To carry out this command, type **delete-status-file** into the command line and press <Enter>.

Warning on Reboot

The Net-Net SBC issues a warning when you attempt to reboot the system without having saved configuration changes. If you encounter this warning, you can simply save your configuration (using the ACLI **save-config** command), and then proceed with the reboot. If you want to reboot without saving changes, you can confirm to the reboot but any changes to the configuration (made since the last save) will be lost).

System Watchdog Timer

The Net-Net SBC's watchdog timer ensures that the system will reset itself if it becomes unstable. If a set period of time elapses before the timer is reset by another process, the Net-Net system will initiate a hardware reset. The watchdog timer expires after 31 seconds. This period is not configurable.

The watchdog process runs at a very high priority so that it is always active. As long as other essential processes are running, the watchdog timer will be reset before it expires. If an essential system process encounters a problem, forcing the system software to hang or enter into an unstable state, the watchdog timer will not be reset. As a consequence, the watchdog timer will expire, and the system will reboot.

Watchdog Timer Configuration

The watchdog timer has the following five configuration features:

1. The watchdog state is persistent across reboot.
2. The watchdog timer is disabled by default.
3. Changes to the watchdog timer state are activated in real time.
4. The watchdog timer state can only be changed from ACLI Superuser mode.
5. The watchdog timer state can be viewed from ACLI Superuser and User modes.

Availability

Available in build sd201p29

ACLI Example

The following template shows the usage of the watchdog command.

```
ACMEPACKET# watchdog [enable | disable | fetch]
```

- enable—enables the watchdog timer
- disable—disables the watchdog timer
- fetch—prints the current state of the watchdog timer to the screen

To enable the watchdog timer on your Net-Net SBC:

1. Enter the Superuser mode in the ACLI.

```
ACMEPACKET#
```

2. Type **watchdog <space> enable** and press <Enter> to enable the watchdog timer.

```
ACMEPACKET# watchdog enable
```

```
Watchdog timer started
```

```
ACMEPACKET#
```

3. Type **watchdog <space> fetch** and press <Enter> to confirm that the watchdog timer has been enabled.

```
ACMEPACKET# watchdog fetch
```

```
Watchdog timer is enabled
```

```
ACMEPACKET#
```

Configuring the Front Panel Interface

You can quickly configure the front-panel media interfaces on the Net-Net SBC using the **set-front-interface** command located in the topmost level of the ACLI when you are in Superuser mode.

```
set-front-interface parameter <slot> <port> state
```

When configuring front ports, you must identify the port and slot pair. The conventions you must use are:

- Slot: The Net-Net SBC accepts two PHY cards. When facing the front of the Net-Net SBC, the left card is Slot 0, and the right card is Slot 1.
- Port: Net-Net SBC's PHY cards have either 1, 2, or 4 ports. When facing the front of the Net-Net SBC, the leftmost port is Port 0, and the rightmost port is either Port 0 (for a 1 port card), Port 1 (for a 2 port card), or Port 3 (for a 4 port card).

Front interfaces configured by using the **set-front-interface** command are not persistent after a reboot. You can also configure front interfaces by using the standard configuration elements and followed by the **activate-configuration** command.

The following sections describe the parameters available for the **set-front-interface** command.

admin-state

This parameter enables or disables administrative state for the front interfaces. Admin-state turns a port and slot pair on or off. If enabled, the port and slot pair can pass traffic. If disabled, the port and slot pair can not pass traffic.

```
set-front-interface admin-state 0 1 enabled
```

auto-negotiation

This command enables or disables the auto-negotiation protocol for front interfaces, both 10/100 and GigE. Auto-negotiation is used by the NICs to provision bandwidth and duplex mode for optimum speed between two sides of a physical link. If enabled, the port and slot pair are set to use auto-negotiation. If disabled, the port and slot pair are set to not use auto-negotiation.

```
set-front-interface auto-negotiation 0 1 enabled
```

If auto-negotiation is enabled, the duplex-mode and speed parameters do not need to be set.

duplex-mode

This command sets either full-duplex mode or half-duplex mode for the front interfaces on 10/100 ethernet cards. The duplex mode determines if traffic can flow bidirectionally or not. If set to FULL, the identified port will run in full-duplex mode. If set to HALF, the identified port will run in half-duplex mode.

```
set-front-interface duplex-mode 0 1 full
```

speed

This command sets a port and slot pair to either 10 Mbps or 100 Mbps. It is only applicable for front interfaces on 10/100 physical layer cards. If set to 10, the identified port and slot pair will operate at 10 Mbps. If set to 100, the identified port and slot pair will operate at 100 Mbps.

```
set-front-interface speed 0 1 100
```

ARP Information

The ACLI's ARP commands are used to associated IPv4 addresses (Layer 3) with Ethernet MAC addresses (Layer 2). You can view the ARP table, add or remove an entry, or test an entry.

show arp

The **show arp** command is one of the many **show** commands available to you on the Net-Net SBC. It displays the Link Level ARP table, ARP entries, and ARP table statistics. An example output is shown below.

ACMEPACKET# **show arp**

LINK LEVEL ARP TABLE						
destination	gateway	flags	Refcnt	Use	Interface	
172.30.0.1	00:0f:23:4a:d8:80	405	1	0	wancom0	

Total ARP Entries = 3

Intf	VLAN	IP-Address	MAC	time-stamp	type
0/0	0	010.000.045.001	00:00:00:00:00:00	1106930884	invalid

Special Entries:

0/0	0	000.000.000.000	00:00:00:00:00:00	1106930884	gateway
0/0	0	010.000.045.000	00:00:00:00:00:00	1106930884	network

Gateway Status:

Intf	VLAN	IP-Address	MAC	time-stamp	hb	status
0/0	0	010.000.045.001	00:00:00:00:00:00	1106930884		unreachable

-- ARP table info --

```
Maximum number of entries : 512
Number of used entries    : 3
Length of search key      : 1 (x 64 bits)
First search entry address : 0x3cb0
length of data entry      : 2 (x 64 bits)
First data entry address  : 0x7960
Enable aging              : 0
Enable policing           : 0
```

ACMEPACKET#

arp-add

The **arp-add** command allows you to add ARP entries into the ARP table. Since some network devices do not support ARP, static ARP entries sometimes need to be added to the ARP table manually. The syntax for using the **arp-add** command is:

```
arp-add <slot> <port> <vlan-id> <IP address> <MAC address>
```

If there is no VLAN tagging on this interface, set vlan-id to 0.

arp-delete

The **arp-delete** command allows you to remove ARP entries from the ARP table. You only need to identify the IPv4 address, VLAN tag, and slot and port pair to be removed. The syntax for using the **arp-delete** command is:

```
arp-delete <slot> <port> <vlan-id> <IP address>
```

arp-check

The **arp-check** command allows you to test a particular address resolution. When this command is carried out, a test message is sent. The test is successful when an OK is returned. If there is no VLAN identifier to be entered, then enter a value of 0. The syntax for using the **arp-check** command is:

```
arp-check <slot> <port> <vlan-id> <IP address>
```

NAT Information

The ACLI can display NAT table information and the NAT table itself in a variety of formats: by entry range, by table entry range in tabular form, by matching source and destination addresses. This information is used primarily for debugging purposes.

NAT information is displayed using the **show nat** command with the appropriate arguments.

show nat info

The **show nat info** command allows displays general NAT table information. The output is used for quick viewing of a Net-Net system's overall NAT functions, including the maximum number of NAT table entries, the number of used NAT table entries, the length of the NAT table search key, the first searchable NAT table entry address, the length of the data entry, the first data entry address, and whether or not aging and policing are enabled in the NAT table.

```
ACMEPACKET# show nat info
-- NAT table info --
Maximum number of entries : 7768
Number of used entries    : 0
Length of search key      : 2 (x 64 bits)
First search entry address : 0x0
Length of data entry      : 4 (x 64 bits)
First data entry address  : 0x0
Enable aging              : 1
Enable policing           : 0
ACMEPACKET#
```

show nat by-addr

The **show nat by-addr** command displays NAT table information that matches source and destination addresses. When using this command, you can specify the entries to display according to source address (SA) and/or destination address (DA) values.

The Net-Net system matches these values to the NAT table entries and shows the pertinent information. If no addresses are entered, the Net-Net system shows all of the table entries. NAT entries can be matched according to SA or DA or both.

```
show nat by-addr <source IPv4 address> <destination IPv4 address>
```

The table below explains the output of the **show nat by-addr** command.

Parameter	Description
SA_flow_key	Source IPv4 address key used for matching in the look-up process.
DA_flow_key	Destination IPv4 address key used for matching in the look-up process.
SP_flow_key	UDP source port used for matching in the look-up process.
DP_flow_key	UDP destination port used for matching in the look-up process.
VLAN_flow_key	If this is a non-zero value, then there is an associated VLAN. If this value is zero, then there is no associated VLAN.

Parameter	Description
SA_prefix	These values determine how many bits in the key are considered in the look-up process for a match, where SA is the source IPv4 address, DA is the destination IPv4 address, SP is the UDP source port, and DP is the UDP source port.
DA_prefix	
SP_prefix	
DP_prefix	
Protocol_flow_key	This value stands for the protocol used, where the following values and protocols correspond: <ul style="list-style-type: none"> • 1 = ICMP • 6 = IP • 17 = UDP
Ingress_flow_key	This value uniquely identifies from where the packet came, and it is a combination of the Ingress Slot and Ingress Port values.
Ingress Slot	Together with the Ingress Port, this value makes up the Ingress_flow_key.
Ingress Port	Together with the Ingress Slot, this value makes up the Ingress_flow_key.
XSA_data_entry	This is the translated (i.e., post-lookup) source IPv4 address value.
XDA_data_entry	This is the translated (i.e., post-lookup) destination IPv4 address value.
XSP_data_entry	This is the translated (i.e., post-lookup) source port value.
XDП_data_entry	This is the translated (i.e., post-lookup) destination port value.
Egress_data_entry	This value uniquely identifies the outbound interface for the packet, and it is a combination of the Egress Slot and Egress Port values. This is the functional equivalent to the Ingress_flow_key.
Egress Slot	Together with the Egress Port, this value makes up the Egress_data_entry.
Egress Port	Together with the Egress Slot, this value makes up the Egress_data_entry.
flow_action	This value displays the defined flow_action (i.e., flag) bits. The flow action bit mask includes the following bit options: <ul style="list-style-type: none"> • bit 1 - 1=MPLS strip • bit 2 - 1=Diffserv clear • bit 5 - 1=Latch source address • bit 6 - 1=Collapse flow • bit 7 - 1=Slow Path • bit 8 - 1=QoS Requirement • bit 9 - 1=RTCP, 0=RTP is bit 8 is set • bit 10 - 1=packet capture if bit 8 is set • bit 11 - 1=full packet capture, 0=header packet capture, if bit 9 is set Bits 8 through 11 only apply to QOS.
optional_data	This value is related to the flow_action value. If the flow_action Slow Path bit (bit 7) is set, then the optional_data value is the UDP destination port for delivery to the host. The optional_data value may also contain DSCP markings.
VLAN_data_entry	This value refers to the outbound VLAN look-up process. A non-zero value means that there is an associated VLAN, while a zero value means that there is no associated VLAN.
host_table_index	This value refers to the virtual index for the host management of CAM processing.
init_flow_guard	This timer is used to age the entries in the CAM.

Parameter	Description
<code>inact_flow_guard</code>	This timer is used to age the entries in the CAM.
<code>max_flow_guard</code>	This timer is used to age the entries in the CAM.

In the above table, the following values are equivalent:

- SA = Source IPv4 Address
- DA = Destination IPv4 Address
- SP = UDP Source Port
- DP = UDP Destination Port
- X = Translated

Using a zero in the source address location of the command execution line is a wildcard value. This is used for displaying NAT information by destination address only.

show nat by-index

The **show nat by-index** command displays a specified range of entries in the NAT table, with a maximum of 5024 entries. The syntax for using the **show nat by-index** command is:

```
show nat by-index <starting entry> <ending entry>
```

To view lines 10 through 50 of the NAT table, you would enter the following:

```
show nat by-index 10 50
```

If you do not specify a range, the system uses the default range of 1 through 200. The range you enter corresponds to line numbers in the table, and not to the number of the entry itself.

show nat in-tabular

The **show nat in-tabular** command displays a specified range of entries in the NAT table display in table form, with a maximum of 5024 entries. This tabular output allows for ease in viewing the sometimes lengthy NAT table information. The syntax is modeled on the **show nat by-index** command:

```
show nat in-tabular 10 50
```

In this abbreviated display, the fields that are shown for each NAT entry are:

- SA_key—equivalent to SA_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- DA_key—equivalent to DA_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- SP_key—equivalent to SP_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- DP_key—equivalent to DP_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- VLAN_key—equivalent to VLAN_data_entry in other **show nat** commands.
- ING—equivalent to Ingress_flow_key in other **show nat** commands.
- PROTO—equivalent to Protocol_flow_key in other **show nat** commands.

- WEIGHT—Flow weight.

The display of the show nat in-tabular requires a 132-column display. Please adjust your terminal program appropriately.

SNMP Community and Trap Receiver Management

You can view and reset the counters for SNMP community table and SNMP trap receivers using the ACLI commands described in this section.

SNMP Community Table

The SNMP community table stores information about the SNMP servers that you configure. These configurations set the community name and define what kind of information that server can access.

show snmp-community-table

The **show snmp-community-table** command displays all of the configuration information for the SNMP community. It also shows the total responses in and total responses out. Type **show snmp-community-table** followed by pressing <Enter> in the ACLI to use this command. For example:

```
ACMEPACKET# show snmp-communi ty-table
communi ty-name : publ ic
access-mode      : READ-ONLY
ip-addresses     : 10. 0. 200. 61
                  172. 30. 0. 13
total requests in : 111
total responses out : 111

communi ty-name : test
access-mode      : READ-ONLY
ip-addresses     : 172. 30. 0. 13
                  10. 0. 200. 61
total requests in : 21
total responses out : 21

communi ty-name : test1
access-mode      : READ-ONLY
ip-addresses     : 10. 0. 200. 61
                  172. 30. 0. 13
total requests in : 101
total responses out : 101
```

reset snmp-community-table

You can specifically reset the counters on SNMP community table statistics by using the ACLI **reset snmp-community-table** command. This set of statistics also resets when you use the ACLI **reset all** command.

```
ACMEPACKET# reset snmp-communi ty-table
```

Trap Receiver

The trap receiver is a network management system (NMS) to which the Net-Net SBC sends SNMP traps to report system events. The SNMP agent uses trap receiver information that you configure to send traps to NMSs.

When you use the ACLI **show trap-receiver** table command, the Net-Net system displays all of the configuration information for the SNMP community and the total number of traps sent to it.

show trap-receiver

The **show trap-receiver** command displays all of the configuration information for the SNMP community and the total number of traps sent to it. For example:

```
ACMEPACKET# show trap-receiver
```

```
community-name : public
filter-level    : All
ip-address      : 10.0.0.43
total traps out : 3
```

```
community-name : test
filter-level    : All
ip-address      : 10.0.200.61
total traps out : 3
```

reset trap-receiver

You can specifically reset the counters for trap receiver statistics by using the ACLI **reset trap-receiver** command. This set of statistics also resets when you use the ACLI **reset all** command.

```
ACMEPACKET# reset trap-receiver
```

Login Banner

You can customize the displayed text banner, visible at the start of each ACLI session on your Net-Net SBC. This feature lets you tailor the appearance of the ACLI's initial login screen to make it more company- or customer-specific. This file is stored in the `/code/banners/` directory, which the system will create for you if it does not exist when you upload the file (called `banner.txt`).

ACLI Audit Trail

You can configure your Net-Net SBC to send a history of all user-entered commands to a common audit log file. When you enable this feature, all commands entered from any ACLI session are written to the `cli.audit.log` file. You can also display the log file using the **show logfile cli.audit** command. In addition, the system records what configuration a user selects when using the **select** command. Prompted passwords are not saved, but the requests for changes to them are.

The `cli.audit.log` file is stored in the log directory, and it is lost when you reboot your system; this file is not available off-box. The ACLI audit trail is enabled by default, but you can turn it off by changing the system configuration's **cli-audit-trail** parameter to `disabled`.

This chapter explains how to access Net-Net 4000 SBC inventory management statistics to review the hardware components and licenses installed on the system, as well as active and stored configurations, and configuration information for specific elements or realms.

Accessing Inventory Management Data

You can access inventory management statistics by using the ACLI show command with different subcommands. You can access all show commands at the User level, you do not need Superuser privileges.

Hardware Inventory

This section describes the statistics you can view about the different Net-Net 4000 SBC hardware components.

Components

You can view hard-coded, programmable read-only memory (PROM) information about the following Net-Net 4000 SBC hardware components:

- mainboard (chassis)
- CPU
- physical interface card 0
- physical interface card 1
- CAM (Net-Net SD2 IDT PROM only)

show prom-info mainboard

Display the mainboard PROM information by using the **show prom-info mainboard** command. For example:

ACMEPACKET# **show prom-info mainboard**

Contents of Main Board PROM

```

Assy, Session Director with CAM
Part Number:                102-1001-00
Serial Number:              010323001127
Functional Rev:             1.18
Board Rev:                  2
PCB Family Type:           Session Director
ID:                         Session Director I
Format Rev:                 3
Options:                    0
Manufacturer:              MSL, Lowell
Week/Year:                  23/2003
Sequence Number:           001127

```

```

Number of MAC Addresses:      16
Starting MAC Address:        00 08 25 01 07 60

```

show prom-info CPU

Display the host CPU PROM information by using the **show prom-info CPU** command. For example:

```
ACMEPACKET# show prom-info CPU
```

Contents of Host CPU PROM

```

Assy, Processor 7455 Daughter Card
Part Number:                002-0300-01
Serial Number:              010303000456
Functional Rev:             1.10
Board Rev:                  4
PCB Family Type:            Session Director
ID:                         Host CPU (7451/7455)
Format Rev:                 3
Options:                    0
Manufacturer:               MSL, Lowell
Week/Year:                  03/2003
Sequence Number:            000456
Number of MAC Addresses:    0
Starting MAC Address:       00 00 00 00 00 00

```

show prom-info PHY0

Display PROM information for the left physical interface card by using the **show prom-info PHY0** command. For example:

```
ACMEPACKET# show prom-info PHY0
```

Contents of PHY0

```

Assy, 1 Port Gigabit Ethernet Multimode Phy
Part Number:                002-0200-01
Serial Number:              010307000645
Functional Rev:             1.07
Board Rev:                  3
PCB Family Type:            Gigabit PHY
ID:                         1 Port Multi-Mode Gigabit
Format Rev:                 3
Options:                    0
Manufacturer:               MSL, Lowell
Week/Year:                  07/2003
Sequence Number:            000645
Number of MAC Addresses:    0
Starting MAC Address:       00 00 00 00 00 00

```

show prom-info PHY1

Display PROM information for the right physical interface card by using the **show prom-info PHY1** command. For example:

```
ACMEPACKET# show prom-info PHY1
```

Contents of PHY1


```

Assy, 1 Port Gigabit Ethernet Multimode Phy
Part Number:                002-0200-01
Serial Number:              010303000406
Functional Rev:             1.07
Board Rev:                  3
PCB Family Type:           Gigabit PHY
ID:                         1 Port Multi-Mode Gigabit
Format Rev:                 3
Options:                    0
Manufacturer:               MSL, Lowell
Week/Year:                  03/2003
Sequence Number:           000406
Number of MAC Addresses:    0
Starting MAC Address:       00 00 00 00 00 00

```

Software Inventory

This section explains how to access information about the Net-Net system image used for booting.

System image

You can display the name the Net-Net system image currently booting on your system by using the following commands:

- **show version**
- **bootparam** (if you have Superuser privileges)

Image Filename: Net-Net 4250 and Net-Net 4500

The output from both commands includes the image filename. If that filename starts with either of the following, the Net-Net 4250 is booting from flash memory:

- For the Net-Net 4250, you can use **/tffs0/** (referring to **/boot**). For the Net-Net 4500, you can use **/boot**.
- **/tffs1/** (referring to **/code**)

For example, **/tffs0/sd200b1.gz**.

If the filename starts with **/tftpboot/**, the Net-Net system is booting from an external device. For example, **/tftpboot/sd200b1.gz**.

Location

The output from both commands also includes a code that signals the Net-Net system from where to boot. The code also signals the Net-Net system about which file to use in the booting process. This sequence always starts with 0x (these flags are hexadecimal). For example, 0x8.

show version image

Display information about the Net-Net system image being booted on your system by using the **show version image** command. For example:

```
ACMEPACKET# show version image
```

```
Acme Packet version 1.0 (for Acme Packet Net-Net).
```

```
Kernel: WIND AE version 1.1.
```

Made on Mar 4 2005, 22:14:04.

Boot line:

```
wancom(0,0)goose: sd201b37.gz e=172.30.55.127:ffff0000 h=172.30.0.125
g=172.30.0.1 u=vxftp pw=vxftp f=0x8 tn=ACMEPACKET
```

The sample output contains the image name (sd201b37.gz) and identifies from where the Net-Net system should boot (f=0x8.) The value f=0x8 indicates the Net-Net 4000 SBC will look at the file name defined in the boot configuration parameters to determine where to boot from and what file to use.

bootparam

Display information about the Net-Net system image being booted on your system by using the **bootparam** command. After you issue the bootparam command, you need to press <Enter> to scroll down the list of boot configuration parameters.

In the following example, the system image is identified as sd201b37.gz and the location from where the Net-Net system should boot is identified by the flag's value, 0x8.

For example:

```
ACMEPACKET(configure)# bootparam

'.' = clear field; '-' = go to previous field; q = quit

boot device           : wancom0
processor number      : 0
host name             : goose
file name             : sd201b37.gz
inet on ethernet (e)  : 172.30.55.127:ffff0000
inet on backplane (b) :
host inet (h)         : 172.30.0.125
gateway inet (g)      : 172.30.0.1
user (u)              : vxftp
ftp password (pw) (blank = use rsh) : vxftp
flags (f)             : 0x8
target name (tn)      : ACMEPACKET
startup script (s)    :
other (o)             :
```

NOTE: These changed parameters will not go into effect until reboot. Also, be aware that some boot parameters may also be changed through PHY and Network Interface Configurations.

Version

You can view operating system (OS) information, including the OS version number and the date that the current copy of the OS was made, by using the **show version** command. For example:

show version

```
ACMEPACKET# show version
ACME Net-Net 4250 Firmware C5.0.0 Build A7
Build Date=03/22/07
```

Configuration Information

This section explains how to access information about the Net-Net system current and running configurations. It also explains how to view configuration information for a specific element or for all elements associated with a specific realm.

Overview

You can display information about your system's configuration by using the following commands:

- **show running-config** displays the configuration currently active and running on the Net-Net SBC.

You can also use subcommands with show running-config to specify the element configuration you want to view. See the table in the following section for a list.

- **show configuration** displays the new configuration or configuration that you are modifying.

You can also use subcommands with show configuration to specify the element configuration you want to view. See the table in the following section for a list.

- **display-running-cfg-version** displays the running configuration's version number.
- **display-current-cfg-version** displays the current configuration's version number.
- **realm-specifics <realm ID>** displays realm-specific configuration based on the input realm ID.

Configuration Show Subcommands

The following table lists the subcommands you can use to specify the configuration element whose configuration you want to view. You use these subcommands with the **show running-config** or **show configuration** commands.

Subcommand	Description
to-file	Send output from this command to a file located on the local flash system file system.
account-config	Account configuration
h323-config	H323 configuration
h323-stack	All h323 stacks
iwf-stack	SIP/H.323 IWF stack
host-route	All host routes
local-policy	All local policies
media-profile	All media profiles
media-manager	Media manager
mgcp-config	MGCP configuration
dns-config	All DNS configurations
network-interface	All network interfaces

Subcommand	Description
ntp-config	NTP configuration
phys-interface	All physical interfaces
realm	All realms
MediaPolicy	All media policies
ClassPolicy	All class policies
redundancy-config	Redundancy configuration
ResponseMap	All response maps
session-agent	All session agents
session-group	All session groups
session-translation	All session translations
translation-rules	All translation rules
session-router	Session router
sip-config	All SIP configurations
sip-feature	All SIP features
sip-interface	All SIP interfaces
sip-nat	All SIP NATs
snmp-community	All SNMP communities
static-flow	All static flows
steering-pool	All steering pools
system-config	System configuration
TrapReceiver	All trap receivers
call-recording-server	All IP call recording servers
capture-receiver	All capture receivers
rph-profile	All RPH profiles
rph-policy	All RPHP policies
password-policy	Password policy
enforcement-profile	All enforcement profiles
realm-group	All realm groups
inventory	Displays an inventory of all configured elements

Running configuration Commands

You can display the entire running configuration or specify the element for which you want to view configuration information. The information in this section includes an example of one of the available **show** subcommands, **media-manager**.

show running-config

Display the configuration currently running on the Net-Net SBC by using the **show running-config** command. A sample of the **show running-config** output is included at the end of this section.

show running-configuration media-manager

Display configuration information for media manager only. For example:

```
ACMEPACKET# show running-config media-manager
media-manager
    state                               enabled
    latching                           enabled
    flow-time-limit                     86400
    initial-guard-timer                 300
    subsq-guard-timer                   300
    tcp-flow-time-limit                 86400
    tcp-initial-guard-timer             300
    tcp-subsq-guard-timer               300
    tcp-number-of-ports-per-flow       2
    hnt-rtcp                           disabled
    algd-log-level                      NOTICE
    mbcdd-log-level                     NOTICE
    red-flow-port                       1985
    red-mgcp-port                       1986
    red-max-trans                       10000
    red-sync-start-time                 5000
    red-sync-comp-time                 1000
    max-signaling-bandwidth             10000000
    max-untrusted-signaling             100
    min-untrusted-signaling             30
    app-signaling-bandwidth             0
    tolerance-window                   30
    rtcp-rate-limit                     0
    min-media-allocation                32000
    min-trusted-allocation              1000
    deny-allocation                     1000
    anonymous-sdp                       disabled
    arp-msg-bandwidth                   32000
    last-modified-date                  2007-04-05 09:27:20
task done
```

display-running-cfg-version

Display the saved version number of the configuration currently running on the Net-Net SBC by using the **display-running-cfg-version** command. For example:

```
ACMEPACKET# display-running-cfg-version
Running configuration version is 3
```

The version number value is incremented by one for each new configuration version.

Configuration Commands

You can display the entire new or modified configuration or you can specify the element for which you want to view configuration information. The information in this section includes an example of one of the available show subcommands, **media-manager**.

show configuration

Display the new or modified configuration that will become the running configuration after you execute the **save-config** and **activate-config** commands. The output for this command is similar to the output for the **show running-config** command. A sample of the **show running-config** output is included at the end of this section.

show configuration media-manager

Display configuration information for media manager only. For example:

```
ACMEPACKET# show configuration media-manager
media-manager
    state                      enabled
    latching                   enabled
    flow-time-limit            86400
    initial-guard-timer        300
    subsq-guard-timer          300
    tcp-flow-time-limit        86400
    tcp-initial-guard-timer     300
    tcp-subsq-guard-timer       300
    tcp-number-of-ports-per-flow 2
    hnt-rtcp                   disabled
    algd-log-level              NOTICE
    mbcdd-log-level             NOTICE
    red-flow-port               1985
    red-mgcp-port               1986
    red-max-trans               10000
    red-sync-start-time         5000
    red-sync-comp-time          1000
    max-signaling-bandwidth     10000000
    max-untrusted-signaling     100
    min-untrusted-signaling     30
    app-signaling-bandwidth     0
    tolerance-window           30
    rtcp-rate-limit             0
    min-media-allocation        32000
    min-trusted-allocation      1000
    deny-allocation             1000
    anonymous-sdp                disabled
    arp-msg-bandwidth           32000
    last-modified-date          2007-04-05 09:27:20
task done
```

display-current-cfg-version

Display the saved version number of the current configuration by using the **display-current-cfg-version** command. For example:

```
ACMEPACKET# display-current-cfg-version
Current configuration version is 4
```

The version number value is incremented by one for each new configuration version.

Realm Specific

You can display configuration information for elements associated with a specific realm.

realm-specifics <realm ID>

Display realm-specific configuration based on the input realm ID by using the **realm-specifics <realm ID>** command. The information displayed includes the following:

- realm configuration
- steering pool
- session agent
- session translation
- class policy
- local policy (if the source realm or destination realm is defined)

For example:

```
ACMEPACKET# realm-specifics testrealm
realm-config
    identifier                testrealm
    addr-prefix               0.0.0.0
    network-interfaces
    mm-in-realm               disabled
    mm-in-network             enabled
    mm-same-ip                enabled
    mm-in-system              disabled
    msm-release               disabled
    qos-enable                disabled
    max-bandwidth             0
    ext-policy-svr            boffo.com
    max-latency               0
    max-jitter                0
    max-packet-loss           0
    observ-window-size        0
    parent-realm
    dns-realm
    media-policy
    in-translated
    out-translated
    in-manipulated
    out-manipulated
    class-profile
    average-rate-limit        0
    access-control-trust-level low
    invalid-signal-threshold  0
    maximum-signal-threshold  0
    untrusted-signal-threshold 758
    deny-period               30
    symmetric-latching        disabled
    pai-strip                 disabled
    trunk-context
    early-media-allow         reverse
    additional-prefixes       10.0.0.0/24
                                172.16.0.0
    restricted-latching       peer-ip
    restriction-mask           17
    accounting-enable         enabled
```

Last-modified-date

2006-07-06 12:43:39

Running Configuration Example

The following example shows the output of the **show running-config** command. All configuration parameters are displayed on the screen. You see similar output when you execute the show configuration command.

```

ACMEPACKET# show running-config access-control
access-control
    real-m-id                RS
    source-address            172.30.1.10
    destination-address       170.30.1.10
    application-protocol      SIP
    transport-protocol        ALL
    access                    permit
    average-rate-limit        30
    trust-level               high
    invalid-signal-threshold  15
    maximum-signal-threshold  60
    untrusted-signal-threshold 0
    deny-period              10
    last-modified-date        2006-07-12 12:56:06
account-config
    hostname                  local host
    port                      1813
    strategy                  Hunt
    state                     enabled
    max-msg-delay             60
    max-wait-failover         100
    trans-at-close            disabled
    file-output               disabled
    max-file-size             1000000
    max-files                 5
    file-rotate-time         60
    ftp-push                  disabled
    ftp-address
    ftp-port                  21
    ftp-user
    ftp-password
    ftp-remote-path
    generate-start            OK
    generate-interim
Reinvite-Response
account-server
    hostname                  172.30.11.15
    port                      1813
    state                     enabled
    min-round-trip            250
    max-inactivity            60
    restart-delay             30
    bundle-vsa                enabled
    secret                    foo
    NAS-ID
account-server
    hostname                  172.30.11.16

```


port	1813
state	enabled
min-round-trip	250
max-inactivity	60
restart-delay	30
bundle-vsa	enabled
secret	foo
NAS-ID	
last-modified-date	2006-03-01 22:37:33
authentication	
source-port	1812
type	local
protocol	pap
certificate-record	
name	
country	US
state	MA
locality	burlington
organization	acme
unit	packet
common-name	ap
key-size	1024
alternate-name	RS
trusted	enabled
h323-config	
state	enabled
log-level	INFO
response-tmo	4
connect-tmo	32
rfc2833-payload	101
alternate-routing	proxy
last-modified-date	2006-07-07 07:49:57
h323-stack	
name	tester
state	disabled
isgateway	enabled
realm-id	test
assoc-stack	acme
local-ip	172.30.1.150
max-calls	100
max-channels	10
registration-ttl	15
terminal-alias	
	e164=17823484839
prefixes	
	url=http://www.acmepacket.com
ras-port	1030
auto-gk-discovery	enabled
multicast	172.30.1.150:11
gatekeeper	170.30.1.150:57
gk-identifier	RS
q931-port	1720
alternate-transport	
	173.30.1.150:15

q931-max-calls	200
h245-tunneling	disabled
fs-in-first-msg	disabled
call-start-fast	enabled
call-start-slow	disabled
media-profiles	
	acme
process-registration	disabled
allow-anonymous	all
proxy-mode	H225
h245-stage	connect
q931-start-port	0
q931-number-ports	0
dynamic-start-port	0
dynamic-number-ports	0
rfc2833-mode	transparent
filename	packet11
tcp-keepalive	disabled
last-modified-date	2006-07-07 08:39:01
enum-config	
name	test
top-level-domain	com
realm-id	test_realm
enum-servers	172.3.11.115
timeout	11
cacheinactivityTimer	3600
last-modified-date	2006-07-07 07:37:11
iwf-stack	
state	disabled
media-profiles	
logging	disabled
last-modified-date	2005-02-15 10:34:41
host-route	
dest-network	10.0.0.0
netmask	255.0.0.0
gateway	172.30.0.1
last-modified-date	2005-01-08 22:40:00
local-policy	
from-address	
	192.168.0.50
to-address	
	10.10.10.10
source-realm	*
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	urgent
last-modified-date	2006-06-12 08:48:57
policy-attribute	
next-hop	172.168.0.10
realm	
action	none
terminate-recursion	enabled
carrier	

start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	
state	enabled
media-profiles	
local-policy	
from-address	
	172.30.1.150
to-address	
	170.30.1.150
source-realm	
	RS
activate-time	2006-07-10 11:38:30
deactivate-time	2006-07-11 11:38:30
state	enabled
policy-priority	normal
last-modified-date	2006-07-10 10:02:52
policy-attribute	
next-hop	172.30.1.150
realm	RS
action	none
terminate-recursion	disabled
carrier	me
start-time	1000
end-time	2000
days-of-week	H, U-S
cost	1000
app-protocol	SIP
state	enabled
media-profiles	
media-profile	
name	RS
media-type	data
payload-type	acme
transport	rtp
req-bandwidth	1000
frames-per-packet	30
parameters	silencesuppression=0
average-rate-limit	60
peak-rate-limit	90
max-burst-size	120
last-modified-date	2006-07-12 13:02:10
media-manager	
state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2

hnt-rtcp	di sabl ed
al gd-log-l evel	NOTI CE
mbcd-log-l evel	NOTI CE
red-fl ow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-ti me	5000
red-sync-comp-ti me	1000
max-si gnal i ng-bandwi dth	10000000
max-untrusted-si gnal i ng	100
mi n-untrusted-si gnal i ng	30
app-si gnal i ng-bandwi dth	0
tol erance-wi ndow	30
rtcp-rate-l i mi t	0
mi n-medi a-al l ocati on	32000
mi n-trusted-al l ocati on	1000
deny-al l ocati on	1000
anonymous-sdp	di sabl ed
arp-msg-bandwi dth	32000
l ast-modi fi ed-date	2007-04-05 09: 27: 20
task done	
mgcp-confi g	
pri vate-real m	RS
pri vate-address	172. 30. 1. 150
pri vate-port	11
publ i c-real m	acme
publ i c-ca-host	packet
publ i c-ca-address	170. 2. 30. 150
publ i c-ca-port	15
publ i c-gw-host	rs
publ i c-gw-address	150. 20. 1. 158
publ i c-gw-port	20
second-publ i c-gw-port	22
al g-port	2427
mode	Li neUni t
di vi sor	256
uni t-prefi x	
audi t-i nterval	0
nat-traversal	di sabl ed
dns-authenti cati on	di sabl ed
dns-transl ati on	
ca-redundancy	di sabl ed
ca-pi ng-method	
ca-pi ng-i nterval	0
ca-fai l over-i p-addresses	
l ast-modi fi ed-date	175. 30. 1. 150
l ast-modi fi ed-date	2006-07-07 12: 42: 25
dns-confi g	
cli ent-real m	dns_real m
descri pti on	test descri p
cli ent-address-l i st	
	10. 0. 0. 1
	192. 168. 10. 1
	17. 16. 0. 1

last-modified-date	2005-02-15 11:33:50
server-dns-attributes	
server-real m	
domain-suffi x	
server-address-l i st	
source-address	
source-port	3973
transacti on-ti meout	19136512
network-i nterface	
name	f00
sub-port-i d	0
hostname	
i p-address	10.10.0.10
pri -uti l i ty-addr	
sec-uti l i ty-addr	
netmask	255.255.0.0
gateway	10.10.0.1
sec-gateway	
gw-heartbeat	
state	di sabl ed
heartbeat	0
retry-count	0
retry-ti meout	1
heal th-score	0
dns-i p-pri mary	
dns-i p-backup1	
dns-i p-backup2	
dns-domai n	
dns-ti meout	11
hi p-i p-l i st	
ftp-address	
i cmp-address	
snmp-address	
tel net-address	
last-modified-date	2006-06-13 16:41:09
network-i nterface	
name	f01
sub-port-i d	0
hostname	
i p-address	10.10.0.11
pri -uti l i ty-addr	
sec-uti l i ty-addr	
netmask	255.255.0.0
gateway	10.10.0.1
sec-gateway	
gw-heartbeat	
state	di sabl ed
heartbeat	0
retry-count	0
retry-ti meout	1
heal th-score	0
dns-i p-pri mary	
dns-i p-backup1	
dns-i p-backup2	

dns-domain	
dns-timeout	11
hip-ip-list	
ftp-address	
icmp-address	
snmp-address	
telnet-address	
last-modified-date	2006-06-13 16:41:34
network-parameters	
tcp-keepalive-count	100
tcp-keepalive-timer	120
tcp-keepalive-mode	1
last-modified-date	2006-07-12 13:07:21
phys-interface	
name	phyTEST
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	
speed	
last-modified-date	2004-11-17 02:40:21
phys-interface	
name	phyTEST-RIGHT
operation-type	Media
port	0
slot	1
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	
speed	
last-modified-date	2004-11-17 02:44:47
phy-interface	
name	wancom0
operation-type	Control
port	0
slot	0
virtual-mac	
wancom-health-score	50
last-modified-date	2004-12-06 03:27:15
realm	
identifier	testrealm
addr-prefix	0.0.0.0
network-interfaces	
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	disabled
msm-release	disabled
qos-enable	disabled
max-bandwidth	0

ext-policy-svr	boffo.com
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translational	
out-translational	
in-manipulation	
out-manipulation	
class-profile	
average-rate-limit	0
access-control-trust-level	low
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	758
deny-period	30
symmetric-latching	disabled
pair-strip	disabled
trunk-context	
early-media-alow	reverse
additiional-prefixed	10.0.0.0/24
	172.16.0.0
restricted-latching	peer-ip
restriction-mask	17
accounting-enable	enabled
last-modified-date	2006-07-06 12:43:39
realm-config	
identifier	testrealm
addr-prefix	0.0.0.0
network-interfaces	
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	disabled
msm-release	disabled
qos-enable	disabled
max-bandwidth	0
ext-policy-svr	boffo.com
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translational	
out-translational	
in-manipulation	
out-manipulation	
class-profile	
average-rate-limit	0

access-control-trust-level	low
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	758
deny-period	30
symmetric-latching	disabled
pair-strip	disabled
trunk-context	
early-media-allow	reverse
additional-prefixes	10.0.0.0/24
	172.16.0.0
restricted-latching	peer-ip
restriction-mask	17
accounting-enable	enabled
last-modified-date	2006-07-06 12:43:39
realm-config	
identifier	testrealm
addr-prefix	0.0.0.0
network-interfaces	
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	disabled
msm-release	disabled
qos-enable	disabled
max-bandwidth	0
ext-policy-svr	boffo.com
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
class-profile	
average-rate-limit	0
access-control-trust-level	low
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	758
deny-period	30
symmetric-latching	disabled
pair-strip	disabled
trunk-context	
early-media-allow	reverse
additional-prefixes	10.0.0.0/24
	172.16.0.0
restricted-latching	peer-ip
restriction-mask	17
accounting-enable	enabled

last-modified-date	2006-07-06 12:43:39
realm-config	
identifier	testrealm
addr-prefix	0.0.0.0
network-interfaces	
mm-in-realm	disabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	disabled
msm-release	disabled
qos-enable	disabled
max-bandwidth	0
ext-policy-svr	boffo.com
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
class-profile	
average-rate-limit	0
access-control-trust-level	low
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	758
deny-period	30
symmetric-latching	disabled
pair-strip	disabled
trunk-context	
early-media-allow	reverse
additional-prefixes	10.0.0.0/24
172.16.0.0	
restricted-latching	peer-ip
restriction-mask	17
accounting-enable	enabled
last-modified-date	2006-07-06 12:43:39
MediaPolicy	
name	RS
tos-values	
	audio:0x64
last-modified-date	2006-07-12 13:09:55
ClassPolicy	
profile-name	test_profile
to-address	10.44.55.66
media-policy	media_policy_test
last-modified-date	2005-02-15 10:01:14
redundancy-config	
state	enabled
log-level	INFO

```

health-threshold 75
emergency-threshold 50
port 9090
advertisement-time 500
percent-drift 210
initial-time 1250
becoming-standby-time 45000
becoming-active-time 100
cfg-port 1987
cfg-max-trans 10000
cfg-sync-start-time 5000
cfg-sync-comp-time 1000
gateway-heartbeat-interval 0
gateway-heartbeat-retry 0
gateway-heartbeat-timeout 1
gateway-heartbeat-health 0
peer
    name test_peer
    state enabled
    type Unknown
    destination
        address 192.168.0.5:9090
        network-interface phyTEST:0
last-modified-date 2005-02-15 13:41:09
ResponseMap
    last-modified-date 2005-02-15 10:34:03
    name test_map
    entries
        699 -> ()
session-agent
    hostname RS
    ip-address 172.30.1.150
    port 5060
    state enabled
    app-protocol SIP
    app-type
    transport-method UDP
    realm-id tester
    description
    carriers
        carrier1
    allow-next-hop-ip enabled
    constraints disabled
    max-sessions 0
    max-outbound-sessions 0
    max-burst-rate 0
    max-sustain-rate 0
    min-seizures 5
    min-asr 0
    time-to-resume 0
    ttr-no-response 0
    in-service-period 0
    burst-rate-window 0
    sustain-rate-window 0

```

req-uri -carrier-mode	None
proxy-mode	Redi rect
redi rect-acti on	Proxy
l oose-routi ng	enabl ed
send-medi a-sessi on	enabl ed
response-map	tester
pi ng-method	si p
pi ng-i nterval	0
medi a-profi les	testi ng
i n-transl ati on i d	i d
out-transl ati on i d	i d2
trust-me	di sabl ed
request-uri -headers	enabl ed
stop-recurse	
l ocal -response-map	l ocal
pi ng-to-user-part	yes
pi ng-from-user-part	no
l i -trust-me	di sabl ed
i n-mani pul ati on i d	i n
out-mani pul ati on i d	out
p-asserted-i d	
trunk-group	tgname1
max-regi ster-sustai n-rate	0
earl y-medi a-all ow	none
i nval i date-regi strati ons	di sabl ed
rfc2833-mode	none
rfc2833-payl oad	0
l ast-modi fi ed-date	2006-07-07 10: 04: 28
sessi on-agent	
hostname	SA-test2
i p-address	
port	5060
state	enabl ed
app-protocol	SI P
app-type	
transport-method	UDP
real m-i d	
descri pti on	
carri ers	
all ow-next-hop-l p	enabl ed
constrai nts	di sabl ed
max-sessi ons	0
max-outbound-sessi ons	0
max-burst-rate	0
max-sustai n-rate	0
ti me-to-resume	0
ttr-no-response	0
i n-servi ce-peri od	0
burst-rate-wi ndow	0
sustai n-rate-wi ndow	0
req-uri -carrier-mode	None
proxy-mode	
redi rect-acti on	

loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
last-modified-date	2005-02-15 10:23:48
session-group	
group-name	SA-group
description	
state	disabled
app-protocol	SIP
strategy	Hunt
dest	
	dest1
	dest2
last-modified-date	2005-02-15 10:24:38
session-translation	
id	test
rules-calling	rule
rules-called	rule2
last-modified-date	2005-02-15 10:27:41
translation-rules	
id	test_translation_rule
type	none
add-string	
add-index	0
delete-string	
delete-index	0
last-modified-date	2005-02-15 13:36:15
session-router	
state	disabled
system-number-type	Pots
sr-primary-name	
sr-primary-address	
sr-secondary-name	
sr-secondary-address	
pac-name	
pac-password	
divi-resources	disabled
holiday	
date	2005-05-05
description	happy birthday
last-modified-date	2005-02-15 13:19:27
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	
egress-realm-id	
nat-mode	None

registrar-domain	
registrar-host	
registrar-port	0
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1
pac-route-weight	1
pac-call-id-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
last-modified-date	2006-07-06 12:51:11
sip-feature	
name	test_feature
realm	test_realm
support-mode-inbound	Pass
require-mode-inbound	Reject
proxy-require-mode-inbound	Pass
support-mode-outbound	Pass
require-mode-outbound	Reject
proxy-require-mode-outbound	Pass
last-modified-date	2005-02-15 13:38:35
sip-interface	
state	enabled
realm-id	testrealm
sip-port	
address	192.168.10.12
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	register-prefix
carriers	
proxy-mode	
redirect-action	
contact-mode	maddr
nat-traversal	none
nat-interval	30
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled

uri-fqdn-domain	
options	disable-privacy
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401, 407
port-map-start	0
port-map-end	0
in-manipulations	
out-manipulations	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-grp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
last-modified-date	2006-06-12 12:08:34
sip-nat	
realm-id	in_sf
domain-suffix	
ext-proxy-address	
ext-proxy-port	5060
ext-address	
home-address	
home-proxy-address	
home-proxy-port	0
route-home-proxy	disabled
address-prefix	*
tunnel-redirect	disabled
use-url-parameter	none
parameter-name	
user-nat-tag	-acme-
host-nat-tag	ACME-
headers	Call-ID Contact From Join Record-Route Refer-To Replaces Reply-To Route To Via firmrtv
last-modified-date	2005-02-15 10:33:24
snmp-community	
community-name	public
access-mode	READ-ONLY
ip-addresses	

	10.0.1.42
last-modified-date	2004-12-08 20:08:56
static-flow	
in-realm-id	
in-source	0.0.0.0
in-destination	0.0.0.0
out-realm-id	test100
out-source	0.0.0.0
out-destination	0.0.0.0
protocol	UDP
alg-type	none
average-rate-limit	0
last-modified-date	2006-07-07 12:08:20
steering-pool	
ip-address	192.168.200.100
start-port	10000
end-port	60000
realm-id	h323192
network-interface	
last-modified-date	2005-05-25 01:28:52
surrogate-agent	
register-host	
register-user	acme
state	enabled
realm-id	
description	
customer-host	
customer-next-hop	175.3.11.157
register-contact-host	
register-contact-user	
password	
register-expires	600000
replace-contact	disabled
route-to-registrar	enabled
aor-count	1
auth-user	packet
last-modified-date	2006-07-07 12:56:06
tls-profile	
name	test
end-entity-certificate	enabled
trusted-ca-certificates	
	enabled
cipher-list	
	tlsv1
verify-depth	10
mutual-authenticate	disabled
system-config	
hostname	
description	acme
location	burlington
mib-system-contact	
mib-system-name	
mib-system-location	
snmp-enabled	enabled

enable-snmp-auth-traps	disabled
enable-snmp-syslog-notify	disabled
enable-snmp-monitor-traps	disabled
enable-env-monitor-traps	disabled
snmp-syslog-histable-length	1
snmp-syslog-level	WARNING
system-log-level	INFO
process-log-level	NOTICE
process-log-ip-address	0.0.0.0
process-log-port	0
call-trace	disabled
internal-trace	disabled
log-filter	all
default-gateway	0.0.0.0
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control-alarm-threshold	enabled
last-modified-date	2006-07-11 13:30:31
TrapReceiver	
ip-address	10.0.1.42:162
filter-level	All
community-name	public
last-modified-date	2004-12-08 20:09:23
lawful-intercept:	
state	enabled
type	ALIP
log-level	INFO
realm	test-realm
alip-agent-address	0.0.0.0:0
alip-keepalive-timer	30
alip-intercept-timeout	30
df-ccc-network-interface	192.168.0.10:2020
df-ccc-src-port	0
alip-transport-protocol	TCP
alip-tls-profile	profilename

Software License Inventory

This section explains how to view license information for your Net-Net system.

About Licenses

The components of the Net-Net SBC software are licensed by Acme Packet, Inc. for your use. In order to use these components and deploy their related services in your network, you must have a valid license for each of them.

The following software components, interfaces, and features are licensed. If you do not have a license for a given component, interfaces, or feature, its configuration parameters are not visible.

Licence	Description
Session capacity	Determines the maximum number of sessions allowed by a Net-Net system for all protocols combined: SIP, MGCP, H.323, and SIP<-->H.323 IWF (interworking). Each flow that doubles back (or hairpins) through the Net-Net SBC counts as two flows. Options for session capacity are: 250, 500, 1000, 2000, 4000, 8000, 16000, and 32000. When your Net-Net system reaches a 100% of its capacity, an alarm is generated and a trap sent.
SIP	Enables SIP signaling.
H.323	Enables H.323 signaling.
SIP<-->H.323	Enables SIP<-->H.323 IWF signaling. In order to run IWF between these two protocols, you must also have valid SIP and H.323 licenses.
MGCP	Enables MGCP signaling.
QoS	Enables measurement for QoS (jitter, packet latency, and packet loss) on the Net-Net SBC.
ACP	Enables the Net-Net SBC to respond to ACP requests. Required for Net-Net EMS use.
Routing policies	Establishes routing policies on the Net-Net SBC.
Load balancing	Establishes distribution of traffic across gateways, application servers, softswitches, and so on.
Accounting	Establishes RADIUS servers to which the Net-Net SBC can make connections and send CDRs.
HA	Enables two Net-Net SBCs to work as a pair so that, in case of failover, one system can take over for the other. The two systems paired as HA nodes checkpoint configuration, signaling state, and media. Ensure that the same licensed capabilities are enabled on both SDs that act as HA peers.
PAC	Enables the Net-Net system to operate in a PAC configuration with other Net-Net systems.

Unlicensed Signaling Protocols

If any of the signaling protocols are not licensed, the Net-Net system behaves as if it was not configured for those protocols. When this happens, the system writes an error message to the corresponding process log file.

If you exceed the session capacity license, the Net-Net system responds to signaling messages as if any other constraint has been exceeded. For example, for a SIP signaling message, the system responds with a 503 Service Unavailable, as if a SIP `Session Agent Max. Sessions` constraint has been exceeded.

If you do not have a license for the ACP feature, only LOGIN and license-related GET, SAVE, and DELETE requests will be accepted on the Net-Net system's system manager port. Any other requests to the system manager or LEM ports are rejected with a 603 Decline response.

Viewing License Information

You can view a list of the features that are currently enabled on your system, which indicates their licenses are installed. You can also view detailed license information. The available license commands are the following:

- **show features** command at the main CLI user prompt
- **show** command from the license menu (if you have Superuser privileges)

show features

Display features that are currently enabled because the licenses for those features are installed on the system by using the **show features** command. For example:

```
ACMEPACKET# show features
Total session capacity: 32000
Enabled features: SIP, MGCP, H323, IWF, QOS, ACP, Routing,
                  Load Balancing, Accounting, High Availability, PAC
```

license show

Display the list of features that are available by using the **show** command for the license. The **show** command displays the features that are available and, if applicable, the start or end time of the license's activation.

To access the show command on the license menu:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter>.

```
ACMEPACKET(configure)# system
```

3. Type **license** and press <Enter>.

```
ACMEPACKET(system)# license
ACMEPACKET(license)#
```

4. Type **show** and press <Enter>.

For example:

```
acmepacket(license)# show
License #1: 2000 sessions, SIP, MGCP, ACP
no expiration
installed at 12:34:42 SEP 01 2004
License #2: H323
expired at 23:59:59 SEP 08 2004
installed at 12:35:43 SEP 01 2004
License #3: 250 sessions, IWF
expires at 23:59:59 SEP 29 2004
installed at 12:36:44 SEP 01 2004
License #4: QOS
starts at 00:00:00 SEP 29 2004
expires at 23:59:59 OCT 27 2004
installed at 12:37:45 SEP 01 2004
Total session capacity: 2250
host(license)#
```

The next example shows installed licenses that have no expiration date:

```
ACMEPACKET(system)# license
```

```
ACMEPACKET(license)# show
```

```
License #1: 32000 sessions, SIP, MGCP, H323, IWF, QOS, ACP,
```

Routing, Load Balancing, Accounting, High Availability, PAC
no expiration

installed at 11:48:05 MAR 04 2005

Total session capacity: 32000

show sessions

Display session capacity for your license and session use information by using the **show sessions** command. For example:

ACMEPACKET# **show features**

Total session capacity: 32000

Enabled features: SIP, MGCP, H323, IWF, QOS, ACP, Routing,
Load Balancing, Accounting, High Availability, PAC, LI

ACMEPACKET# **show sessions**

15:13:33-165517 Capacity=32000

Session Statistics	Active	High	Total	Total	PerMax	High
Total Sessions	0	0	0	0	0	0
SIP Sessions	0	0	0	0	0	0
H.323 Calls	0	0	0	0	0	0
MGCP Connections	0	0	0	0	0	0

IWF Statistics	Active	High	Total	Total	PerMax	High
H.323-to-SIP Calls	0	0	0	0	0	0
SIP-to-H.323 Calls	0	0	0	0	0	0

ACMEPACKET#

Introduction

This chapter describes how to upgrade the Net-Net 4250 SBC software image.

- For standalone Net-Net SBCs, upgrading the Net-Net SBC image requires a reboot, which stops all processing on the Net-Net SBC.
- For HA nodes, upgrading your Net-Net SBC image also requires a reboot. Remember that the Net-Net SBCs in the HA node cannot switch over while one Net-Net SBC is rebooting.

For these reasons, we recommend that you perform upgrade procedures and system reboots on standalone Net-Net SBCs and on HA nodes during appropriate times such as:

- Regularly scheduled maintenance
- Off-peak hours
- Periods of low traffic volume

Preparing for Upgrade

This section provides information about how to prepare for upgrading your software image.

Transferring Files

For upgrades and other tasks, you need to move files on and off of the Net-Net SBC. You can use FTP or SFTP programs for this. FTP (File Transfer Protocol) is an insecure method of moving files across a network. It should only be used if your network is totally trusted. SFTP (secure FTP) is a secure method of moving files across a network. It should be used if your network is considered insecure. Passwords and files are encrypted when using SFTP.

FTP and SFTP both use the client-server model. You can use an FTP or SFTP client on a remote host to send and retrieve files from the Net-Net SBC, acting as the FTP server. Make sure the FTP service is enabled on your Net-Net SBC before you connect with an FTP client.

Uploading SBC Software Image

To configure your Net-Net SBC to boot from a local system image, you must copy the image file to the local file system. The Net-Net SBC looks in the /boot directory for a boot image.

Obtain the name and location of the software image file you want to use. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.

To copy a system image to the Net-Net SBC's local file system:

1. Use an FTP client to connect to the Net-Net SBC using the default username: **user** and password: **acme**. The IPv4 address of the Net-Net SBC is configured in the bootparams. You can also SFTP into the Net-Net SBC.
2. Change directory to where you want to upload a file.
 - `cd /boot` for system images
3. Type **bin** <enter> to force the FTP program into binary mode. This step is not applicable if you are using SFTP.
4. Upload the file you wish to transfer by typing **put filename** <enter>.

```
C:\Documents and Settings>ftp 172.30.55.127
Connected to 172.30.55.127.
220 VxWorks (1.0) FTP server ready
User (172.30.55.127: (none)): user
331 Password required
Password:
230 User logged in
ftp> cd /boot
250 Changed directory to "/boot"
ftp> bin
200 Type set to I, binary mode
ftp> put SBC201b35.gz
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 9587350 bytes sent in 51.64Seconds 185.65Kbytes/sec.
ftp>
```

Downloading Running Configuration

The Net-Net SBC can be configured to download its system image at boot time from a remote FTP server. Downloading a Net-Net SBC software image at boot time is configured in the bootparam element.

System Configuration Files Release Compatibility

In most instances, upgrading to a higher version of the Net-Net SBC software updates lower-versioned configuration files to the current revision level. Within the S-C6.x release family, any software release can read any configuration file version. When downgrading software within the S-C6.x release family, configured parameters used in unsupported features are ignored. Because upconversions are potentially destructive, you should always create backups that are known to work with every version of the Net-Net SBC software you have deployed.

Note that once you save a C5.x or earlier configuration file with an S-C6.x release family software image, the configuration file is no longer backward compatible with a C5.x or earlier software version.

Upgrade Paths and Release 2.2

It is only possible to upgrade from Release 2.2 to Release 4.1. You cannot upgrade from Release 2.2 to Release 4.0. Therefore, this chapter depicts no upgrade or backout scenarios between Releases 2.2 and 4.0.

If you are upgrading from Release 2.2 to Release 4.1 and you use the enhancement for SIP port mapping that requires you set the `via-reg-key` option as part of the SIP interface configuration, you might encounter difficulty upgrading to certain patches of Release 2.2 or in general to Release 4.1. This issue resolves itself after the

switchover between Net-Net SBCs in the HA node and after endpoints refresh registration.

ACLI Upgrade Preparation Command

The most common problems that arise during Net-Net 4000 upgrade are caused by a user mistyping information during the upgrade procedure. The ACLI upgrade preparation (**load-image**) command guides users through the upgrade process, thereby keeping errors to a minimum.

In addition, you do not have to keep track of the following information when you use the ACLI **load-image** command: boot flash file system name, size of the boot flash, and need to update boot parameters (i.e., knowing the image filename must start with /tffs0 for the Net-Net 4250 or with /boot for the Net-Net 4500). You also do not have to be concerned with accidentally deleting a boot image.

The ACLI **load-image** command tells you whether or not the new image loads successfully. And if the new image fails to load successfully, the Net-Net SBC informs you what caused the failure.

The ACLI **load-image** command organizes the upgrade process in these ways:

- From a list of choices, you select an image to delete so you can make room for the new one if necessary. If the space remaining in boot flash is less than 50%, the Net-Net SBC prompts you to delete an old image to make room but does not allow you to delete the boot image currently in use.
- You specify the name, location, and credentials to use when downloading the new image.
- The command ensures there is enough space available in flash memory for the new image.
- Using FTP, the Net-Net SBC downloads the image file for you.
- The command prompts you to adjust boot parameters as required.
- At the end of the procedure, the Net-Net SBC recommends the next step to take in the upgrade process.

ACLI Instructions and Examples

The following section provides an example of the ACLI **load-image** command where there is insufficient space.

The ACLI **load-image** command asks for three pieces of information before prompting you for your password. You can either enter these all in one line (with a <Space> between each), or you can press <Enter> after each entry to move to the next piece of information require to load the new image. The information you enter is:

- The IP address of the remote host
- The remote filename with path
- Username for the remote host

After you enter your username, the system prompts you for your password. Note that when you enter your password at the prompt, your entry does not echo.

Loading a New Image

To load a new image using the ACLI preparation command:

1. In Superuser mode, type `load-image` and press <Enter>. The next line that appears starts the process of entering the information required for loading the image.

ACMEPACKET# **load-image**

Enter remote host:

2. Enter the IP address of the remote host.

Enter remote host: **192.30.8.50**

Enter remote filename (with path):

3. Enter the remote filename with path from the root of the FTP server.

Enter remote filename (with path): **/image/nnC511p4.gz**

User name (192.30.8.50):

4. Enter your username for the remote host.

User name (192.30.8.50): **user**

Password:

5. Enter the password for the remote host. Your entry will not echo on the screen.

Password: **[Password]**

The image loading process starts. If it is successful, the Net-Net SBC displays the following message:

Successfully transferred image to /boot

6. Next, the Net-Net SBC confirms you want to change the boot parameters. Type a **y** and press <Enter> to make the change, or type an **n** and press <Enter> to reject the change.

WARNING: This will change the image filename from <old image> to <new image>. This will become the running image after a reboot.

Change bootparam filename [y/n]?: **y**

When There is Insufficient Space for a New Image

If you try to load a new image and the Net-Net SBC does not have enough space, it first advises you of the insufficient space and then prompts you to delete an old image. You might have to delete more than one image to make enough room for your new image, so the Net-Net SBC continues to prompt you for deletions until you have enough room.

To make space for a new image by deleting an old one:

1. As you move through the process of loading a new image, you might encounter an error message and prompt. These messages note the insufficiency of space and prompt you to delete old images.

WARNING: Boot flash has insufficient space. Delete an old image. [y/n]? **y**

2. By typing a **y** and pressing <Enter>, you inform the system you want to delete images. It then offers you a list of images you can delete, each referenced by a number. Choose the number corresponding to the image you want to delete and press <Enter>.

1: sd414p26.gz

2: nnC511p3.gz

selection: **1**

The command will loop again if there is insufficient space. And if you do not make a selection, the command exits.

S-C6.1.0 to S-C6.2.0 Upgrade

As you are upgrading your Net-Net SBC software image from Release S-C6.1.0 to Release S-C6.2.0, you should be aware of the following:

- Refer to the “Data Storage Security” section of this guide’s *System Management* chapter for important information about working with systems for which password secure mode is enabled.
- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations within the S-C6.x family are compatible; this means, for example, that you can run a Release S-C6.2.0 configuration with a Release S-C6.1.0 or C6.0 software image as long as you have not enabled password secure mode.

If you choose to revert to Release S-C6.1.0 after having upgraded to Release S-C6.2.0, then the new Release S-C6.2.0 parameters are inherited by the Release S-C6.1.0 configuration. The Release S-C6.1.0 software cannot apply these settings, and so they are silently ignored.

- You do not need to change any of your licensing information. Licenses are automatically transferred from Release S-C6.1.0 to Release S-C6.2.0.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release S-C6.2.0 software:

1. Obtain the name and location of the Release S-C6.2.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release S-C6.1.0 configuration using the ACLI **verify-config** command.
3. Back up a working Release S-C6.1.0 version configuration. Name the file descriptively for easily falling back to this configuration if needed.
4. Verify that your Net-Net 4250 has been upgraded to the bootloader dated Jul 2 2009 or later.

Stand-alone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release S-C6.1.0 to Release S-C6.2.0. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC’s local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release S-C6.1.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

NETNETSBC# **check-space-remaining boot**

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release S-C6.2.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release S-C6.2.0 file name next to the Release S-C6.1.0 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /tffs0/nnC500xxx.gz and /tffs0/nnSC610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number  : 0
host name        : boothost
file name        : /tffs0/nnC600xxx.gz /tffs0/nnSC620.xz
```

Note that /tffs0/ directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/nnSC620.xz.gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release S-C6.2.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, have 100% health, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release S-C6.2.0 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(342\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.

7. Change the bootparams on Net-Net SBC2 to boot from the new Release S-C6.2.0 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release S-C6.1.0 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release S-C6.1.0 to Release S-C6.2.0 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.
You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.
 - 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
 - 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.


```
NETNETSBC1# di spl ay-current-cfg-versi on
Current confi gurati on versi on i s 5
NETNETSBC1#

NETNETSBC2# di spl ay-current-cfg-versi on
Current confi gurati on versi on i s 5
NETNETSBC2#
```
 - 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.


```
NETNETSBC1# di spl ay-runni ng-cfg-versi on
Runni ng confi gurati on versi on i s 5
NETNETSBC1#

NETNETSBC2# di spl ay-runni ng-cfg-versi on
Runni ng confi gurati on versi on i s 5
NETNETSBC2#
```
2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.


```
NETNETSBC1# check-space-remai ni ng boot

boot: 29759488/29760512 bytes (99%) remai ni ng
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the di ags. gz file and the currently running release on the flash memory (in the event that a rollback is required).
3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.

4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release S-C6.2.0 software image.

- 4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to bring displaying the list of boot parameters.

- 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnSC610xxx.gz and /tffs0/nnSC620.xz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnSC610xxx.gz /tffs0/nnSC620.xz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release S-C6.2.0 file name next to the Release S-C6.1.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4250 Firmware SC6. 2. 0
10/02/08
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release S-C6.1.0 for any reason, use [HA Backout Procedure 1 \(341\)](#) in this chapter's [HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 \(341\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release S-C6.1.0 for any reason, use [HA Backout Procedure 2 \(342\)](#) in this chapter's [HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 \(341\)](#) section.

C6.0 to S-C6.1.0 Upgrade

As you are upgrading your Net-Net SBC software image from Release C6.0 to Release S-C6.1.0, you should be aware of the following:

- Refer to the “Data Storage Security” section of this guide’s *System Management* chapter for important information about working with systems for which password secure mode is enabled.
- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations for Release C6.0 and Release S-C6.1.0 are compatible; this means, for example, that you can run a Release S-C6.1.0 configuration with a Release C6.0 software image as long as you have not enabled password secure mode.

If you choose to revert to Release C6.0 after having upgraded to Release S-C6.1.0, then the new Release S-C6.1.0 parameters are inherited by the Release C6.0 configuration. The Release C6.0 software cannot apply these settings, and so they are silently ignored.

- You do not need to change any of your licensing information. Licenses are automatically transferred from Release C6.0 to Release S-C6.1.0.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release S-C6.1.0 software:

1. Obtain the name and location of the Release S-C6.1.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release C6.0 configuration using the ACLI **verify-config** command.
3. Back up a working Release C6.0 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Stand-alone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release C6.0 to Release S-C6.1.0. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC’s local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release S-C6.1.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

NETNETSBC# **check-space-remaini ng boot**

boot: 29759488/29760512 bytes (99%) remaini ng
NETNETSBC#

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release S-C6.1.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release S-C6.1.0 file name next to the Release C6.0 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /tffs0/nnC500xxx.gz and /tffs0/nnSC610xxx.gz, where xxx represents the individual software numbers for these releases.

NETNETSBC1# **confi gure termi nal**
NETNETSBC1(confi gure)# **bootparam**

'.' = clear field; '-' = go to previ ous field; ^D = qui t

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC600xxx.gz /tffs0/nnSC610xxx.gz
```

Note that /tffs0/ directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/nnSC610xxx.gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release S-C6.1.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, have 100% health, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release S-C6.1.0 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(345\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.

7. Change the bootparams on Net-Net SBC2 to boot from the new Release S-C6.1.0 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release S-C6.1.0 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release C6.0 to Release S-C6.1.0 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.
You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di splay-current-cfg-versi on
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# di splay-current-cfg-versi on
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di splay-runni ng-cfg-versi on
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# di splay-runni ng-cfg-versi on
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remai ni ng boot
```

```
boot: 29759488/29760512 bytes (99%) remaini ng
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the di ags. gz file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.

4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release S-C6.1.0 software image.

- 4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC600xxx.gz and /tffs0/nnSC610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

'.' = clear field; '-' = go to previous field; ^D = quit

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC600xxx.gz /tffs0/nnSC610xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release S-C6.1.0 file name next to the Release C6.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4250 Firmware SC6.1.0
10/02/08
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release C6.0 for any reason, use [HA Backout Procedure 1 \(344\)](#) in this chapter's [HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 \(341\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release C6.0 for any reason, use [HA Backout Procedure 2 \(347\)](#) in this chapter's [HA Backout Procedures: Release C5.1 to Release C5.0 \(346\)](#) section.

C5.1 to C6.0 Upgrade

As you are upgrading your Net-Net SBC software image from Release C5.1 to Release C6.0, you should be aware of the following:

- Refer to the “Data Storage Security” section of this guide’s *System Management* chapter for important information about working with systems for which password secure mode is enabled.
- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations for Release C5.1 and Release C6.0 are compatible; this means, for example, that you can run a Release C6.0 configuration with a Release C5.1 software image as long as you have not enabled password secure mode.

If you choose to revert to Release C5.1 after having upgraded to Release C6.0, then the new Release C6.0 parameters are inherited by the Release C5.1 configuration. The Release C5.1 software cannot apply these settings, and so they are silently ignored.

- You do not need to change any of your licensing information. Licenses are automatically transferred from Release C5.1 to Release C6.0.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release C5.1 software:

1. Obtain the name and location of the Release C6.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release C5.1 configuration using the ACLI **verify-config** command.
3. Back up a working Release C5.1 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Stand-alone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release C5.1 to Release C6.0. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC’s local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release C6.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

NETNETSBC# **check-space-remaining boot**

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release C6.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release C6.0 file name next to the Release C5.1 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /tffs0/nnC500xxx.gz and /tffs0/nnC510xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC510xxx.gz /tffs0/nnC600xxx.gz
```

Note that /tffs0/ directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/sd410xxx.gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release C6.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, have 100% health, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release C6.0 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(347\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release C6.0 software image.

8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release C6.0 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release C5.1 to Release C6.0 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.
You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.sgz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release C6.0 software image.

4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC510xxx.gz and /tffs0/nnC600xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC510xxx.gz /tffs0/nnC600xxx.gz
```

4c. As shown in Step 4b directly above, type the appropriate Release C6.0 file name next to the Release C5.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4250 Firmware C6.0.0
10/02/07
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release C5.1 for any reason, use [HA Backout Procedure 1 \(346\)](#) in this chapter's [HA Backout Procedures: Release C5.1 to Release C5.0 \(346\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release C5.1 for any reason, use [HA Backout Procedure 2 \(347\)](#) in this chapter's [HA Backout Procedures: Release C5.1 to Release C5.0 \(346\)](#) section.

C5.0 to C5.1 Upgrade

As you are upgrading your Net-Net SBC software image from Release C5.0 to Release C5.1, you should be aware of the following:

- Refer to the “Data Storage Security” section of this guide’s *System Management* chapter for important information about working with systems for which password secure mode is enabled.
- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations for Release C5.0 and Release C5.1 are compatible; this means, for example, that you can run a Release C5.1 configuration with a Release C5.0 software image as long as you have not enabled password secure mode.

If you choose to revert to Release C5.0 after having upgraded to Release C5.1, then the new Release C5.1 parameters are inherited by the Release C5.0 configuration. The Release C5.0 software cannot apply these settings, and so they are silently ignored.

- You do not need to change any of your licensing information. Licenses are automatically transferred from Release C5.0 to Release C5.1.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release C5.1 software:

1. Obtain the name and location of the Release C5.1 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release C5.0 configuration using the ACLI **verify-config** command.
3. Back up a working Release C5.0 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Stand-alone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release C5.0 to Release C5.1. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC’s local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release C5.1 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the `/boot` directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release C5.1 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release C5.1 file name next to the Release C5.0 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/nnC500xxx.gz` and `/tffs0/nnC510xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC500xxx.gz /tffs0/nnC510xxx.gz
```

Note that `/tffs0/` directs the Net-Net SBC to look in the `/boot` directory for the image you specify. The above example looks for the `/boot/sd410xxx.gz` boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release C5.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, have 100% health, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release C5.1 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(347\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release C5.1 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release C5.1 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release C5.0 to Release C5.1 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.
You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di spl ay-runni ng-cfg-versi on
Runni ng configuration versi on is 5
NETNETSBC1#
```

```
NETNETSBC2# di spl ay-runni ng-cfg-versi on
Runni ng configuration versi on is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remai ni ng boot
```

```
boot: 29759488/29760512 bytes (99%) remai ni ng
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `di ags. gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release C5.1 software image.
 - 4a. Access the boot parameters on Net-Net SBC1:
 - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC500xxx.gz and /tffs0/nnC510xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

'.' = clear field; '-' = go to previous field; ^D = quit

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC500xxx.gz /tffs0/nnC510xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release C5.1 file name next to the Release C5.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4250 Firmware C5.1.0
10/02/07
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release C5.0 for any reason, use [HA Backout Procedure 1 \(346\)](#) in this chapter's [HA Backout Procedures: Release C5.1 to Release C5.0 \(346\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release C5.0 for any reason, use [HA Backout Procedure 2 \(347\)](#) in this chapter's [HA Backout Procedures: Release C5.1 to Release C5.0 \(346\)](#) section.

4.1 to C5.0 Upgrade

As you are upgrading your Net-Net SBC software image from Release 4.1 to Release C5.0, you should be aware of the following:

- You should not enable password secure mode on any Net-Net SBC running Release C5.0 until you are certain you do not want to fall back to a prior release. For more information, see the “Data Storage Security” section of this guide’s *System Management* chapter. By default, this feature is disabled.
- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations for Release 4.1 and Release C5.0 are compatible; this means, for example, that you can run a Release C5.0 configuration with a Release 4.1 software image as long as you have not enabled password secure mode.

If you choose to revert to Release 4.1 after having upgraded to Release C5.0, then the new Release C5.0 parameters are inherited by the Release 4.1 configuration. The Release 4.1 software cannot apply these settings, and so they are silently ignored.

- You do not need to change any of your licensing information. Licenses are automatically transferred from Release 4.1 to Release C5.0.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release C5.0 software:

1. Obtain the name and location of the Release C5.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release 4.1 configuration using the ACLI **verify-config** command.
3. Back up a working Release 4.1 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Standalone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release 4.1 to Release C5.0. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC’s local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release C5.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release C5.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release C5.0 file name next to the Release 4.1 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/sd410xxx.gz` and `/tffs0/nnC500xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/sd410xxx.gz /tffs0/nnC500xxx.gz
```

Note that `/tffs0/` directs the Net-Net SBC to look in the `/boot` directory for the image you specify. The above example looks for the `/boot/sd410xxx.gz` boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release C5.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, healthy, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release C5.0 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(355\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release C5.0 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release C5.0 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release 4.1 to Release C5.0 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized. You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized. Some processes might indicated they are disabled if not licensed.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# di spl ay-runni ng-cfg-versi on
Runni ng configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# di spl ay-runni ng-cfg-versi on
Runni ng configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaini ng boot
```

```
boot: 29759488/29760512 bytes (99%) remaini ng
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.sgz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release C5.0 software image.
 - 4a. Access the boot parameters on Net-Net SBC1:
 - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
 - 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/sd410xxx.gz and /tffs0/nnC500xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number  : 0
host name        : boothost
file name        : /tffs0/sd410xxx.gz /tffs0/nnC500xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release C5.0 file name next to the Release 4.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4250 Firmware C5.0.0
06/30/07
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release 4.1 for any reason, use [HA Backout Procedure 1 \(354\)](#) in this chapter's [HA Backout Procedures: Release C5.0 to Release 4.1 \(349\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release 4.1 for any reason, use [HA Backout Procedure 2 \(355\)](#) in this chapter's [HA Backout Procedures: Release C5.0 to Release 4.1 \(349\)](#) section.

4.0 to 4.1 Upgrade

As you are upgrading your Net-Net SBC software image from Release 4.0 to Release 4.1, you should be aware of the following:

- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance

- Off-peak hours
- Periods of low traffic volume
- Configurations for Release 4.0 and Release 4.1 are compatible; this means, for example, that you can run a Release 4.1 configuration with a Release 4.0 software image.

If you choose to revert to Release 4.0 after having upgraded to Release 4.1, then the new Release 4.1 parameters are inherited by the Release 4.0 configuration. The Release 4.0 software cannot apply these settings, and so they are silently ignored.

- If you are currently running Release 4.1, you do not need to change any of your licensing information. Licenses are automatically transferred from Release 4.0 to Release 4.1.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system. This differs from the process of upgrading to Release 2.0, for which there are special considerations.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release 4.1 software:

1. Obtain the name and location of the Release 4.1 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your Release 4.0 configuration using the ACLI **verify-config** command.
3. Back up a working Release 4.0 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Standalone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release 4.0 to Release 4.1. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release 4.1 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release 4.1 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release 4.1 file name next to the Release 4.0 file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/SBC400xxx.gz` and `/tffs0/SBC410xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/SBC400xxx.gz /tffs0/SBC410xxx.gz
```

Note that `/tffs0/` directs the Net-Net SBC to look in the `/boot` directory for the image you specify. The above example looks for the `/boot/SBC410xxx.gz` boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release 4.1.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, healthy, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release 4.1 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(352\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release 4.1 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release 4.1 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release 4.0 to Release 4.1 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.

You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release 4.1 software image.
 - 4a. Access the boot parameters on Net-Net SBC1:
 - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
 - 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC400xxx.gz` and `/tffs0/SBC410xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/SBC400xxx.gz /tffs0/SBC410xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release 4.1 file name next to the Release 4.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Firmware 4.1.0
08/02/06
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release 4.0 for any reason, use [HA Backout Procedure 1 \(351\)](#) in this chapter's [HA Backout Procedures: Release C5.0 to Release 4.1 \(349\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI **show health** command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release 4.0 for any reason, use [HA Backout Procedure 2 \(352\)](#) in this chapter's [HA Backout Procedures: Release C5.0 to Release 4.1 \(349\)](#) section.

2.x to 4.0 Upgrade

As you are upgrading your Net-Net SBC software image from Release 2.x to Release 4.0, you should be aware of the following:

- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume

- Configurations for Release 2.x and Release 4.0 are compatible; this means, for example, that you can run a Release 4.0 configuration with a Release 2.x software image.

If you choose to revert to Release 2.x after having upgraded to Release 4.0, then the new Release 4.0 parameters are inherited by the Release 2.x configuration. The Release 2.x software cannot apply these settings, and so they are silently ignored.

- If you are currently running Release 2.x, you do not need to change any of your licensing information. Licenses are automatically transferred from Release 2.x to Release 4.0. However, you need to add licenses if you are using new Release 4.0 features that require licenses (such as RACF).

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system. This differs from the process of upgrading to Release 2.0, for which there are special considerations.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release 4.0 software:

- Obtain the name and location of the Release 4.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
- Verify the integrity of your Release 2.x configuration using the ACLI **verify-config** command.
- Back up a working Release 2.x version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Standalone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release 2.x to Release 4.0. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

- On the Net-Net SBC, check for adequate space in the `/boot` directory to upload the new Release 4.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
ACMEPACKET# check-space-remaini ng boot
```

```
boot: 29759488/29760512 bytes (99%) remaini ng
ACMEPACKET#
```

- Upload the Net-Net SBC software image file to the `/boot` directory using an FTP or SFTP client.
- Change the boot configuration parameters to use the new Release 4.0 image. Scroll through the boot parameters by pressing `<Enter>`. Stop when you reach the **file name** boot parameter and type the appropriate Release 4.0 file name next to the release 2.x file name. Press `<Enter>` to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/SBC210xxx.gz` and `/tffs0/SBC400xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number  : 0
host name        : boothost
file name        : /tffs0/SBC210xxx.gz /tffs0/SBC400xxx.gz
```

Note that `/tffs0/` directs the Net-Net SBC to look in the `/boot` directory for the image you specify. The above example looks for the `/boot/SBC400xxx.gz` boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release 4.0.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, healthy, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release 4.0 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(355\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release 4.0 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release 4.0 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release 2.x to Release 4.0 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.

You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release 4.0 software image.
 - 4a. Access the boot parameters on Net-Net SBC1:
 - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
 - 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC210xxx.gz` and `/tffs0/SBC400xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name        : boothost
file name        : /tffs0/SBC210xxx.gz /tffs0/SBC400xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release 4.0 file name next to the Release 2.x file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Firmware 4.0.0
01/31/06
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release 2.0 for any reason, use [HA Backout Procedure 1 \(354\)](#) in this chapter's [HA Backout Procedures: Release 4.0 to Release 2.0/2.1 \(354\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI **show health** command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

Note: At this point, if you need to revert to Release 2.x for any reason, use [HA Backout Procedure 2 \(355\)](#) in this chapter's [HA Backout Procedures: Release 4.0 to Release 2.0/2.1 \(354\)](#) section.

2.0/2.1 to 2.2 Upgrade

As you are upgrading your Net-Net SBC software image from Release 2.0/2.1 to Release 2.2, you should be aware of the following:

- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume

- Configurations for Release 2.0/2.1 and Release 2.2 are compatible; this means, for example, that you can run a Release 2.2 configuration with a Release 2.0/2.1 software image.

If you choose to revert to Release 2.0/2.1 after having upgraded to Release 2.2, then the new Release 2.2 parameters are inherited by the Release 2.0/2.1 configuration. The Release 2.0/2.1 software cannot apply these settings, and so they are silently ignored.

- If you are currently running Release 2.2, you do not need to change any of your licensing information. Licenses are automatically transferred from Release 2.0/2.1 to Release 2.2.

In the HA node descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system. This differs from the process of upgrading to Release 2.0, for which there are special considerations.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release 2.2 software:

- Obtain the name and location of the Release 2.2 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
- Verify the integrity of your Release 2.0/2.1 configuration using the CLI **verify-config** command.
- Back up a working Release 2.0/2.1 version configuration. Name the file descriptively for easily falling back to this configuration if needed.

Standalone Upgrade

This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release 2.0/2.1 to Release 2.2. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

- On the Net-Net SBC, check for adequate space in the `/boot` directory to upload the new Release 2.2 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

- Upload the Net-Net SBC software image file to the `/boot` directory using an FTP or SFTP client.
- Change the boot configuration parameters to use the new Release 2.2 image.

Scroll through the boot parameters by pressing `<Enter>`. Stop when you reach the **file name** boot parameter and type the appropriate Release 2.2 file name next to the release 2.0/2.1 file name. Press `<Enter>` to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/SBC210xxx.gz` and `/tffs0/SBC220xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name        : boothost
file name        : /tffs0/SBC210xxx.gz /tffs0/SBC220xxx.gz
```

Note that `/tffs0/` directs the Net-Net SBC to look in the `/boot` directory for the image you specify. The above example looks for the `/boot/SBC220xxx.gz` boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running Release 2.2.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, healthy, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Release 2.2 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA Backout Procedure 2 \(355\)](#).)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release 2.2 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC2 is running the Release 2.2 software image.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release 2.0/2.1 to Release 2.2 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized. You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.
 - 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.

- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.sgz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release 2.2 software image.

- 4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC210xxx.gz` and `/tffs0/SBC220xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```

boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/SBC210xxx.gz /tffs0/SBC220xxx.gz

```

- 4c. As shown in Step 4b directly above, type the appropriate Release 2.2 file name next to the Release 2.0/2.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```

NETNETSBC1# show version
ACME Firmware 2.2.0
01/31/06
NETNETSBC1#

```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release 2.0/2.1 for any reason, use [HA Backout Procedure 1 \(354\)](#) in this chapter's [HA Backout Procedures: Release 4.0 to Release 2.0/2.1 \(354\)](#) section.

8. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# notify berpd force
```

9. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI show health command.

```
NETNETSBC2# show health
```

10. Carry out Steps 2 through 6 on Net-Net SBC2 to change the software image version.

At this point, if you need to revert to Release 2.0/2.1 for any reason, use [HA Backout Procedure 2 \(355\)](#) in this chapter's [HA Backout Procedures: Release C5.0 to Release 4.1 \(349\)](#) section.

2.0 to 2.1 Upgrade

As you are upgrading your Net-Net SBC software image from Release 2.0 to Release 2.1, you should be aware of the following:

- You might want to perform upgrade procedures during:
 - Regularly scheduled maintenance
 - Off-peak hours
 - Periods of low traffic volume
- Configurations for Release 2.0 and Release 2.1 are compatible; this means, for example, that you can run a Release 2.1 configuration with a Release 2.0 software image.

If you choose to revert to Release 2.0 after having upgraded to Release 2.1, then the new, Release 2.1 parameters are inherited by the Release 2.0 configuration.

The Release 2.0 software cannot apply these settings, and so they are silently ignored.

- If you are currently running Release 2.0, you do not need to change any of your licensing information. Licenses are automatically transferred from Release 2.0 to Release 2.1.

In the descriptions and processes outlined below, Net-Net SBC1 begins the upgrade process as the standby system and Net-Net SBC2 as the active system. This differs from the process of upgrading to Release 2.0, for which there are special considerations.

Pre-Upgrade Checklist

Before initially loading Net-Net SBC Release 2.1 software:

1. Obtain the name and location of the Release 2.1 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at support@acmepacket.com.
2. Verify the integrity of your release 2.0 configuration using the ACLI **verify-config** command.
3. Back up a working Release 2.0 configuration. Name the file descriptively for easily falling back to this configuration if needed.

Standalone Upgrade

Upgrading a single Net-Net SBC to Release 2.1 is a quick procedure. This process incurs system downtime; your Net-Net SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

Upgrade Procedure

The following procedure describes how to upgrade a Net-Net SBC running Release 2.0 to Release 2.1. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

1. On the Net-Net SBC, check for adequate space in the `/boot` directory to upload the new Net-Net SBC Release 2.1 software boot image. Use the **check-space-remaining boot** command.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the `/boot` directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Net-Net SBC software 2.1 image.

Scroll through the boot parameters by pressing `<Enter>`. Stop when you reach the **file name** boot parameter and type the appropriate release 2.1 file name next to the release 2.0 file name. Press `<Enter>` to continue scrolling through the boot parameters.

The following example uses the filenames `/tffs0/SBC200xxx.gz` and `/tffs0/SBC210xxx.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

'.' = clear field; '-' = go to previous field; ^D = quit

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/SBC200xxx.gz /tffs0/SBC210xxx.gz
```

Note that /tffs0/ directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/SBC210xxx.gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.
5. Reboot the Net-Net SBC.

Note: Do not save or activate your configuration prior to rebooting.

The Net-Net SBC should now be successfully running Net-Net SBC Release 2.1.

HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Upgrading an HA pair is an involved process. Please read the following procedures carefully before beginning the upgrade. You can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

Upgrade Overview

The following overview is presented to increase your familiarity with the procedure before attempting the upgrade.

1. Confirm that the two Net-Net SBCs are synchronized, healthy, and share the same running and current configuration version numbers.
2. Change the bootparams on Net-Net SBC1 to boot from the new Net-Net SBC Release 2.1 software image.
3. Reboot Net-Net SBC1.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see backout procedure 2.)
6. Force Net-Net SBC1 to become the active peer, and verify that it has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Net-Net SBC Release 2.1 software image.
8. Reboot Net-Net SBC2.
9. Confirm that Net-Net SBC1 is running the Net-Net SBC Release 2.1 software image.
10. When the Net-Net SBCs are synchronized, save and activate the configuration.

Upgrade Process

To upgrade your Net-Net SBC's software image from Release 2.0 to Release 2.1 for an HA Node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.

You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples above, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diag.gz` file and the currently certified release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release 2.1 software image.
 - 4a. Access the boot parameters on Net-Net SBC1:
 - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
 - 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC200xxx.gz` and `/tffs0/SBC210xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

'.' = clear field; '-' = go to previous field; ^D = quit

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/SBC200xxx.gz /tffs0/SBC210xxx.gz
```

- 4c. As shown in Step 4b directly above, type the appropriate Release 2.1 file name next to the Release 2.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Firmware 2.1.0
08/22/05
NETNETSBC1#
```

7. Confirm that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the following examples, all of the configuration versions are 6.

- 7a. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 6
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 6
NETNETSBC2#
```

- 7b. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 6
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 6
NETNETSBC2#
```

8. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

Note: At this point, if you need to revert to Release 2.0 for any reason, use [HA Backout Procedure 1 \(359\)](#) in this chapter's [HA Backout Procedures: Release 2.1 to Release 2.0 \(359\)](#) section.

9. Initiate a switchover on Net-Net SBC1.

```
NETNETSBC1# noti fy berpd force
```

10. Wait for Net-Net SBC2 to transition to the standby state. Confirm that it is in the standby state by using the ACLI **show health** command.

```
NETNETSBC2# show heal th
```

11. Carry out Steps 2 through 4 on Net-Net SBC2 to change the software image version.

Note: Do not save or activate your configuration prior to rebooting.

12. Once Net-Net SBC1 and Net-Net SBC2 are synchronized, use the ACLI **save-config** command on Net-Net SBC1 to save the configuration.

```
NETNETSBC1# save-confi g
```

13. After you have saved the configuration on Net-Net SBC1, use the ACLI **activate-config** command to activate the configuration.

```
NETNETSBC1# acti vate-confi g
```

Note: At this point, if you need to revert to Release 2.0 for any reason, use [HA Backout Procedure 2 \(361\)](#) in this chapter's [HA Backout Procedures: Release 2.1 to Release 2.0 \(359\)](#) section.

HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0

Release S-C6.2.0 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release S-C6.1.0, you should be aware of their impact on the process of falling back from Release S-C6.2.0 to Release S-C6.1.0.

If you choose to revert to Release S-C6.1.0 after having upgraded to Release S-C6.2.0, then the new, Release S-C6.2.0 parameters are inherited by the Release S-C6.1.0 configuration. The Release S-C6.1.0 configuration cannot apply these settings, and so they are silently ignored.

HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release S-C6.2.0, but decide that you need to revert to Release S-C6.1.0, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release S-C6.2.0 and Net-Net SBC2 is the active system running Release S-C6.1.0.

To backout from upgrading to Release S-C6.2.0 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show heal th
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release S-C6.1.0 software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC600xxx. gz and /tffs0/nnC610xxx. gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnSC620. xz /tffs0/nnSC610xxx. gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release S-C6.1.0 file name next to the Release S-C6.2.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

3. Reboot Net-Net SBC1.

```
NETNETSBC1# reboot
```

4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.

- 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
- 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

5. Fail back to normal active/standby modes and verify calls.

HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release S-C6.2.0, but decide that you need to revert to Release S-C6.1.0, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

To backout from upgrading to Release S-C6.2.0 with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release S-C6.1.0 software image.

- 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:

- Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnSC610xxx.gz and /tffs0/nnC620xxx.xz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnSC620xxx.gz /tffs0/nnSC610xxx.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release S-C6.1.0 file name next to the Release S-C6.2.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.

```
NETNETSBC2# show version
ACME Net-Net 4250 Firmware C6.1.0
06/30/08
NETNETSBC2#
```

4. Initiate a switchover on Net-Net SBC2.

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release S-C6.1.0. Net-Net SBC1 is now the standby system running Release S-C6.2.0.

5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 2 of this procedure.
7. Reboot Net-Net SBC1.

HA Backout Procedures: Release S-C6.1.0 to Release C6.0

Release S-C6.1.0 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release C6.0, you should be aware of their impact on the process of falling back from Release S-C6.1.0 to Release C6.0.

If you choose to revert to Release C6.0 after having upgraded to Release S-C6.1.0, then the new, Release S-C6.1.0 parameters are inherited by the Release C6.0 configuration. The Release C6.0 configuration cannot apply these settings, and so they are silently ignored.

HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release S-C6.1.0, but decide that you need to revert to Release C6.0, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release C6.0 and Net-Net SBC2 is the active system running Release S-C6.1.0.

To backout from upgrading to Release S-C6.1.0 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show health
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release C6.0 software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC600xxx.gz and /tffs0/nnC610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device      : wancom0
processor number : 0
host name       : boothost
file name       : /tffs0/nnC610xxx.gz /tffs0/nnC600xxx.gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release C6.0 file name next to the Release S-C6.1.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
3. Reboot Net-Net SBC1.
- ```
NETNETSBC1# reboot
```
4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.



- 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
- 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release S-C6.1.0, but decide that you need to revert to Release C6.0, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

### To backout from upgrading to Release S-C6.1.0 with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release C6.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/nnC600xxx.gz and /tffs0/nnC610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/nnC610xxx.gz /tffs0/nnC600xxx.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release C6.0 file name next to the Release S-C6.1.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
- 1d. Exit to the main Superuser prompt.  

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```
2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.  

```
NETNETSBC2# show version
ACME Net-Net 4250 Firmware C6.0.0
06/30/08
NETNETSBC2#
```
4. Initiate a switchover on Net-Net SBC2.  

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release C6.0. Net-Net SBC1 is now the standby system running Release S-C6.1.0.
5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release C5.1 to Release C5.0

---

Release C5.1 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release C5.0, you should be aware of their impact on the process of falling back from Release C5.1 to Release C5.0.

If you choose to revert to Release C5.0 after having upgraded to Release C5.1, then the new, Release C5.1 parameters are inherited by the Release C5.0 configuration. The Release C5.0 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release C5.1, but decide that you need to revert to Release C5.0, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release C5.0 and Net-Net SBC2 is the active system running Release C5.1.

#### To backout from upgrading to Release C5.1 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.  

```
NETNETSBC1# show health
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release C5.0 software image.
  - 2a. Access the boot parameters on Net-Net SBC1:
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
  - 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.
 

The following example uses the filenames /tffs0/nnC500xxx.gz and /tffs0/nnC510xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam

'.' = clear field; '-' = go to previous field; ^D = quit

boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/nnC510xxx.gz /tffs0/nnC510xxx.gz
```
  - 2c. As in the example in Step 2b directly above, type the appropriate Release C5.0 file name next to the Release C5.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
3. Reboot Net-Net SBC1.
 

```
NETNETSBC1# reboot
```
4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.
  - 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
  - 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.
 

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#

NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```
5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release C5.0, but decide that you need to revert to Release C5.0, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

**To backout from upgrading to Release C5.1 with the both Net-Net SBCs in the HA node upgraded:**

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release C5.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.  
  
 The following example uses the filenames /tffs0/nnC500xxx. gz and /tffs0/nnC510xxx. gz, where xxx represents the individual software numbers for these releases.  
  

```

NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam

',.' = clear field; '-' = go to previous field; ^D = quit

boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/nnC510xxx. gz /tffs0/nnC500xxx. gz

```
  - 1c. As in the example in Step 1b directly above, type the appropriate Release C5.0 file name next to the Release C5.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
  - 1d. Exit to the main Superuser prompt.  
  

```

NETNETSBC2(configure)# exit
NETNETSBC2#

```
2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.  
  

```

NETNETSBC2# show version
ACME Net-Net 4250 Firmware C5.0.0
06/30/07
NETNETSBC2#

```
4. Initiate a switchover on Net-Net SBC2.  
  

```

NETNETSBC2# notify berpd force

```

At this point, Net-Net SBC2 becomes the active system running Release c5.0. Net-Net SBC1 is now the standby system running Release C5.1.
5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.

## 7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release C5.0 to Release 4.1

---

Release C5.0 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release 4.1, you should be aware of their impact on the process of falling back from Release C5.0 to Release 4.1.

If you choose to revert to Release 4.1 after having upgraded to Release C5.0, then the new, Release C5.0 parameters are inherited by the Release 4.1 configuration. The Release 4.1 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release C5.0, but decide that you need to revert to Release 4.1, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release 4.1 and Net-Net SBC2 is the active system running Release C5.0.

#### To backout from upgrading to Release 4.1 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show heal th
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release 4.1 software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/sd410xxx. gz and /tffs0/nnC500xxx. gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/nnC500xxx. gz /tffs0/sd410xxx. gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release 4.1 file name next to the Release C5.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
3. Reboot Net-Net SBC1.

NETNETSBC1# **reboot**

4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.
  - 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
  - 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release C5.0, but decide that you need to revert to Release 4.1, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

### To backout from upgrading to Release C5.0 with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release 4.1 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/sd410xxx.gz and /tffs0/nnC500xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
```

file name : /tffs0/nnC500xxx.gz /tffs0/sd410xxx.gz

- 1c. As in the example in Step 1b directly above, type the appropriate Release 4.1 file name next to the Release C5.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.
 

```
NETNETSBC2# show version
ACME Firmware 4.1.0
01/31/06
NETNETSBC2#
```
4. Initiate a switchover on Net-Net SBC2.
 

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release 4.1. Net-Net SBC1 is now the standby system running Release C5.0.
5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release 4.1 to Release 4.0

---

Release 4.1 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release 4.0, you should be aware of their impact on the process of falling back from Release 4.1 to Release 4.0.

If you choose to revert to Release 4.0 after having upgraded to Release 4.1, then the new, Release 4.1 parameters are inherited by the Release 4.0 configuration. The Release 4.0 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release 4.1, but decide that you need to revert to Release 4.0, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release 4.1 and Net-Net SBC2 is the active system running Release 4.0.

#### To backout from upgrading to Release 4.1 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show health
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release 4.0 software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/SBC400xxx.gz and /tffs0/SBC410xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC410xxx.gz /tffs0/SBC400xxx.gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release 4.0 file name next to the Release 4.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

3. Reboot Net-Net SBC1.

```
NETNETSBC1# reboot
```

4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.

- 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.

- 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release 4.1, but decide that you need to revert to Release 4.0, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.



**To backout from upgrading to Release 4.1 with the both Net-Net SBCs in the HA node upgraded:**

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release 4.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.  
  
 The following example uses the filenames /tffs0/SBC400xxx.gz and /tffs0/SBC410xxx.gz, where xxx represents the individual software numbers for these releases.  
  

```

NETNETSBC2# configure terminal
NETNETSBC2(configure)# bootparam

'.' = clear field; '-' = go to previous field; ^D = quit

boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC410xxx.gz /tffs0/SBC400xxx.gz

```
  - 1c. As in the example in Step 1b directly above, type the appropriate Release 4.0 file name next to the Release 4.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
  - 1d. Exit to the main Superuser prompt.  
  

```

NETNETSBC2(configure)# exit
NETNETSBC2#

```
2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.  
  

```

NETNETSBC2# show version
ACME Firmware 4.0.0
01/31/06
NETNETSBC2#

```
4. Initiate a switchover on Net-Net SBC2.  
  

```

NETNETSBC2# notify berpd force

```

At this point, Net-Net SBC2 becomes the active system running Release 4.0. Net-Net SBC1 is now the standby system running Release 4.1.
5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration.
7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release 4.0 to Release 2.0/2.1

---

Release 4.0 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release 2.0/2.1, you should be aware of their impact on the process of falling back from Release 4.0 to Release 2.0/2.1.

If you choose to revert to Release 2.0/2.1 after having upgraded to Release 4.0, then the new, Release 4.0 parameters are inherited by the Release 2.0/2.1 configuration. The Release 2.0/2.1 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release 4.0, but decide that you need to revert to Release 2.0/2.1, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release 4.0 and Net-Net SBC2 is the active system running Release 2.0/2.1.

#### To backout from upgrading to Release 4.0 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show heal th
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release 2.x software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC210xxx.gz` and `/tffs0/SBC400xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
```

```
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
```

```
processor number : 0
```

```
host name : boothost
```

```
file name : /tffs0/SBC400xxx.gz /tffs0/SBC210xxx.gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release 2.x file name next to the Release 4.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
3. Reboot Net-Net SBC1.

NETNETSBC1# **reboot**

4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.
  - 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
  - 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release 4.0, but decide that you need to revert to Release 2.0/2.1, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

### To backout from upgrading to Release 4.0 with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release 2.0/2.1 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/SBC210xxx. gz and /tffs0/SBC400xxx. gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
```

file name : /tffs0/SBC400xxx.gz /tffs0/SBC210xxx.gz

- 1c. As in the example in Step 1b directly above, type the appropriate Release 2.0/2.1 file name next to the Release 4.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(confi gure)# exi t
NETNETSBC2#
```

2. Reboot Net-Net SBC2.

3. Using the ACLI **show version** command to confirm that you are using the appropriate release.

```
NETNETSBC2# show versl on
ACME Firmware 2.1.0
01/31/06
NETNETSBC2#
```

4. Initiate a switchover on Net-Net SBC2.

```
NETNETSBC2# noti fy berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release 2.0/2.1. Net-Net SBC1 is now the standby system running Release 4.0.

5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release 2.2 to Release 2.0/2.1

---

Release 2.2 contains configurations that support new features and functions available in the release. Since these parameters do not appear in Release 2.0/2.1, you should be aware of their impact on the process of falling back from Release 2.2 to Release 2.0/2.1.

If you choose to revert to Release 2.0/2.1 after having upgraded to Release 2.2, then the new, Release 2.2 parameters are inherited by the Release 2.0/2.1 configuration. The Release 2.0/2.1 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release 2.2, but decide that you need to revert to Release 2.0/2.1, use the following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release 2.2 and Net-Net SBC2 is the active system running Release 2.0/2.1.

#### To backout from upgrading to Release 2.2 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show heal th
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release 2.0/2.1 software image.
  - 2a. Access the boot parameters on Net-Net SBC1:
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
  - 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.
 

The following example uses the filenames /tffs0/SBC210xxx.gz and /tffs0/SBC220xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam

'.' = clear field; '-' = go to previous field; ^D = quit

boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC220xxx.gz /tffs0/SBC210xxx.gz
```
  - 2c. As in the example in Step 2b directly above, type the appropriate Release 2.0/2.1 file name next to the Release 2.2 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
3. Reboot Net-Net SBC1.
 

```
NETNETSBC1# reboot
```
4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.
  - 4a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
  - 4b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.
 

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#

NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```
5. Fail back to normal active/standby modes and verify calls.

## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release 2.2, but decide that you need to revert to Release 2.0/2.1, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

**To backout from upgrading to Release 2.2 with the both Net-Net SBCs in the HA node upgraded:**

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release 2.0/2.1 software image.

- 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:

- Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/SBC210xxx.gz and /tffs0/SBC220xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC220xxx.gz /tffs0/SBC210xxx.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release 2.0/2.1 file name next to the Release 2.2 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.

```
NETNETSBC2# show version
ACME Firmware 2.1.0
01/31/06
NETNETSBC2#
```

4. Initiate a switchover on Net-Net SBC2.

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release 2.0/2.1. Net-Net SBC1 is now the standby system running Release 2.2.

5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## HA Backout Procedures: Release 2.1 to Release 2.0

Release 2.1 contains configuration parameters that support the features and functions available in the release. Since these parameters do not appear in Release 2.0, you should be aware of their impact on the process of falling back from Release 2.1 to Release 2.0.

If you choose to revert to Release 2.0 after having upgraded to Release 2.1, then the new, Release 2.1 parameters are inherited by the Release 2.0 configuration. The Release 2.0 configuration cannot apply these settings, and so they are silently ignored.

### HA Backout Procedure 1

If you reach the point in your upgrade procedure where you have upgraded Net-Net SBC1 to Release 2.1, but decide that you need to revert to Release 2.0, use this following procedure.

In Backout Procedure 1, Net-Net SBC1 is that standby system running Release 2.1 and Net-Net SBC2 is the active system running Release 2.0.

#### To backout from upgrading to Release 2.1 with the standby system upgraded:

1. Use the ACLI **show health** command to make sure that Net-Net SBC1 is in the standby mode and Net-Net SBC2 is in active mode.

```
NETNETSBC1# show health
```

2. Change the boot parameters on Net-Net SBC1 to use the appropriate Release 2.0 software image.

- 2a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/tffs0/SBC200xxx.gz` and `/tffs0/SBC210xxx.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC210xxx.gz /tffs0/SBC200xxx.gz
```

- 2c. As in the example in Step 2b directly above, type the appropriate Release 2.0 file name next to the Release 2.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 2d. Exit to the main Superuser prompt.

```
NETNETSBC1(configure)# exit
NETNETSBC1#
```

3. On Net-Net SBC1, delete the configuration using the ACLI **delete-config** command. You are asked to confirm the deletion. To confirm, type **y** and press <Enter>. Then you are informed first that you need to reboot the Net-Net SBC in order for changes to take effect, and then that the task is completed.

```

NETNETSBC1# del ete-confi g

Do you really want to ERASE the current config? [y/n]?: y
Deleting configuration
NOTE: need to reboot for changes to take effect
task done
NETNETSBC1#

```

4. Reboot Net-Net SBC1.
5. When Net-Net SBC1 comes up, it should have no configuration. Verify that it does not have a configuration by using the ACLI **show config** command. Nothing appears except a line informing you that the task is complete.

```

NETNETSBC1# show confi g
task done

```

6. Use the ACLI **show version** command to confirm that you are using the appropriate release.

```

NETNETSBC1# show versi on
ACME Firmware 2.0.0
05/31/05
NETNETSBC1#

```

7. On Net-Net SBC1, acquire the configuration from Net-Net SBC2. Be sure to use the correct wancom IPv4 address for Net-Net SBC2. In the example below, 10.0.0.2 is the IPv4 address of wancom0 on Net-Net SBC2.

```

NETNETSBC1# acqui re-confi g 10.0.0.2
Current config will be replaced by acquired config.
Continue [y/n]?: y
Acquire-Config received, processing.
waiting 120000 for request to finish
Request 'ACQUIRE-CONFIG' has finished, Acquire Complete

```

8. Reboot and activate the configuration on Net-Net SBC1 again.

```

NETNETSBC1# reboot force activate

```

9. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.

- 9a. On both Net-Net SBCs, use the ACLI **show health** command to make sure that all processes are synchronized.
- 9b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```

NETNETSBC1# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC1#

```

```

NETNETSBC2# di spl ay-current-cfg-versi on
Current configuration version is 5
NETNETSBC2#

```

10. Fail back to normal active/standby modes have been restored and verify calls.



## HA Backout Procedure 2

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release 2.1, but decide that you need to revert to Release 2.0, use this procedure.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

**To backout from upgrading to Release 2.1 with the both Net-Net SBCs in the HA node upgraded:**

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release 2.0 software image.

- 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:

- Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.

- 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /tffs0/SBC200xxx. gz and /tffs0/SBC210xxx. gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : wancom0
processor number : 0
host name : boothost
file name : /tffs0/SBC210xxx. gz /tffs0/SBC200xxx. gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release 2.0 file name next to the Release 2.1 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. On Net-Net SBC2, delete the configuration using the ACLI **delete-config** command. You are asked to confirm the deletion. To confirm, type y and press <Enter>. Then you are informed first that you need to reboot the Net-Net SBC in order for change to take effect, and then that the task is completed.

```
NETNETSBC2# delete-config
```

```

```

```
Do you really want to ERASE the current config: ? [y/n]: y
```

```
Deleting configuration
```

```
NOTE: need to reboot for changes to take effect
```

```
task done
```

NETNETSBC2#

3. Reboot Net-Net SBC2.
4. When Net-Net SBC2 comes up, it should have no configuration. Verify that it does not have a configuration by using the ACLI **show config** command. Nothing appears except a line informing you that the task is complete.

NETNETSBC2# **show config**  
task done

5. Using the ACLI **show version** command to confirm that you are using the appropriate release.

NETNETSBC2# **show version**  
ACME Firmware 2.0.0  
05/31/05  
NETNETSBC2#

6. Restore the Release 2.0 configuration that you backed up on Net-Net SBC2. In the following example, the name of the back-up being restored is NetNetSBC2\_022305.tar.gz.

NETNETSBC2# **display-backups**  
BACK\_UP\_CONFIG.tar.gz  
02\_Feb\_2005.tar.gz  
01\_Feb\_2005\_Test.tar.gz  
running\_test\_one  
NetNetSBC2\_022305.tar.gz  
NETNETSBC2# **restore-backup-config NetNetSBC2\_022305.tar.gz**

7. Save the configuration using the ACLI **save-config** command on Net-Net SBC2.

NETNETSBC2# **save-config**

8. On Net-Net SBC2, reboot and activate the configuration in one step by using the ACLI reboot force activate command.

NETNETSBC2# **reboot force activate**

9. Initiate a switchover on Net-Net SBC2.

NETNETSBC2# **notify berpd force**

At this point, Net-Net SBC2 becomes the active system running Release 2.0. Net-Net SBC1 is now the standby system running Release 2.1.

10. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
11. On Net-Net SBC1, delete the configuration as you did in Step 2 of this procedure.
12. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
13. Reboot Net-Net SBC1.

## Introduction

---

This chapter provides information about how to upgrade your Net-Net 4500 software image. Since Release CX6.0.0 is the first software release available on the Net-Net 4500, this chapter shows you how to change different versions of that software image.

This section also shows you how to upgrade your Net-Net 4250 configuration to use on the Net-Net 4500 SBC. Note, however, that using your Net-Net 4250 configuration on the Net-Net 4500 causes the configuration to be converted to the `data.tar.gz` file format. A configuration in this format cannot be moved back to the a Net-Net 4250 unless that system is already upgraded to Release C6.0.0; it would be unusable on any Net-Net 4250 running a release prior to C6.0.0.

## Notes on Boot Parameters

The processes for changing Net-Net 4500 software images are fundamentally the same as they are for the Net-Net 4250. The exception is that some of the boot parameters are different. For the Net-Net 4500, the following boot parameters changed:

- The boot device for the Net-Net 4500 is `eth0`.
- The path that appears as part of the file name is `/boot` (instead of `/tffs0`), and the name of the image itself starts with `nnCX` (rather than just `nnC`).

## Net-Net 3800

The Net-Net 3800 also runs the same software as the Net-Net 4500; it also runs an image called, for example, S-Cx6.2.0.

## Preparing for Upgrade

Preparing for an upgrade is the same as it is in the for the Net-Net 4250, and is described in the [Preparing for Upgrade \(301\)](#) section of this guide's [Net-Net 4500 Upgrading \(363\)](#) chapter.

## Password Secure Mode

Note that all Net-Net 4500 SBCs have password secure mode enabled—meaning that you must accurately track your password information. To learn more about password secure mode, refer to this guide's [Data Storage Security \(242\)](#) section.

## Upgrading S-CX6.2.0 Software Images

---

This document explains how to upgrade S-CX6.2.0 images on your Net-Net 4500 SBC.

## Pre-Upgrade Checklist

**Before initially loading Net-Net SBC Release S-CX6.2.0 software:**

1. Obtain the name and location of the Release S-CX6.1.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at [support@acmepacket.com](mailto:support@acmepacket.com).
2. Verify the integrity of your configuration using the ACLI **verify-config** command.
3. Back up a well-working configuration. Name the file descriptively so you can fall back to this configuration easily.
4. Verify that your Net-Net 4500 has been upgraded to the bootloader dated Aug 11 2009 or later.

## Stand-alone Upgrade

This process incurs system downtime; your Net-Net 4500 SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

### Upgrade Procedure

The following procedure describes how to upgrade a Net-Net 4500 SBC running to a new software image. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

#### To upgrade a software image on a stand-alone system:

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release S-CX6.2.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 8+ MB.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release S-CX6.2.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release CX6.0.0 file name next to the previous file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /boot/nnCX600.gz and /boot/nnSCX610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnSCX610.gz /boot/nnSCX620xxx.xz
```

Note that /boot directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/nnSCX620xxx.xz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running the new release.

## HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

### Upgrade Process

#### To upgrade a software image for an HA node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.

You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diags.gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the `/boot` directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release S-CX6.2.0 software image.

---

**Caution:** From the point that you upgrade the image file, do not make any configuration changes. Likewise, do not use the `save-config` or `activate-config` commands.

---

- 4a. Access the boot parameters on Net-Net SBC1:
  - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
- 4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/boot/nnSCX610.gz` and `/boot/nnSCX620xxx.xz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnSCX610.gz /boot/nnSCX62xxx.xz
```

- 4c. As shown in Step 4b directly above, type the new Release S-CX6.2.0 file name next to the previous one. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
- 4d. Reboot Net-Net SBC1.
5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.
 

```
NETNETSBC1# verify-config
```
6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.
 

```
NETNETSBC1# show version
ACME Net-Net 4500 Firmware SCX6.2.0
Build Date=10/20/09
NETNETSBC1#
```
7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.
8. Reboot Net-Net SBC1.
 

```
NETNETSBC1# reboot
```

WARNING: you are about to reboot this SD!

-----

Reboot this SD [y/n]?: **y**

9. When Net-Net SBC1 has finished rebooting, verify the systems have correctly synchronized redundancy data by using the ACLI **show health** command.
10. As you did for Net-Net SBC1, configure the boot parameters on Net-Net SBC2 so to use the new Net-Net Release S-CX6.2.0 software image. Then reboot Net-Net SBC2.

NETNETSBC2# **reboot**

-----

WARNING: you are about to reboot this SD!

-----

Reboot this SD [y/n]?: **y**

Rebooting Net-Net SBC2 causes Net-Net SBC1 to become the active system in the HA node.

11. When Net-Net SBC2 has finished rebooting, use the ACLI **show health** command to confirm it is in the standby state.

**Note:** At this point, if you need to revert to older Release SCX6.1.0 image for any reason, use [HA Backout Procedure \(367\)](#) in this chapter.

12. When you have confirmed that both systems are running Release C6.2.0, use the **save-config** command. Saving the configuration creates a persistent configuration file in the file format `data.tar.gz`.

## HA Backout Procedure

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release S-CX6.2.0 that you decide you no longer want to use, you can fall back to a previous release. This section shows you how to fall back to an older image with both systems in your HA node upgraded.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

### To backout to a previous (older) release with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release SCX6.1.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a **c** and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/boot/nnSCX620xxx.xz` and `/boot/nnSCX610.gz`, where `xxx` represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

'.' = clear field; '-' = go to previous field; ^D = quit

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnSCX620xxx.xz /boot/nnSCX610.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release S-CX6.1.0 file name next to the Release S-CX6.2.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.

```
NETNETSBC2# show version
ACME Net-Net 4500 Firmware S-CX6.1.0 GA
07/15/08
NETNETSBC2#
```

4. Initiate a switchover on Net-Net SBC2.

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release S-CX6.1.0. Net-Net SBC1 is now the standby system running Release S-CX6.1.0xxx.

5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## Upgrading S-CX6.1.0 Software Images

This document explains how to upgrade S-CX6.1.0 images on your Net-Net 4500 SBC.

### Pre-Upgrade Checklist

#### Before initially loading Net-Net SBC Release S-CX6.1.0 software:

1. Obtain the name and location of the Release CX6.0.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at [support@acmepacket.com](mailto:support@acmepacket.com).
2. Verify the integrity of your configuration using the ACLI **verify-config** command.



3. Back up a well-working configuration. Name the file descriptively so you can fall back to this configuration easily.

## Stand-alone Upgrade

This process incurs system downtime; your Net-Net 4500 SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

### Upgrade Procedure

The following procedure describes how to upgrade a Net-Net 4500 SBC running to a new software image. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

#### To upgrade a software image on a stand-alone system:

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release S-CX6.1.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release S-CX6.1.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release CX6.0.0 file name next to the previous file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /boot/nnCX600. gz and /boot/nnSCX610xxx. gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnCX600. gz /boot/nnSCX610xxx. gz
```

Note that /boot directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/nnSCX610xxx. gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running the new release.

## HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can

back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

## Upgrade Process

### To upgrade a software image for an HA node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized. You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.

- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diags.gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release S-CX6.1.0 software image.

---

**Caution:** From the point that you upgrade the image file, do not make any configuration changes. Likewise, do not use the save-config or activate-config commands.

---

4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

4b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames /boot/nnC600.gz and /boot/nnSCX610xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnC600.gz /boot/nnSCX61xxx.gz
```

4c. As shown in Step 4b directly above, type the new Release S-CX6.1.0 file name next to the previous one. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

4d. Reboot Net-Net SBC1.

5. After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

6. Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4500 Firmware SCX6.1.0 Patch 2
Build Date=07/20/08
NETNETSBC1#
```

7. Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

8. Reboot Net-Net SBC1.

```
NETNETSBC1# reboot
```

```

WARNING: you are about to reboot this SD!

```

```
Reboot this SD [y/n]?: y
```

9. When Net-Net SBC1 has finished rebooting, verify the systems have correctly synchronized redundancy data by using the ACLI **show health** command.
10. As you did for Net-Net SBC1, configure the boot parameters on Net-Net SBC2 so to use the new Net-Net Release S-CX6.1.0 software image. Then reboot Net-Net SBC2.

```
NETNETSBC2# reboot
```

```

WARNING: you are about to reboot this SD!

```

```
Reboot this SD [y/n]?: y
```

Rebooting Net-Net SBC2 causes Net-Net SBC1 to become the active system in the HA node.

11. When Net-Net SBC2 has finished rebooting, use the ACLI **show health** command to confirm it is in the standby state.

**Note:** At this point, if you need to revert to older Release CX6.0.0 image for any reason, use [HA Backout Procedure \(377\)](#) in this chapter.

12. When you have confirmed that both systems are running Release C6.1.0, use the **save-config** command. Saving the configuration creates a persistent configuration file in the file format `data.tar.gz`.

## HA Backout Procedure

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release S-CX6.1.0 that you decide you no longer want to use, you can fall back to a previous release. This section shows you how to fall back to an older image with both systems in your HA node upgraded.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

**To backout to a previous (older) release with the both Net-Net SBCs in the HA node upgraded:**

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release CX6.0.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/boot/nnSCX610xxx.gz` and `/boot/nnCX600.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
```

```
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnSCX610xxx.gz /boot/nnC600.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release CX6.0.0 file name next to the Release S-CX6.1.0 file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.

- 1d. Exit to the main Superuser prompt.

```
NETNETSBC2(configure)# exit
NETNETSBC2#
```

2. Reboot Net-Net SBC2.

3. Using the ACLI **show version** command to confirm that you are using the appropriate release.

```
NETNETSBC2# show version
ACME Net-Net 4500 Firmware CX6.0.0 GA
07/15/08
NETNETSBC2#
```

4. Initiate a switchover on Net-Net SBC2.

```
NETNETSBC2# notify berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release CX6.0.0. Net-Net SBC1 is now the standby system running Release CX6.0.0xxx.

5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## Upgrading CX6.0.0 Software Images

This document explains how to upgrade CX6.0.0 images on your Net-Net 4500 SBC.

### Pre-Upgrade Checklist

#### Before initially loading Net-Net SBC Release CX6.0.0 software:

1. Obtain the name and location of the Release CX6.0.0 software image file. Your Acme Packet customer support representative has this information and can be contacted directly or by e-mail at [support@acmepacket.com](mailto:support@acmepacket.com).
2. Verify the integrity of your configuration using the ACLI **verify-config** command.
3. Back up a well-working configuration. Name the file descriptively so you can fall back to this configuration easily.

### Stand-alone Upgrade

This process incurs system downtime; your Net-Net 4500 SBC stops passing traffic for a period of time. Please plan for your standalone upgrade accordingly.

## Upgrade Procedure

The following procedure describes how to upgrade a Net-Net 4500 SBC running to a new software image. This procedure assumes that the Net-Net SBC is booting from an image located on the Net-Net SBC's local file system.

### To upgrade a software image on a stand-alone system:

1. On the Net-Net SBC, check for adequate space in the /boot directory to upload the new Release CX6.0.0 boot image. Use the **check-space-remaining boot** command. Images consume approximately 13,000,000 bytes.

```
NETNETSBC# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC#
```

2. Upload the Net-Net SBC software image file to the /boot directory using an FTP or SFTP client.
3. Change the boot configuration parameters to use the new Release CX6.0.0 image.

Scroll through the boot parameters by pressing <Enter>. Stop when you reach the **file name** boot parameter and type the appropriate Release CX6.0.0 file name next to the previous file name. Press <Enter> to continue scrolling through the boot parameters.

The following example uses the filenames /boot/nnCX600.gz and /boot/nnCX600xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnCX600.gz /boot/nnCX600xxx.gz
```

Note that /boot directs the Net-Net SBC to look in the /boot directory for the image you specify. The above example looks for the /boot/nnCX600xxx.gz boot image.

4. Reboot the Net-Net SBC using the **reboot** command.

The Net-Net SBC should now be successfully running the new release.

## HA Upgrade

In the descriptions and processes outlined below, Net-Net SBC1 is initially the standby system and Net-Net SBC2 is initially the active system. Please read the following procedures carefully before beginning the upgrade. If necessary, you can back out of the upgrade once during the upgrade procedure and once after you have completed the upgrade procedure.

## Upgrade Process

### To upgrade a software image for an HA node:

1. Confirm that Net-Net SBC1 and Net-Net SBC2 start up and are synchronized.

You must also make sure that all of the running and current configurations on Net-Net SBC1 and Net-Net SBC2 have the same number. In the examples below, all of the configuration versions are 5.

- 1a. On Net-Net SBC1 and Net-Net SBC2, use the ACLI **show health** command to make sure that all processes are synchronized.
- 1b. On Net-Net SBC1, show the current configuration version by using the ACLI **display-current-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its current configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-current-cfg-version
Current configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-current-cfg-version
Current configuration version is 5
NETNETSBC2#
```

- 1c. On Net-Net SBC1, show the running configuration version by using the ACLI **display-running-cfg-version** command. Then use the same command on Net-Net SBC2 and be sure that its running configuration version is the same as the one on Net-Net SBC1.

```
NETNETSBC1# display-running-cfg-version
Running configuration version is 5
NETNETSBC1#
```

```
NETNETSBC2# display-running-cfg-version
Running configuration version is 5
NETNETSBC2#
```

2. On Net-Net SBC1, before loading the software image to the flash, check the remaining space in the /boot directory using the ACLI **check-space-remaining boot** command.

```
NETNETSBC1# check-space-remaining boot
```

```
boot: 24759488/25760512 bytes (99%) remaining
NETNETSBC1#
```

If you see less than 50% of the memory remaining, delete older stored firmware images to make space.

At a minimum, we recommend that you leave the `diags.gz` file and the currently running release on the flash memory (in the event that a rollback is required).

3. Upload the Net-Net SBC software image file to the /boot directory using an FTP client.
4. Change the boot configuration parameters on Net-Net SBC1 to use the appropriate Release CX6.0.0 software image.

---

**Caution:** From the point that you upgrade the image file, do not make any configuration changes. Likewise, do not use the `save-config` or `activate-config` commands.

---

## 4a. Access the boot parameters on Net-Net SBC1:

- In the ACLI configure terminal menu, type **bootparam** and press <Enter> to being displaying the list of boot parameters.

## 4b. Scroll through the boot parameters by pressing &lt;Enter&gt;. Stop when you reach the file name boot parameter.

The following example uses the filenames /boot/nnC600.gz and /boot/nnCX600xxx.gz, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnC600.gz /boot/nnC60xxx0.gz
```

## 4c. As shown in Step 4b directly above, type the new Release CX6.0.0 file name next to the previous one. Be sure that the file name is correct, or you might boot the wrong image. Press &lt;Enter&gt; to continue scrolling through the boot parameters.

## 4d. Reboot Net-Net SBC1.

- After Net-Net SBC1 has completed the boot process, use the **verify-config** command to confirm that the configuration has been upgraded properly.

```
NETNETSBC1# verify-config
```

- Confirm the Net-Net SBC1 is running the new boot image using the **show version** command.

```
NETNETSBC1# show version
ACME Net-Net 4500 Firmware CX6.0.0 Patch 2
Build Date=07/20/08
NETNETSBC1#
```

- Use the ACLI **show health** command to confirm that Net-Net SBC1 is the standby system.

- Reboot Net-Net SBC1.

```
NETNETSBC1# reboot
```

```

WARNING: you are about to reboot this SD!

```

```
Reboot this SD [y/n]?: y
```

- When Net-Net SBC1 has finished rebooting, verify the systems have correctly synchronized redundancy data by using the ACLI **show health** command.

- As you did for Net-Net SBC1, configure the boot parameters on Net-Net SBC2 so to use the new Net-Net Release CX6.0.0 software image. Then reboot Net-Net SBC2.

```
NETNETSBC2# reboot
```

```

```



WARNING: you are about to reboot this SD!

-----

Reboot this SD [y/n]?: **y**

Rebooting Net-Net SBC2 causes Net-Net SBC1 to become the active system in the HA node.

11. When Net-Net SBC2 has finished rebooting, use the ACLI **show health** command to confirm it is in the standby state.

**Note:** At this point, if you need to revert to older Release CX6.0.0 image for any reason, use [HA Backout Procedure \(377\)](#) in this chapter.

12. When you have confirmed that both systems are running Release C6.0.0, use the **save-config** command. Saving the configuration creates a persistent configuration file in the file format `data.tar.gz`.

## HA Backout Procedure

If you reach the point in your upgrade procedure where you have upgraded both Net-Net SBCs in the HA node to Release CX6.0.0 that you decide you no longer want to use, you can fall back to a previous release. This section shows you how to fall back to an older image with both systems in your HA node upgraded.

In the descriptions and processes outlined below, Net-Net SBC1 is the active system and Net-Net SBC2 is the standby system. The procedure uses these designations because when you have completed upgrade process specific to these releases, Net-Net SBC1 is the active system.

### To backout to a previous (older) release with the both Net-Net SBCs in the HA node upgraded:

1. Change the boot parameters on Net-Net SBC2 to use the appropriate Release CX6.0.0 software image.
  - 1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
    - Reboot the Net-Net SBC using any of the ACLI **reboot** commands. Stop the booting process by hitting the Space bar on your keyboard to halt boot-up when you see this message: Press any key to stop auto-boot. . . . Type a c and press <Enter> to begin displaying the boot parameters.
    - In the ACLI configure terminal menu, type **bootparam** and press <Enter> to begin displaying the list of boot parameters.
  - 1b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

The following example uses the filenames `/boot/nnCX600xxx.gz` and `/boot/nnCX600.gz`, where xxx represents the individual software numbers for these releases.

```
NETNETSBC1# configure terminal
NETNETSBC1(configure)# bootparam
```

```
'.' = clear field; '-' = go to previous field; ^D = quit
```

```
boot device : eth0
processor number : 0
host name : boothost
file name : /boot/nnCX600xxx.gz /boot/nnC600.gz
```

- 1c. As in the example in Step 1b directly above, type the appropriate Release CX6.0.0 file name next to the Release CX6.0.0xxx file name. Be sure that the file name is correct, or you might boot the wrong image. Press <Enter> to continue scrolling through the boot parameters.
- 1d. Exit to the main Superuser prompt.  

```
NETNETSBC2(confi gure)# exi t
NETNETSBC2#
```
2. Reboot Net-Net SBC2.
3. Using the ACLI **show version** command to confirm that you are using the appropriate release.  

```
NETNETSBC2# show version
ACME Net-Net 4500 Firmware CX6.0.0 GA
07/15/08
NETNETSBC2#
```
4. Initiate a switchover on Net-Net SBC2.  

```
NETNETSBC2# noti fy berpd force
```

At this point, Net-Net SBC2 becomes the active system running Release CX6.0.0. Net-Net SBC1 is now the standby system running Release CX6.0.0xxx.
5. On Net-Net SBC1, change the boot parameters as you did in Step 1 of this procedure.
6. On Net-Net SBC1, restore the back up configuration as you did in Step 6 of this procedure.
7. Reboot Net-Net SBC1.

## Moving a Configuration

---

This section outlines a process for moving your Net-Net 4250 configuration to your Net-Net 4500. You accomplish this task the same way you would move a back-up configuration from one Net-Net 4250 to another using FTP, and then restoring the back on the other Net-Net 4250.

Process summary:

1. Create a backup configuration file on your Net-Net 4250.
2. Using FTP, copy your Net-Net 4250 backup from to your Net-Net 4500.
3. Restore the newly-transferred backup on your Net-Net 4500.

## Backup Commands

The Net-Net 4000 SBC includes a set of commands for easily working with backup configurations. These commands are **backup-config**, **display-backups**, **delete-backup-config**, **restore-backup-config**.

To back up the Net-Net 4000 configuration, use the **backup-config** command. You can confirm your backup has been created with the **display-backups** command. When the **backup-config** command is executed, the Net-Net system checks if sufficient resources exist to complete the operation. If resources are sufficient, the Net-Net system creates the backup. If resources are insufficient, the task is not completed and the SD software instead displays the limiting resources, recommending that the task be completed at another time.

Backups are created as gzipped tar files in a .tar.gz format. They are stored in the /code/bkups directory on the Net-Net 4000.

## Creating a Backup on Your Net-Net 4250

### To create a backup:

1. In the ACLI at the Superuser prompt, enter the **backup-config** command followed by a descriptive filename for the backup you are creating.

```
ACMEPACKET4250# backup-config 02_Feb_2008

task done
ACMEPACKET4250#
```

## Listing Backups

You can view a list of the backups available on your system using the ACLI **display-backups** command.

### To list available backup configurations:

1. In Superuser mode, enter the **display-backups** command. A list of available backup files from the /code/bkups directory is displayed on the screen.

```
ACMEPACKET4250# display-backups
test-config.tar.gz
test-config.tar.gz
runningcfgtest.tar.gz
runningtest_one.tar.gz
BACKUP_CONFIG.tar.gz
02_Feb_2008.tar.gz
01_Feb_2008.tar.gz
ACMEPACKET#
```

## Copying the Backup to Your Net-Net 4500

Using FTP, you simply copy the backup configuration file from your Net-Net 4250 to your Net-Net 4500.

### To copy a backup configuration from your Net-Net 4250 to your Net-Net 4500:

1. Use an FTP client to connect to the Net-Net 4250 using the default username: user and password: acme. The IP address of the Net-Net 4250 is configured in the bootparams.
2. Change directory to where you want to upload a file.
  - cd /code/bkups for backup configurations
3. Type bin and press <Enter> to force the FTP program into binary mode.
4. Upload the file you wish to transfer by typing put filename and pressing <Enter>.

```
C:\Documents and Settings>ftp 172.30.55.127
Connected to 172.30.55.127.
220 VxWorks (1.0) FTP server ready
User (172.30.55.127: (none)): user
331 Password required
Password:
230 User logged in
ftp> cd /code/bkups
```

```

250 Changed directory to "/code/bkups"
ftp> bin
200 Type set to I, binary mode
ftp> put 02_Feb_2008.tar.gz
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 9587350 bytes sent in 51.64Seconds 185.65Kbytes/sec.
ftp>

```

## Restoring Backups

### To restore a backup configuration on your Net-Net 4500:

1. In Superuser mode, enter the **restore-backup-config** command followed by the backup filename you wish to restore to the current configuration. You must explicitly name the backup file you wish to restore, including the file extension

```

ACMEPACKET4500# restore-backup-config 02_Feb_2008.tar.gz
Need to perform save-config and activate/reboot activate for changes to take effect...
task done
ACMEPACKET4500#

```

2. Save your configuration.

```

ACMEPACKET4500# save-config

```

3. Activate your configuration.

```

ACMEPACKET4500# activate-config

```

## Configuration Overview

The Net-Net SBC uses three configuration spaces: the current configuration, last-saved configuration, and the running configuration. The current configuration is a temporary workspace where changes to the Net-Net SBC configuration are initially stored before they go “live.” Once you are satisfied with your edits, they are saved to the last-saved configuration space, as a backup configuration that is persistent across reboot. Finally, when you execute the **activate-config** command the Net-Net SBC goes “live” using this configuration and makes a copy of the configuration. The copy is also stored on the Net-Net SBC’s file system and is called the running configuration, reflecting the running state of the Net-Net SBC.

The following table lists the three configuration spaces along with the creation command and location of configuration.

| Configuration Name       | ACLI Command to create | Location of Configuration |
|--------------------------|------------------------|---------------------------|
| Current Configuration    | done                   | /ramdrv/data              |
| Last-saved Configuration | save-config            | /code/config              |
| Running Configuration    | activate-config        | /ramdrv/running           |

## Configuration Process

**To make configuration changes, set a current configuration, create a last-saved configuration, and finally enact your changes by making a running configuration:**

1. Set all the necessary parameters on the SD. Each time you complete configuring a full configuration element, type **done** to set that element and update the current configuration. When all configuration elements are set, back out of configuration tree to the topmost ACLI level at the superuser prompt. The following example sets an arbitrary configuration element and backs you out to the superuser prompt.

```
ACMEPACKET(host-route)# dest-network 10.0.0.0
ACMEPACKET(host-route)# netmask 255.255.0.0
ACMEPACKET(host-route)# gateway 172.30.0.1
ACMEPACKET(host-route)# done
host-routes
 dest-network 10.0.0.0
 netmask 255.255.0.0
 gateway 172.30.0.1
ACMEPACKET(host-route)# exi t
ACMEPACKET(system)# exi t
ACMEPACKET(configure)# exi t
```

2. Save all configurations to the last-saved configuration by using the **save-config** command. This step is mandatory.

```
ACMEPACKET# save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET#
```

3. Set the Net-Net SBC to enact the last-saved configuration into the running state by using the **activate-config** command. This will make the last-saved configuration the running configuration and write it to the local file system.

```
ACMEPACKET# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
H323 Active Stack Cnt: 0
Request to 'ACTIVATE-CONFIG' has finished,
Activate Complete
ACMEPACKET#
```

## Verifying & Regenerating Configurations

The **verify-config** command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Net-Net SBC.

When the **verify-config** command is run, anything configured that is inconsistent produces either an error or a warning message. An error message lets the user know that there is something wrong in the configuration that will affect the way Net-Net SBC runs. A warning message lets the user know that there is something wrong in the configuration, but it will not affect the way the Net-Net SBC runs. The following is an example of the **verify-config** output:

```
ACMEPACKET# verify-config

ERROR: realm-config [r172] is missing entry for network-interface
ERROR: sip-nat [nat172] is missing ext-address entry
ERROR: sip-nat [nat172] is missing ext-proxy-address entry
ERROR: sip-nat [nat172] is missing domain-suffix entry
WARNING: sip-nat [nat172] has ext-address [5.6.7.8] which is different from sip-
interface [sip172] sip-port address [1.2.3.4]

Total:
4 errors
1 warning
```

Every time a user executes the **save-config** command, **verify-config** is automatically run. If any configuration problems are found, you receive a message pointing to the number of errors found during the saving, along with a recommendation to run the **verify-config** command to view the errors fully. The following is an example of the **save-config** verification output:

```
ACMEPACKET# save-config

```

Results of config verification:

4 configuration errors

2 configuration warnings

Run "verify-config" for more details

-----  
Save-Config received, processing.

waiting 1200 for request to finish

Request to 'SAVE-CONFIG' has Finished,

Save complete

Currently active and saved configurations do not match!

To sync & activate, run 'activate-config' or 'reboot activate'.

## Verifying Address Duplication

The **verify-config** command, entered either directly or via the **save-config** command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- Every address entered is checked against the Primary and Secondary Utility addresses
- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

The following tables display the entire list of addresses which are checked for duplication, the network-interface or realm which they are checked against, and the port range:

## Network-Interface

| Parameter Name   | Address Type | Network Interface or Realm | Port Start | Port End |
|------------------|--------------|----------------------------|------------|----------|
| pri-utility-addr | Primary      | itself                     | 0          | 0        |
| sec-utility-addr | Secondary    | itself                     | 0          | 0        |
| ip-address       | Unknown      | itself                     | 0          | 0        |
| ftp-address      | Unknown      | itself                     | 0          | 0        |
| snmp-address     | Unknown      | itself                     | 0          | 0        |
| telnet-address   | Unknown      | itself                     | 0          | 0        |
| dns-ip-primary   | Unknown      | itself                     | 0          | 0        |
| dns-ip-backup1   | Unknown      | itself                     | 0          | 0        |
| dns-ip-backup2   | Unknown      | itself                     | 0          | 0        |
| hip-ip-address   | Unknown      | itself                     | 0          | 0        |
| icmp-address     | Unknown      | itself                     | 0          | 0        |

**Steering-Pool**

| Parameter Name | Address Type | Network Interface or Realm    | Port Start | Port End |
|----------------|--------------|-------------------------------|------------|----------|
| ip-address     | UDP          | network-interface or realm-id | start-port | end-port |

**SIP-Interface**

| Parameter Name   | Address Type                     | Network Interface or Realm | Port Start     | Port End     |
|------------------|----------------------------------|----------------------------|----------------|--------------|
| sip-port address | transport-protocol (UDP or TCP)  | realm-id                   | sip-port port  | 0            |
| sip-port address | UDP if transport-protocol is UDP | realm-id                   | port-map-start | port-map-end |

**SIP-NAT**

| Parameter Name     | Address Type | Network Interface or Realm | Port Start | Port End |
|--------------------|--------------|----------------------------|------------|----------|
| ext-proxy-address  | Unknown      | realm-id                   | 0          | 0        |
| home-proxy-address | Unknown      | realm-id                   | 0          | 0        |
| home-address       | Unknown      | realm-id                   | 0          | 0        |
| ext-address        | Unknown      | realm-id                   | 0          | 0        |

\* The **home-address** value must be unique across all network interfaces configured on the Net-Net SBC.

**MGCP-Config**

| Parameter Name       | Address Type | Network Interface or Realm | Port Start         | Port End     |
|----------------------|--------------|----------------------------|--------------------|--------------|
| private-address      | UDP          | private-realm              | private-port       | 0            |
| public-ca-address    | UDP          | public-realm               | pub-ca-port        | 0            |
| public-gw-address/32 | UDP          | public-realm               | pub-gw-port        | 0            |
| public-gw-address/32 | UDP          | public-realm               | second-pub-gw-port | 0            |
| public-gw-address/32 | UDP          | public-realm               | port-map-start     | port-map-end |



**H323-Stack**

| Parameter Name     | Address Type | Network Interface or Realm | Port Start         | Port End                                     |
|--------------------|--------------|----------------------------|--------------------|----------------------------------------------|
| local-ip           | TCP          | realm-id                   | q031-port          | 0                                            |
| local-ip           | TCP          | realm-id                   | q931-start-port    | q931-start-port + q931-number-ports - 1      |
| local-ip           | TCP          | realm-id                   | dynamic-start-port | dynamic-start-port + dynamic-number-port - 1 |
| local-ip           | UDP          | realm-id                   | ras-port           | 0                                            |
| gatekeeper         | Unknown      | realm-id                   | 0                  | 0                                            |
| alternate-protocol | UDP          | realm-id                   | it's port          | 0                                            |

\* If an **h323-stack's** **q931-port** (TCP) parameter is configured with a value of 1720, there is an address duplication exception. This configured port can exist within two port map ranges; the value of **q931-start-port** and its entire port range, and the value of **dynamic-start-port** and its entire port range.

**Local-Policy>Local-Policy-Attributes**

| Parameter Name | Address Type | Network Interface or Realm | Port Start | Port End |
|----------------|--------------|----------------------------|------------|----------|
| next-hop       | Unknown      | realm                      | 0          | 0        |

**Session-Agent**

| Parameter Name                           | Address Type | Network Interface or Realm                          | Port Start | Port End |
|------------------------------------------|--------------|-----------------------------------------------------|------------|----------|
| ip-address                               | UDP or TCP   | realm-id                                            | port       | 0        |
| host-name (If different from ip-address) | UDP or TCP   | realm-id                                            | port       | 0        |
| ip-address                               | UDP or TCP   | egress-realm-id if no realm-id or different from it | port       | 0        |
| host-name (If different from ip-address) | UDP or TCP   | egress-realm-id if no realm-id or different from it | port       | 0        |

**Static-Flow**

| Parameter Name     | Address Type                                        | Network Interface or Realm | Port Start | Port End |
|--------------------|-----------------------------------------------------|----------------------------|------------|----------|
| in-source/32       | Unknown                                             | in-realm-id                | 0          | 0        |
| in-destination/32  | UDP or TCP if ALG is TFTP or otherwise unknown      | in-realm-id                | start-port | end-port |
| out-source/32      | UDP or TCP if ALG is TFTP or NAPT otherwise unknown | out-realm-id               | start-port | end-port |
| out-destination/32 | Unknown                                             | out-realm-id               | 0          | 0        |

**Capture-Receiver**

| Parameter Name | Address Type | Network Interface or Realm | Port Start | Port End |
|----------------|--------------|----------------------------|------------|----------|
| address        | Unknown      | network-interface          | 0          | 0        |

**Realm-Config**

| Parameter Name  | Address Type | Network Interface or Realm | Port Start        | Port End |
|-----------------|--------------|----------------------------|-------------------|----------|
| stun-server-ip  | UDP          | network-interfaces         | stun-server-port  | 0        |
| stun-server-ip  | UDP          | network-interfaces         | stun-changed-port | 0        |
| stun-changed-ip | UDP          | network-interfaces         | stun-server-port  | 0        |
| stun-changed-ip | UDP          | network-interfaces         | stun-changed-port | 0        |

**Verify-Config Errors and Warnings**

The following tables list every error and warning the **verify-config** command produces for each configuration element:

**Access-Control**

| Error Text                                                                      | Reason for Error                   |
|---------------------------------------------------------------------------------|------------------------------------|
| WARNING: access-control [id] has unsupported application-protocol [x]           | Unsupported protocols [x]          |
| ERROR: access-control [id] has reference to realm-id [xyz] which does not exist | Realm was not found in realm table |

## Account-Config

| Error Text                                                                                                                  | Reason for Error                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| ERROR: account-config is enabled, but there are no account servers configured                                               | State is enabled, file-output is disabled and there are not servers                       |
| WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled                       | State and file-output are enabled, there are not account servers and ftp-push is disabled |
| WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled        | State and ftp-push are enabled, account servers are configured, file-output is disabled   |
| ERROR : account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured     | State and ftp-push are enabled, but there is no ftp-address or push-receiver configured   |
| ERROR: account-config has reference to push-receiver [xyz] which can not get password                                       | Password failed decryption                                                                |
| ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set                              | Push-receiver has no remote-path set                                                      |
| ERROR: account-config has reference to push-receiver [xyz] which does not have username set                                 | Push-receiver has no username set                                                         |
| ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP                | Push-receiver has no password set for FTP                                                 |
| WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP              | Push-receiver has set public key, but protocol is FTP                                     |
| ERROR: account-config has reference to push-receiver [xyz] which does not have password or public key set for protocol SFTP | Push-receiver has no password or public key set for SFTP                                  |
| ERROR: account-config has push-receiver [xyz] with reference to public-key [zyx] which does not exist                       | Public key was not found in public key table                                              |
| ERROR: account-config has account-server [IP:Port] with empty secret                                                        | Account-server [IP:Port] has empty secret field                                           |

## Authentication

| Error Text                                                                                | Reason for Error                           |
|-------------------------------------------------------------------------------------------|--------------------------------------------|
| ERROR: authentication has specified unsupported protocol [x] for type [y]                 | Unsupported protocols for given type       |
| ERROR: authentication has no configured active radius servers for authentication type [x] | No configured active radius for given type |

## Call-Recording-Server

| Error Text                                                                                 | Reason for Error                                          |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ERROR: call-recording-server must have a name                                              | Name is missing                                           |
| ERROR: call-recording-server [id] must have a primary-signaling-addr or primary-media-addr | There has to be either primary signaling or media address |

| Error Text                                                                                        | Reason for Error                                          |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ERROR: call-recording-server [id] is missing primary-realm                                        | Realm name is missing                                     |
| ERROR: call-recording-server [id] has reference to the primary-realm [xyz] which does not exist   | Primary-realm [xyz] was not found in realm-config table   |
| ERROR: call-recording-server [id] has reference to the secondary-realm [xyz] which does not exist | Secondary-realm [xyz] was not found in realm-config table |

## Capture-Receiver

| Error Text                                                                                 | Reason for Error                                           |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist | Network-interface was not found in network-interface table |

## Certificate-Record

| Error Text                                                              | Reason for Error                                     |
|-------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: certificate-record [id] is not trusted and will not be loaded    | Certificate record is not trusted                    |
| ERROR: certificate-record [id] cannot extract private key               | Certificate record failed to extract the private key |
| ERROR: certificate-record [id] cannot convert PKCS7 string to structure | Failure to convert PKCS7 record to the structure     |

## Class-Policy

| Error Text                                                                            | Reason for Error                                           |
|---------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: class-policy [id] has reference to the media-policy [xyz] which does not exist | Media-policy [xyz] was not found in the media-policy table |

## DNS-Config

| Error Text                                                                      | Reason for Error                                     |
|---------------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: dns-config [id] is missing client-realm entry                            | Missing client realm                                 |
| ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist | Realm was not found in the realm-config table        |
| ERROR: dns-config [id] does not have any server-dns-attributes                  | Server-dns-attributes are missing                    |
| ERROR: dns-config [id] is missing server-realm entry                            | Realm entry is missing (source address is empty)     |
| ERROR: dns-config [id] is missing server-realm entry for source-address [x]     | Realm entry is missing (source address is not empty) |
| ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist | Realm was not found in the realm-config table        |

**ENUM-Config**

| Error Text                                                                       | Reason for Error                                |
|----------------------------------------------------------------------------------|-------------------------------------------------|
| ERROR: enum-config [id] is missing realm-id entry                                | Missing realm                                   |
| ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist | Realm [xyz] was not found in realm-config table |
| ERROR: enum-config [id] has no enum-servers                                      | List of ENUM servers is empty                   |

**Ext-Policy-Server**

| Error Text                                                                       | Reason for Error                              |
|----------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: ext-policy-server [id] is missing realm entry                             | Missing realm                                 |
| ERROR: ext-policy-server [id] address is not valid                               | Invalid address entry                         |
| ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid | Invalid protocol entry                        |
| ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist  | Realm was not found in the realm-config table |

**H323-Stack**

| Error Text                                                                          | Reason for Error                                   |
|-------------------------------------------------------------------------------------|----------------------------------------------------|
| ERROR: h323-stack [id] has no realm-id                                              | Missing realm entry                                |
| ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist     | Realm was not found in the realm-config table      |
| WARNING: h323-stack [id] is missing local-ip address entry                          | Missing address entry                              |
| WARNING : h323-stack [id] has reference to media-profile [xyz] which does not exist | Media profile was not found in media profile table |
| ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist  | Stack name was not found in the h323-stack table   |

**Host-Route**

| Error Text                                                                                            | Reason for Error                                            |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| WARNING: host-route [id] has reference to gateway [xyz] which does not exist in any network-interface | gateway entry was not found in any network-interface object |

**IWF-Config**

| Error Text                                                                    | Reason for Error                                   |
|-------------------------------------------------------------------------------|----------------------------------------------------|
| WARNING: iwf-config has reference to media-profile [xyz] which does not exist | media profile was not found in media profile table |

## Local-Policy

| Error Text                                                                                                           | Reason for Error                                                                                |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist                                    | Source-realm [xyz] was not found in realm-config table                                          |
| WARNING: local-policy [id] has no policy-attributes set                                                              | No policy-attributes set                                                                        |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist        | Realm [xyz] was not found in realm-config table                                                 |
| ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry                                | Next-hop is missing for given attribute                                                         |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid         | Invalid value for the next-hop                                                                  |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist     | Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group) |
| WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist | Media-policy [xyz] was not found in media-policy table                                          |

## Local-Routing-Config

| Error Text                                                                                 | Reason for Error                                     |
|--------------------------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist | specified file is missing from /boot/code/lrt folder |

## MGCP-Config

| Error Text                                                                                                     | Reason for Error                                               |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ERROR: mgcp-config [id] is missing private-realm entry                                                         | Private-realm empty                                            |
| ERROR: mgcp-config [id] has reference to private-realm [xyz] which does not exist                              | Realm was not found in realm-config table                      |
| ERROR: mgcp-config [id] is missing public-realm entry                                                          | Public-realm empty                                             |
| ERROR: mgcp-config [id] has reference to public-realm [xyz] which does not exist                               | Realm was not found in the realm-config table                  |
| ERROR: mgcp-config [id] has identical private-address and public-gw-address [x] for the same network interface | Private-address and public-gw-address are identical on same NI |

## Network-Interface

| Error Text                                                                              | Reason for Error                                                  |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist | Phy-interface [xyz] was not found in phy-interface table          |
| ERROR: network-interface [id] is missing pri-utility-addr entry                         | If redundancy is enabled pri-utility-addr entry has to be entered |

| Error Text                                                                          | Reason for Error                                                                                       |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| ERROR: network-interface [id] is missing sec-utility-addr entry                     | If redundancy is enabled sec-utility-addr entry has to be entered                                      |
| ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty | Dns-domain is empty. Word "address" will be plural "addresses" if there are more DNS addresses entered |
| ERROR: network-interface [id] has reference to DNS address, but ip-address is empty | Ip-address is empty. Word "address" will be plural "addresses" if there are more DNS addresses entered |

## Phy-Interface

| Error Text                                                                                                | Reason for Error                                                                  |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| ERROR: phy-interface [id] has invalid operation-type value [x]                                            | Operation-type value is invalid                                                   |
| ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name                         | If type is MAINTENANCE or CONTROL name has to start with either "eth" or "wancom" |
| ERROR: phy-interface [id] of type [x] has duplicated port [y] and slot [z] values with phy-interface [di] | Port and slot values are duplicated with another phy-interface                    |

## Public-Key

| Error Text                                                                         | Reason for Error                |
|------------------------------------------------------------------------------------|---------------------------------|
| ERROR: public-key [id] has no public/private key pair generated for public-key [x] | No public/private key generated |
| ERROR: public-key [id] cannot extract private key                                  | Cannot extract private key      |

## Realm-Config

| Error Text                                                                             | Reason for Error                                             |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which does not exist    | Missing external BW manager                                  |
| ERROR: realm-config [id] is missing entry for network-interface                        | Missing Network Interface                                    |
| ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist | Network interface was not found in network-interface table   |
| ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist      | Media-policy was not found in media-policy table             |
| ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist     | Class-profile was not found in class-profile table           |
| ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist  | In-translationid was not found in session translation table  |
| ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist | Out-translationid was not found in session translation table |

| Error Text                                                                                    | Reason for Error                                                                               |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist        | In-manipulationid was not found in manipulation table                                          |
| ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist       | Out-manipulationid was not found in manipulation table                                         |
| ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist      | Enforcement-profile was not found in enforcement-profile table                                 |
| ERROR: realm-config [id] has reference to call-recording-server-id [xyz] which does not exist | Call-recording-server-id was not found in call-recording-server-table                          |
| ERROR: realm-config [id] has reference to codec-policy [xyz] which does not exist             | Codec-policy was not found in codec-policy table                                               |
| ERROR: realm-config [id] has reference to constraint-name [xyz] which does not exist          | Constraint-name was not found in session constraint table                                      |
| ERROR: realm-config [id] has reference to qos-constraint [xyz] which does not exist           | Qos-constraint was not found in qos constraint table                                           |
| ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms           | Realm and its parent realm are part of the closed loop where they referring back to themselves |
| ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist                | Dns-realm doesn't exist in the realm table                                                     |
| WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)   | Realm name and parent name are the same                                                        |
| ERROR: realm-config [id] has reference to parent-realm [xyz] which does not exist             | Parent realm doesn't exist in the realm table                                                  |
| ERROR: realm-config [id] has identical stun-server-port and stun-changed port [x]             | Stun-server-ip is identical to stun-changed-ip, when stun is enabled                           |
| ERROR: realm-config [id] has identical stun-server-ip and stun-changed-ip [x]                 | Stun-server-port is identical to stun-changed-port, when stun is enabled                       |

## Realm-Group

|                                                                                       |                                           |
|---------------------------------------------------------------------------------------|-------------------------------------------|
| ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist      | Realm was not found in realm-config table |
| ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist | Realm was not found in realm-config table |



## Redundancy

| Error Text                                                                                                                 | Reason for Error                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr from network-interface [y]        | If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface (pri-utility-addr is missing here)   |
| ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr [z] from network-interface [y]    | If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface                                      |
| ERROR: redundancy-config peer [id] has Address [x] which does not match sec-utility-addr from network-interface [y]        | If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface (sec-utility-addr is missing here) |
| ERROR: redundancy-config peer [id] has IP Address [x] which does not match sec-utility-addr [z] from network-interface [y] | If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface                                    |
| ERROR: redundancy-config peer [id] has reference to network-interface [xyz] which does not exist                           | Network-interface [xyz] was not found in network-interface table                                                                                          |
| ERROR: redundancy-config peer [id] is missing destination object                                                           | Destination object is missing                                                                                                                             |
| ERROR: redundancy-config is missing Primary peer object                                                                    | Primary peer object is missing                                                                                                                            |
| ERROR: redundancy-config is missing Secondary peer object                                                                  | Secondary peer object is missing                                                                                                                          |
| ERROR: redundancy-config is missing both Primary and Secondary peer objects                                                | Primary and Secondary peer objects are missing                                                                                                            |

## Security-Association

| Error Text                                                                                                                                                           | Reason for Error                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: security-association [id] is missing network-interface entry                                                                                                  | Missing network-interface entry                            |
| ERROR: security-association [id] has reference to network-interface [xyz] which does not exist                                                                       | Network-interface was not found in network-interface table |
| ERROR: security-association [id] has invalid local-ip-addr                                                                                                           | Invalid local-ip-addr entry                                |
| ERROR: security-association [id] has invalid remote-ip-addr                                                                                                          | Invalid remote-ip-addr entry                               |
| ERROR: security-association [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface                                           | Network-interface is not valid IPSEC media interface       |
| ERROR: security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password | Failed to decrypt auth-key                                 |
| ERROR: security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long                                         | Invalid length of the auth-key for auth-algo [hmac-md5]    |
| ERROR: security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long                                        | Invalid length of the auth-key for auth-algo [hmac-sha1]   |

| Error Text                                                                                                                                                           | Reason for Error                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password | Failed to decrypt encr-key                    |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 64 bits (odd parity in hex)                                        | Invalid encr-key length for given algorithm   |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 192 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm   |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 128 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm   |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 256 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm   |
| ERROR: security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]                                                              | Has invalid aes-ctr-nonce for given algorithm |
| ERROR: security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)                                                       | Invalid tunnel-mode local-ip-addr             |
| ERROR: security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)                                                     | Invalid tunnel-mode remote-ip-addr            |
| ERROR: security-association [id] has invalid espudp local-ip-addr (must be non-zero)                                                                                 | Invalid espudp local-ip-addr                  |
| ERROR: security-association [id] has invalid espudp remote-ip-addr (must be non-zero)                                                                                | Invalid espudp remote-ip-addr                 |
| ERROR: security-association [id] has invalid espudp local-port (must be non-zero)                                                                                    | Invalid espudp local-port                     |
| ERROR: security-association [id] has invalid espudp remote-port (must be non-zero)                                                                                   | Invalid espudp remote-port                    |

## Security-Policy

| Error Text                                                                     | Reason for Error                |
|--------------------------------------------------------------------------------|---------------------------------|
| ERROR: security-policy [id] has invalid local-ip-addr-match                    | Empty local-ip-addr-match       |
| ERROR: security-policy [id] has invalid local-ip-addr-match [x]                | Invalid local-ip-addr-match     |
| ERROR: security-policy [id] has invalid remote-ip-addr-match                   | Empty remote-ip-addr-match      |
| ERROR: security-policy [id] has invalid remote-ip-addr-match [x]               | Invalid remote-ip-addr-match    |
| ERROR: security-policy [id] is missing network-interface entry                 | Missing network-interface entry |
| ERROR: security-policy [id] priority [x] is identical to security-policy [id2] | Duplication of the priorities   |

| Error Text                                                                                                            | Reason for Error                                           |
|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: security-policy [id] has reference to network-interface [xyz] which does not exist                             | Network-interface was not found in network-interface table |
| ERROR: security-policy [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface | Network-interface is not valid IPSEC media interface       |

## Session-Agent

| Error Text                                                                                | Reason for Error                                               |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist            | Realm was not found in realm table                             |
| ERROR: session-agent [id] has reference to egress-realm-id [xyz] which does not exist     | Realm was not found in realm table                             |
| ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist    | Translation id was not found in translation table              |
| ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist   | Translation id was not found in translation table              |
| ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist   | Manipulation id was not found in manipulation table            |
| ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist  | Manipulation id was not found in manipulation table            |
| ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist | Enforcement-profile was not found in enforcement-profile table |
| ERROR: session-agent [id] has reference to code-policy [xyz] which does not exist         | Codec-policy was not found in codec-policy table               |
| ERROR: session-agent [id] has reference to response-map [xyz] which does not exist        | Response-map was not found in response map table               |
| ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist  | Response-map was not found in response map table               |

## Session-Group

| Error Text                                                                          | Reason for Error                                       |
|-------------------------------------------------------------------------------------|--------------------------------------------------------|
| ERROR: session-group [id] has reference to session-agent [xyz] which does not exist | Session agent was not found in the session agent table |

## Session-Translation

| Error Text                                                                                 | Reason for Error                                             |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ERROR: session-translation [id] has reference to rules-called [xyz] which does not exist   | Translation rule was not found in the translation rule table |
| ERROR: session-translations [id] has reference to rules-calling [xyz] which does not exist | Translation rule was not found in the translation rule table |

## SIP-Config

| Error Text                                                                                 | Reason for Error                                                                                       |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| ERROR: sip-config has reference to home-realm-id [xyz] which does not exist                | Realm was not found in the realm-config table                                                          |
| ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist              | Realm was not found in the realm-config table                                                          |
| ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist          | Enforcement profile was not found in enforcement profile table                                         |
| WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [sip-internal-realm] | Missing home-realm-id, defaulted to sip-internal-realm                                                 |
| WARNING: sip-config home-realm-id [xyz] does not have a sip-interface                      | Sip-interface missing for the home realm                                                               |
| WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects   | Nat-mode needs to be set to either Public or Private if there are sip-nat objects in the configuration |
| ERROR: sip-config object is disabled                                                       | Sip-config is disabled, but there are configured sip-interface objects                                 |

## SIP-Interface

| Error Text                                                                                                | Reason for Error                                                                                    |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ERROR: sip-interface [id] is missing realm-id entry                                                       | missing realm                                                                                       |
| ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist                            | realm was not found in realm-config table                                                           |
| ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist                   | in-manipulationid was not found in manipulation table                                               |
| ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist                  | out-manipulationid was not found in manipulation table                                              |
| ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist                 | enforcement profile was not found in enforcement profile table                                      |
| ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist                        | response-map was not found in response-map table                                                    |
| ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist                  | local-response-map was not found in response-map table                                              |
| ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist                     | constraint-name was not found in session constraint table                                           |
| ERROR: sip-interface [id] has no sip-ports                                                                | sip-ports are missing                                                                               |
| ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist     | tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)               |
| ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist | ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS) |

| Error Text                                                                         | Reason for Error                                       |
|------------------------------------------------------------------------------------|--------------------------------------------------------|
| WARNING: sip-interface [id] has no sip-ports, using SIP-NAT external-address       | no sip-ports so SIP-NAT external-address is used       |
| WARNING: sip-interface [id] has no valid sip-ports, using SIP-NAT external-address | no valid sip-ports so SIP-NAT external-address is used |

## SIP-Manipulation

| Error Text                                                                                                         | Reason for Error                                                   |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| ERROR: sip-manipulation [id] has no header-rules defined                                                           | Missing header rules                                               |
| ERROR: sip-manipulation [id] with header-rule [xyz] is missing new-value entry                                     | Missing new-value entry (checked only for action type "sip-manip") |
| ERROR: sip-manipulation [id] with header-rule [xyz] has reference to new-value [zxy] which does not exist          | New-value entry missing from the sip-manipulation table            |
| ERROR: sip-manipulation [id] with header-rule [xyz] has new-value that refers to itself from sip-manipulation [di] | Looping reference between two objects                              |

## SIP-NAT

| Error Text                                                                                                | Reason for Error                                             |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ERROR: sip-nat [id] is missing home-address entry                                                         | Missing home-address                                         |
| ERROR: sip-nat [id] has invalid home-address [x] entry                                                    | Invalid home-address entry                                   |
| ERROR: sip-nat [id] is missing ext-address entry                                                          | Missing ext-address                                          |
| ERROR: sip-nat [id] has invalid ext-address [x] entry                                                     | Invalid ext-address entry                                    |
| ERROR: sip-nat [id] is missing ext-proxy-address entry                                                    | Missing ext-proxy-address                                    |
| ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry                                               | Invalid ext-proxy-address entry                              |
| ERROR: sip-nat [id] is missing user-nat-tag entry                                                         | Missing user-nat-tag                                         |
| ERROR: sip-nat [id] is missing host-nat-tag entry                                                         | Missing host-nat-tag                                         |
| ERROR: sip-nat [id] is missing domain-suffix entry                                                        | Missing domain-suffix                                        |
| ERROR: sip-nat [id] is missing realm-id entry                                                             | Missing realm entry                                          |
| ERROR: sip-nat [id] does not match sip-interface realm [xyz]                                              | Sip-interface name was not found in realm table              |
| ERROR: sip-nat [id] does not have a sip-interface                                                         | Sip-interface is missing                                     |
| WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]                                               | Duplicated user-nat-tag                                      |
| WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]                                               | Duplicated host-nat-tag                                      |
| WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y] | Sip-nat ext-address needs to be the same as sip-port address |
| ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]                                             | Duplicated home-address                                      |

**Static-Flow**

| Error Text                                                                       | Reason for Error                              |
|----------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: static-flow [id] is missing in-realm-id entry                             | Missing in-realm-id                           |
| ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist  | Realm was not found in the realm-config table |
| ERROR: static-flow [id] is missing out-realm-id entry                            | Missing out-realm-id                          |
| ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist | Realm was not found in the realm-config table |
| ERROR: ext-policy-server [id] has illegal protocol value [xyz]                   | Invalid protocol entry                        |

**Steering-Pool**

| Error Text                                                                              | Reason for Error                                                 |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------|
| ERROR: steering-pool [id] has invalid start-port [x]                                    | Invalid start-port value (smaller than 1025)                     |
| ERROR: steering-pool [id] has start-port [x] greater than end-port [y]                  | Start-port value is greater than end-port value                  |
| ERROR: steering-pool [id] is missing realm entry                                        | Missing realm entry                                              |
| ERROR: steering-pool [id] has reference to realm [xyz] which does not exist             | Realm [xyz] was not found in realm-config table                  |
| ERROR: steering-pool [id] has reference to network-interface [xyz] which does not exist | Network-interface [xyz] was not found in network-interface table |

**Surrogate-Agent**

| Error Text                                                                    | Reason for Error                              |
|-------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: surrogate-agent [id] is missing realm entry                            | Missing realm entry                           |
| ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist | Realm was not found in the realm-config table |
| ERROR: surrogate-agent [id] is missing customer-next-hop entry                | Missing customer-next-hop entry               |
| ERROR: surrogate-agent [id] is missing register-contact-user entry            | Missing register-contact-user entry           |
| ERROR: surrogate-agent [id] is missing register-contact-host entry            | Missing register-contact-host entry           |

**System-Config**

| Error Text                                                                       | Reason for Error                                                        |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| ERROR: system-config has reference to default-gateway [xyz] which does not exist | gateway was not found in the network-interface table or boot parameters |
| ERROR: system-config collect has sample-interval [x] greater than push-interval  | sample-interval greater than push-interval                              |

| Error Text                                                                                                      | Reason for Error                          |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ERROR: system-config collect has start-time [x] greater than end-time [y]                                       | Start-time greater than end-time          |
| ERROR: system-config collect has group [xyz] with sample-interval [x] greater than collection push-interval [y] | Group [xyz] has incorrect sample interval |
| ERROR: system-config collect has group [xyz] with start-time [x] greater than end-time [y]                      | Group [xyz] has incorrect sample interval |
| ERROR: system-config collect has no push-receivers defined                                                      | No push-receivers defined                 |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have user-name set             | No user-name set                          |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have password set              | No password set                           |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have address set               | No address set                            |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have data-store set            | No data-store set                         |

## TLS-Profile

| Error Text                                                                                                                       | Reason for Error                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates                       | End-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD |
| ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.     | Bad private key for the cert-record                                                                                             |
| ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist                                       | Certificate record was not found in cert-record table                                                                           |
| ERROR: tls-profile [id] has an end-entity-certificate records without any end entity certificate                                 | End certificate missing from all end-entity-certificate records or none of them where imported to the SD                        |
| ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length                                           | Found an empty trusted-ca-record in the list                                                                                    |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates                      | Trusted-ca-records entry missing certificate                                                                                    |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] with PKCS7 structure which does not have any certificates | Trusted-ca-records entry with PKCS7 structure missing certificate                                                               |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not exist                                      | Certificate record was not found in cert-record table                                                                           |
| ERROR: tls-profile [id] has no trusted-ca-certificates, but mutual-authentication is enabled                                     | No trusted certificates, but enabled mutual-authentication                                                                      |

The **regenerate-config** command rebuilds the configuration database information. This command is used to fix a corrupted system configuration when running Net-Net SBC software release 1.3.

1. At the superuser command prompt, enter the **regenerate-config** command.

```
ACMEPACKET# regenerate-config
Finish updating all of the configs.
task done
ACMEPACKET#
```

## Viewing Configurations

While configuration archives describe a full Net-Net SBC configuration, you can not display them on the screen for quick reference. To view configurations through a local connection, there are two options.

1. To display the current configuration on the screen, type **show configuration** at a command prompt. You can add a specific configuration element after the show configuration command to display only that element on the screen.

```
ACMEPACKET> show configuration host-route
host-routes
 dest-network 10.0.0.0
 netmask 255.255.0.0
 gateway 172.30.0.1
task done
ACMEPACKET>
```

2. To display the running configuration on the screen, type **show running-configuration** at a command prompt.

## Checking Configuration Versions

The Net-Net SBC maintains a running count of the version of both the running configuration and current configuration. It can be helpful to know when the running and current configurations are out of sync.

While they can differ, the current configuration and the running configuration should generally be the same. After a configuration is modified, saved and activated, the current and running configuration versions should be the same.

### To check the version of each configuration:

1. Type **display-current-cfg-version** at a command prompt to display the version number of the current configuration.

```
ACMEPACKET> display-current-cfg-version
Current configuration version is 3
ACMEPACKET>
```

2. Type **display-running-cfg-version** at a command prompt to display the version number of the running configuration.

```
ACMEPACKET> display-running-cfg-version
Running configuration version is 3
ACMEPACKET>
```

## Deleting Configurations

You can completely delete the data in the last-saved configuration with one command. This can be useful if you want to reconfigure your Net-Net SBC starting



with a blank configuration. You must reboot your Net-Net SBC after issuing the `delete-config` command to complete this task.

**To delete the running and current configuration:**

1. Type **delete-config** at a superuser command prompt. You will be prompted to confirm that you want to complete this task.

```
ACMEPACKET# del ete-confi g

Do you really want to ERASE the current confi g? [y/n]?: y
Del eting confi gurati on
NOTE: need to reboot for changes to take effect
task done
```

2. Reboot the Net-Net SBC using the **reboot** command.

## Configuration Checkpointing

In an HA configuration, configuration checkpointing copies all configuration activity and changes on one Net-Net SBC to the other Net-Net SBC. Checkpointed transactions copy added, deleted, or modified configurations from the active system to the standby system. You only need to perform configuration tasks on the active Net-Net SBC because the standby SD will go through the checkpointing process and synchronize its configuration to the active Net-Net SBC to reflect activity and changes.

The **acquire-config** command is used to manually invoke configuration checkpointing between two Net-Net SBCs in an HA node.

**To synchronize the systems in an HA node:**

1. On either the active or standby Net-Net SBC, type **acquire-config** <IP address of other SD in HA pair>.
  - The IPv4 address for the Net-Net SBC from which to acquire the configuration.
  - For **acquire-config** to work, one rear interface on each SD must be named `wancom1`, and one rear interface on each SD must be named `wancom2`.

```
ACMEPACKET# acqui re-confi g 10.0.1.8
```

2. Following the procedure defined directly above, confirm that the HA node now has synchronized configurations.

```
ACMEPACKET-1# di spl ay-current-cfg-versi on
Current confi gurati on versi on i s 30
ACMEPACKET-1# di spl ay-runni ng-cfg-versi on
Runni ng confi gurati on versi on i s 30
ACMEPACKET-2# di spl ay-current-cfg-versi on
Current confi gurati on versi on i s 30
ACMEPACKET-2# di spl ay-runni ng-cfg-versi on
Runni ng confi gurati on versi on i s 30
```

## Realm-Specific Delete Command

The ACLI provides a way to delete a specific realm and the configurations (objects) associated with that realm. You use the **delete realm-specifics** command with the name of the realm you want to delete. Not only does the Net-Net SBC delete that realm, it also deletes the configurations where that realm is also used as a primary or foreign key—such as steering pools, session agents, and SIP interfaces. A complete list of configurations subject to deletion appears below.

The Net-Net SBC safeguards against unintentionally deleting configurations by showing you a complete list of the configurations it is about to delete, warns you that you are about to delete the realm, and then asks you for confirmation. The list of candidates for deletion appears each with its key identifier so that you can more easily recognize it. You must type in a **y** for **yes** or **n** for **no** to move forward.

Despite these safeguards, you should use the **delete realm-specifics** command with the utmost care. Acme Packet recommends that only advanced Net-Net SBC users work with this command. In fact, the command appears in the configuration menu, to which only Superusers have access.

## Deleted Configurations

This section provides a list of the configuration that use the name of realm either as a primary or as a foreign key. These are the configuration that you can remove from your configuration when you delete a specific realm.

| ACLI Configuration Name | ACLI Parameter Value                                                   |
|-------------------------|------------------------------------------------------------------------|
| access-control          | realm-id                                                               |
| call-recording-server   | primary-realm<br>secondary-realm                                       |
| dns-config              | client-realm                                                           |
| enum-config             | realm-id                                                               |
| ext-policy-server       | realm                                                                  |
| h323>h323-stack         | realm-id                                                               |
| lawful-intercept        | (associated parameters; specified in Net-Net LI support documentation) |
| local-policy            | source-realm                                                           |
| mgcp-config             | private-realm<br>public-realm                                          |
| realm-config            | identifier                                                             |
| session-agent           | realm-id                                                               |
| sip-features            | realm                                                                  |
| sip-interface           | realm-id                                                               |
| sip-nat                 | realm-id                                                               |
| static-flow             | in-realm-id<br>out-realm-id                                            |
| steering-pool           | realm-id                                                               |
| surrogate-agent         | realm-id                                                               |

There are configurations (objects) that use realms but do not reference them directly either as a primary or foreign key. The Net-Net SBC does not delete these configurations when you use the **delete realm-specifics** command:

- media-policy
- class-policy

- translation-rules
- sip-manipulation

**Note:** This command cannot delete realms associated with network management control configurations.

## Deleted Parameter Values

For other configurations that reference realms, only the parameters containing realm identifiers are cleared while the object as a whole remains. When you confirm you want to delete the realm and doing so will clear the parameters set out in this section, the Net-Net SBC informs you of the configuration object and the parameter within it that will be affected.

The following table shows you which parameters are cleared.

| ACLI Configuration Name | ACLI Parameter Value(s)                     |
|-------------------------|---------------------------------------------|
| dns-config              | server-realm                                |
| local-policy            | source-realm<br>next-hop<br>realm           |
| media-manager           | home-realm-id                               |
| realm-config            | parent-realm<br>dns-realm<br>ext-policy-svr |
| realm-group             | source-realm<br>destination-realm           |
| session-agent           | egress-realm                                |
| session-group           | dest                                        |
| sip-config              | egress-realm-id<br>home-realm-id            |

## ACLI Instructions and Examples

This section shows you how to use the **delete realm-specifics** command. Remember that you need to be in Superuser mode to use it.

To use the **delete realm-specifics** command, you need to know the identifier for the realm (and the other configurations associated with the realm) that you want to delete.

These instructions and examples do not include information for parameters that will be emptied for configurations that will otherwise be left intact. This information will appear in the following form: `<attribute> <attribute value> removed from <object name/configuration name> with key <key value>`.

### To delete a specific realm and its associated configurations:

1. In Superuser mode, type **configure terminal** and press <Enter>.
 

```
ACMEPACKET# configure terminal
ACMEPACKET(config)#
```

2. Type `delete realm-specifics`, a <Space>, and the name of the realm you want deleted. The press <Enter>.

After you press <Enter>, the Net-Net SBC displays a list of all configurations on which the deletion will have an impact. It also warns you that you are about to delete the realm.

```
ACMEPACKET(configure)# delete realm-specifics peer_1
RealmConfig with key identifier=peer_1 will be deleted
SteeringPool with key ip-address=192.168.0.11 start-port=21000 realm-id=peer_1 will be deleted
SessionAgent with key hostname=127.0.0.11 will be deleted
SipInterface with key realm-id=peer_1 will be deleted
SipNatConfig with key realm-id=peer_1 will be deleted
```

WARNING: you are about to delete the realm!

Delete the realm? [y/n]?:

3. At the end of the display, the Net-Net SBC asks you to confirm (by typing a **y**) or abort (by typing an **n**) the deletion.

Delete the realm? [y/n]?: **y**

If you confirm the deletion, the Net-Net SBC will list all of the configurations that have been removed.

```
RealmConfig with key identifier=peer_1 deleted
SteeringPool with key ip-address=192.168.0.11 start-port=21000 realm-id=peer_1 deleted
SessionAgent with key hostname=127.0.0.11 deleted
SipInterface with key realm-id=peer_1 deleted
SipNatConfig with key realm-id=peer_1 deleted
ACMEPACKET(configure)#
```

When you abort the deletion, the Net-Net SBC will return you to the ACMEPACKET(configure)# system prompt.

## System Prompt Indicator

Using the **prompt-enabled** command, you can enable a system prompt indicator to show you when a configuration requires saving and activation.

The Net-Net SBC lets you know if a configuration has been changed and you have applied the `done` command, but have not saved and activated yet. When you issue the `done` command and return to Superuser mode, the ACLI prompt prefixes two asterisks (\*\*). When you have saved but not yet activated, the ACLI prompted prefixes one asterisk (\*). This command allows you to decide whether or not you want the Net-Net SBC to give this prompt. To clarify:

- \*\*—Requires save and activate
- \*—Configuration saved, but requires activate

This feature is disabled by default.

## Introduction

---

The Net-Net SBC can concatenate the full system configuration into a single backup file and also archive log files. You can perform a set of actions on backup files or archived log files, such as saving, backing up, listing, and deleting the files.

To save disk space, the Net-Net SBC has archiving features that use the standard tar and gzip utilities. Archiving lets you easily change, move, store, and back up the Net-Net system's log files. After a log file has been archived, it can be transferred via FTP to a remote host. The Net-Net SBC has a set of file manipulation commands that you can apply only to archive files.

Using the **backup** command enables you to successfully save and restore an existing configuration. The major difference between backup and archive files is that backup commands are used for configurations and log archive commands are used with log files.

## Backup Commands

---

The Net-Net SBC includes a set of commands for easily working with backup configurations. These commands are **backup-config**, **display-backups**, **delete-backup-config**, **restore-backup-config**.

Acme Packet suggests that you back up properly functioning configurations on your Net-Net system before making any new major configuration changes. The backup configurations are crucial to have when configuration changes do not function as anticipated and a rollback must be applied immediately.

To back up the Net-Net system configuration, use the **backup-config** command. You can confirm your backup has been created with the **display-backups** command. When the **backup-config** command is executed, the Net-Net system checks if sufficient resources exist to complete the operation. If resources are sufficient, the Net-Net system creates the backup. If resources are insufficient, the task is not completed and the Net-Net SBC instead displays the limiting resources, recommending that the task be completed at another time.

Backups are created as gzipped files in a .gz format. They are stored in the /code/bkups directory on the Net-Net SBC.

## Creating Backups

### To create a backup :

1. In the ACLI at the superuser prompt, enter the **backup-config <filename> [editing | running]** command. Enter **backup-config** followed by a descriptive filename for the backup you are creating. You can also enter an optional argument to specify whether you want to create a backup from the editing configuration cache or the running configuration cache.

```
ACMEPACKET# backup-confi g 01_Feb_2005_Test runni ng
```

```
task done
ACMEPACKET#
```

## Listing Backups

**To list available backup configurations:**

1. In the ACLI at the superuser prompt, enter the **display-backups** command. A list of available backup files from the `/code/bkups` directory is displayed on the screen.

```
ACMEPACKET# display-backups
test_conf1 g. gz
test-conf1 g. gz
runni ngcfgtest. gz
runni ngtest_one. gz
BACK_UP_CONF1 G. gz
02_Feb_2005. gz
01_Feb_2005_Test. gz
ACMEPACKET#
```

## Restoring Backups

**To restore a backup configuration:**

1. In the ACLI at the superuser prompt, enter the **restore-backup-config <filename> [running | saved]** command. Enter **restore-backup-config** followed by the backup filename you wish to restore to the current configuration. You must explicitly name the backup file you wish to restore, including the file extension. You can also enter an optional argument to specify whether you want to restore the last running configuration or the last saved configuration on the Net-Net SBC.

```
ACMEPACKET# restore-backup-conf1 g backup_f1 l e. gz saved
Need to perform save-config and activate/reboot activate for changes
to take effect...
task done
ACMEPACKET#
```

You can restore files from either `.tar.gz` format or just `.gz`. All backup files are gzipped in the `.gz` format.

You must still save and activate the configuration or reboot the Net-Net SBC to apply the backup configuration.

## Deleting Backups

The **delete-backup-config** command deletes the backup configurations from the `/code/bkups` directory on your Net-Net system.

1. In the ACLI at the superuser prompt, enter the **delete-backup-config** command, followed by the backup file you wish to delete.

```
ACMEPACKET# delete-backup-conf1 g FEB_BACKUP. gz
task done
ACMEPACKET#
```

## Viewing Backup Configurations

The **show backup-config** command displays a specified configuration file saved on the Net-Net SBC's standard backup file directory.

1. In the ACLI at the superuser prompt, enter the `show backup-config` command followed by the backup configuration filename you want to view.

```
ACMEPACKET# show backup-config
```

The configuration of the backup file you specify is displayed on the screen. The contents of this output are in the same format as the **show configuration** command. For example:

```
ACMEPACKET# show backup-config
```

```
Possible configuration files are:
```

```
0606_HMRSPNAT_Overlay.gz
```

```
0606_HMRSPPeeri ng.gz
```

```
0605_Si ngI eSI PNATH_i n_access.gz
```

```
0605_Si ngI eSI PNATHTN_ABBN.gz
```

```
0605_SNB_ABBN.gz
```

```
HMR_OAI _config.gz
```

```
0619_HMR_OAI .gz
```

## Archive Commands

---

### Creating Archives

You can create archives of log files. Creating log archives requires a unique procedure described below.

### File Locations

The following table lists source and destination directories used with archive functions.

| Configuration Type | Source Directory | Destination Directory |
|--------------------|------------------|-----------------------|
| Log                | /ramdrv/logs     | /code/logs            |

### Log File Archives

To create an archive that contains all log files on the Net-Net SBC:

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ACMEPACKET# archives
```

```
ACMEPACKET(archives)#
```

2. Type **create LOGS**, followed by a name for the archive file. The Net-Net SBC will pause while it completes the task and alert you when the task has completed.

```
ACMEPACKET(archives)# create LOGS AI I_Logs_27_Feb
```

```
task done
```

```
ACMEPACKET(archives)#
```

### Listing Archives

**To display a list of the archived log files:**

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ACMEPACKET# archives
```

```
ACMEPACKET(archives)#
```

2. Type **display LOGS** to view the available log files.

```
ACMEPACKET(archives)# display LOGS
testlogs1.tar
log.algdd.tar
bluff1.tar
log.mbcd.tar
log.lcmd.tar
log.sipd.tar.gz
log.NOTTESTING.sipd.tar
sipd.log.tar.gz
ACMEPACKET(archives)#
```

## Deleting Archives

**To delete archived log files:**

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ACMEPACKET# archives
ACMEPACKET(archives)#
```

2. Type **delete LOGS**, followed by the filename of the log file to delete.

```
ACMEPACKET(archives)# delete LOGS sipd.log
Archive '/code/logs/sipd.log.tar.gz' deleted.
task done
ACMEPACKET(archives)#
```

## Renaming Archives

**To rename archived log files:**

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ACMEPACKET# archives
ACMEPACKET(archives)#
```

2. Type **rename LOGS**, followed by the filename of the old log file, then the new filename, and then the destination name to which to save the renamed archive.

```
ACMEPACKET(archives)# rename LOGS log.sipd.tar.gz /code/logs
renamed.log.sipd.tar.gz
moving file /code/logs/log.sipd.tar.gz ->
/code/logs/renamed.log.sipd.tar.gz
ACMEPACKET(archives)#
```

The newly renamed file remains in the same directory.

## Viewing Free Space

The **check-space-remaining** command checks the free space in the boot directory, code (flash memory), and ramdrv (on-board volatile memory) devices. This command displays the total number of bytes free and total number of bytes available on the specified device. Each volume is used in the following way:

- **/boot**—A flash memory partition used primarily for system boot images and the bootloader image.
- **/code**—A flash memory partition used to store archives and data that needs to be persistent across reboot.
- **/ramdrv**—A volume used mostly for temporary configurations and log files.



1. In the ACLI at the superuser prompt, enter the **check-space-remaining** command followed by the device you want to check the space on. Valid devices are **boot**, **code**, **ramdrv**. All examples of this command are shown below.

```
ACMEPACKET# check-space-remaining boot
```

```
boot: 29759488/29760512 bytes (99%) remaining
```

```
ACMEPACKET# check-space-remaining code
```

```
code: 26650624/29760512 bytes (89%) remaining
```

```
ACMEPACKET# check-space-remaining ramdrv
```

```
ramdrv: 131604992/132104192 bytes (99%) remaining
```

```
ACMEPACKET#
```



# Appendix A

## Configuration Verification Error and Warning Messages

The following tables list every error and warning message the Net-Net SBC may produce when the **verify-config** command is executed:

### Access-Control

| Error Text                                                                      | Reason for Error                   |
|---------------------------------------------------------------------------------|------------------------------------|
| WARNING: access-control [id] has unsupported application-protocol [x]           | Unsupported protocols [x]          |
| ERROR: access-control [id] has reference to realm-id [xyz] which does not exist | Realm was not found in realm table |

### Account-Config

| Error Text                                                                                                                  | Reason for Error                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| ERROR: account-config is enabled, but there are no account servers configured                                               | State is enabled, file-output is disabled and there are not servers                       |
| WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled                       | State and file-output are enabled, there are not account servers and ftp-push is disabled |
| WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled        | State and ftp-push are enabled, account servers are configured, file-output is disabled   |
| ERROR : account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured     | State and ftp-push are enabled, but there is no ftp-address or push-receiver configured   |
| ERROR: account-config has reference to push-receiver [xyz] which can not get password                                       | Password failed decryption                                                                |
| ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set                              | Push-receiver has no remote-path set                                                      |
| ERROR: account-config has reference to push-receiver [xyz] which does not have username set                                 | Push-receiver has no username set                                                         |
| ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP                | Push-receiver has no password set for FTP                                                 |
| WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP              | Push-receiver has set public key, but protocol is FTP                                     |
| ERROR: account-config has reference to push-receiver [xyz] which does not have password or public key set for protocol SFTP | Push-receiver has no password or public key set for SFTP                                  |

| Error Text                                                                                            | Reason for Error                                |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| ERROR: account-config has push-receiver [xyz] with reference to public-key [zyx] which does not exist | Public key was not found in public key table    |
| ERROR: account-config has account-server [IP:Port] with empty secret                                  | Account-server [IP:Port] has empty secret field |

## Authentication

| Error Text                                                                                | Reason for Error                           |
|-------------------------------------------------------------------------------------------|--------------------------------------------|
| ERROR: authentication has specified unsupported protocol [x] for type [y]                 | Unsupported protocols for given type       |
| ERROR: authentication has no configured active radius servers for authentication type [x] | No configured active radius for given type |

## Call-Recording-Server

| Error Text                                                                                        | Reason for Error                                          |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ERROR: call-recording-server must have a name                                                     | Name is missing                                           |
| ERROR: call-recording-server [id] must have a primary-signaling-addr or primary-media-addr        | There has to be either primary signaling or media address |
| ERROR: call-recording-server [id] is missing primary-realm                                        | Realm name is missing                                     |
| ERROR: call-recording-server [id] has reference to the primary-realm [xyz] which does not exist   | Primary-realm [xyz] was not found in realm-config table   |
| ERROR: call-recording-server [id] has reference to the secondary-realm [xyz] which does not exist | Secondary-realm [xyz] was not found in realm-config table |

## Capture-Receiver

| Error Text                                                                                 | Reason for Error                                           |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist | Network-interface was not found in network-interface table |

## Certificate-Record

| Error Text                                                              | Reason for Error                                     |
|-------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: certificate-record [id] is not trusted and will not be loaded    | Certificate record is not trusted                    |
| ERROR: certificate-record [id] cannot extract private key               | Certificate record failed to extract the private key |
| ERROR: certificate-record [id] cannot convert PKCS7 string to structure | Failure to convert PKCS7 record to the structure     |

## Class-Policy

| Error Text                                                                            | Reason for Error                                           |
|---------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: class-policy [id] has reference to the media-policy [xyz] which does not exist | Media-policy [xyz] was not found in the media-policy table |

## DNS-Config

| Error Text                                                                      | Reason for Error                                     |
|---------------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: dns-config [id] is missing client-realm entry                            | Missing client realm                                 |
| ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist | Realm was not found in the realm-config table        |
| ERROR: dns-config [id] does not have any server-dns-attributes                  | Server-dns-attributes are missing                    |
| ERROR: dns-config [id] is missing server-realm entry                            | Realm entry is missing (source address is empty)     |
| ERROR: dns-config [id] is missing server-realm entry for source-address [x]     | Realm entry is missing (source address is not empty) |
| ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist | Realm was not found in the realm-config table        |

## ENUM-Config

| Error Text                                                                       | Reason for Error                                |
|----------------------------------------------------------------------------------|-------------------------------------------------|
| ERROR: enum-config [id] is missing realm-id entry                                | Missing realm                                   |
| ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist | Realm [xyz] was not found in realm-config table |
| ERROR: enum-config [id] has no enum-servers                                      | List of ENUM servers is empty                   |

## Ext-Policy-Server

| Error Text                                                                       | Reason for Error                              |
|----------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: ext-policy-server [id] is missing realm entry                             | Missing realm                                 |
| ERROR: ext-policy-server [id] address is not valid                               | Invalid address entry                         |
| ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid | Invalid protocol entry                        |
| ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist  | Realm was not found in the realm-config table |

**H323-Stack**

| Error Text                                                                          | Reason for Error                                   |
|-------------------------------------------------------------------------------------|----------------------------------------------------|
| ERROR: h323-stack [id] has no realm-id                                              | Missing realm entry                                |
| ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist     | Realm was not found in the realm-config table      |
| WARNING: h323-stack [id] is missing local-ip address entry                          | Missing address entry                              |
| WARNING : h323-stack [id] has reference to media-profile [xyz] which does not exist | Media profile was not found in media profile table |
| ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist  | Stack name was not found in the h323-stack table   |

**Host-Route**

| Error Text                                                                                            | Reason for Error                                            |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| WARNING: host-route [id] has reference to gateway [xyz] which does not exist in any network-interface | gateway entry was not found in any network-interface object |

**IWF-Config**

| Error Text                                                                    | Reason for Error                                   |
|-------------------------------------------------------------------------------|----------------------------------------------------|
| WARNING: iwf-config has reference to media-profile [xyz] which does not exist | media profile was not found in media profile table |

**Local-Policy**

| Error Text                                                                                                           | Reason for Error                                                                                |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist                                    | Source-realm [xyz] was not found in realm-config table                                          |
| WARNING: local-policy [id] has no policy-attributes set                                                              | No policy-attributes set                                                                        |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist        | Realm [xyz] was not found in realm-config table                                                 |
| ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry                                | Next-hop is missing for given attribute                                                         |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid         | Invalid value for the next-hop                                                                  |
| ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist     | Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group) |
| WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist | Media-policy [xyz] was not found in media-policy table                                          |

## Local-Routing-Config

| Error Text                                                                                 | Reason for Error                                     |
|--------------------------------------------------------------------------------------------|------------------------------------------------------|
| ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist | specified file is missing from /boot/code/lrt folder |

## MGCP-Config

| Error Text                                                                                                     | Reason for Error                                               |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ERROR: mgcp-config [id] is missing private-realm entry                                                         | Private-realm empty                                            |
| ERROR: mgcp-config [id] has reference to private-realm [xyz] which does not exist                              | Realm was not found in realm-config table                      |
| ERROR: mgcp-config [id] is missing public-realm entry                                                          | Public-realm empty                                             |
| ERROR: mgcp-config [id] has reference to public-realm [xyz] which does not exist                               | Realm was not found in the realm-config table                  |
| ERROR: mgcp-config [id] has identical private-address and public-gw-address [x] for the same network interface | Private-address and public-gw-address are identical on same NI |

## Network-Interface

| Error Text                                                                              | Reason for Error                                                                                       |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist | Phy-interface [xyz] was not found in phy-interface table                                               |
| ERROR: network-interface [id] is missing pri-utility-addr entry                         | If redundancy is enabled pri-utility-addr entry has to be entered                                      |
| ERROR: network-interface [id] is missing sec-utility-addr entry                         | If redundancy is enabled sec-utility-addr entry has to be entered                                      |
| ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty     | Dns-domain is empty. Word "address" will be plural "addresses" if there are more DNS addresses entered |
| ERROR: network-interface [id] has reference to DNS address, but ip-address is empty     | Ip-address is empty. Word "address" will be plural "addresses" if there are more DNS addresses entered |

## Phy-Interface

| Error Text                                                                                                | Reason for Error                                                                  |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| ERROR: phy-interface [id] has invalid operation-type value [x]                                            | Operation-type value is invalid                                                   |
| ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name                         | If type is MAINTENANCE or CONTROL name has to start with either "eth" or "wancom" |
| ERROR: phy-interface [id] of type [x] has duplicated port [y] and slot [z] values with phy-interface [di] | Port and slot values are duplicated with another phy-interface                    |

## Public-Key

| Error Text                                                                         | Reason for Error                |
|------------------------------------------------------------------------------------|---------------------------------|
| ERROR: public-key [id] has no public/private key pair generated for public-key [x] | No public/private key generated |
| ERROR: public-key [id] cannot extract private key                                  | Cannot extract private key      |

## Realm-Config

| Error Text                                                                                    | Reason for Error                                                                               |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which does not exist           | Missing external BW manager                                                                    |
| ERROR: realm-config [id] is missing entry for network-interface                               | Missing Network Interface                                                                      |
| ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist        | Network interface was not found in network-interface table                                     |
| ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist             | Media-policy was not found in media-policy table                                               |
| ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist            | Class-profile was not found in class-profile table                                             |
| ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist         | In-translationid was not found in session translation table                                    |
| ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist        | Out-translationid was not found in session translation table                                   |
| ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist        | In-manipulationid was not found in manipulation table                                          |
| ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist       | Out-manipulationid was not found in manipulation table                                         |
| ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist      | Enforcement-profile was not found in enforcement-profile table                                 |
| ERROR: realm-config [id] has reference to call-recording-server-id [xyz] which does not exist | Call-recording-server-id was not found in call-recording-server-table                          |
| ERROR: realm-config [id] has reference to codec-policy [xyz] which does not exist             | Codec-policy was not found in codec-policy table                                               |
| ERROR: realm-config [id] has reference to constraint-name [xyz] which does not exist          | Constraint-name was not found in session constraint table                                      |
| ERROR: realm-config [id] has reference to qos-constraint [xyz] which does not exist           | Qos-constraint was not found in qos constraint table                                           |
| ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms           | Realm and its parent realm are part of the closed loop where they referring back to themselves |
| ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist                | Dns-realm doesn't exist in the realm table                                                     |
| WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)   | Realm name and parent name are the same                                                        |



| Error Text                                                                        | Reason for Error                                                         |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| ERROR: realm-config [id] has reference to parent-realm [xyz] which does not exist | Parent realm doesn't exist in the realm table                            |
| ERROR: realm-config [id] has identical stun-server-port and stun-changed port [x] | Stun-server-ip is identical to stun-changed-ip, when stun is enabled     |
| ERROR: realm-config [id] has identical stun-server-ip and stun-changed-ip [x]     | Stun-server-port is identical to stun-changed-port, when stun is enabled |

## Realm-Group

|                                                                                       |                                           |
|---------------------------------------------------------------------------------------|-------------------------------------------|
| ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist      | Realm was not found in realm-config table |
| ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist | Realm was not found in realm-config table |

## Redundancy

| Error Text                                                                                                                 | Reason for Error                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr from network-interface [y]        | If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface (pri-utility-addr is missing here)   |
| ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr [z] from network-interface [y]    | If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface                                      |
| ERROR: redundancy-config peer [id] has Address [x] which does not match sec-utility-addr from network-interface [y]        | If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface (sec-utility-addr is missing here) |
| ERROR: redundancy-config peer [id] has IP Address [x] which does not match sec-utility-addr [z] from network-interface [y] | If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface                                    |
| ERROR: redundancy-config peer [id] has reference to network-interface [xyz] which does not exist                           | Network-interface [xyz] was not found in network-interface table                                                                                          |
| ERROR: redundancy-config peer [id] is missing destination object                                                           | Destination object is missing                                                                                                                             |
| ERROR: redundancy-config is missing Primary peer object                                                                    | Primary peer object is missing                                                                                                                            |
| ERROR: redundancy-config is missing Secondary peer object                                                                  | Secondary peer object is missing                                                                                                                          |
| ERROR: redundancy-config is missing both Primary and Secondary peer objects                                                | Primary and Secondary peer objects are missing                                                                                                            |

## Security-Association

| Error Text                                                                                                                                                           | Reason for Error                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: security-association [id] is missing network-interface entry                                                                                                  | Missing network-interface entry                            |
| ERROR: security-association [id] has reference to network-interface [xyz] which does not exist                                                                       | Network-interface was not found in network-interface table |
| ERROR: security-association [id] has invalid local-ip-addr                                                                                                           | Invalid local-ip-addr entry                                |
| ERROR: security-association [id] has invalid remote-ip-addr                                                                                                          | Invalid remote-ip-addr entry                               |
| ERROR: security-association [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface                                           | Network-interface is not valid IPSEC media interface       |
| ERROR: security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password | Failed to decrypt auth-key                                 |
| ERROR: security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long                                         | Invalid length of the auth-key for auth-algo [hmac-md5]    |
| ERROR: security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long                                        | Invalid length of the auth-key for auth-algo [hmac-sha1]   |
| ERROR: security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password | Failed to decrypt encr-key                                 |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 64 bits (odd parity in hex)                                        | Invalid encr-key length for given algorithm                |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 192 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm                |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 128 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm                |
| ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 256 bits (odd parity in hex)                                       | Invalid encr-key length for given algorithm                |
| ERROR: security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]                                                              | Has invalid aes-ctr-nonce for given algorithm              |
| ERROR: security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)                                                       | Invalid tunnel-mode local-ip-addr                          |
| ERROR: security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)                                                     | Invalid tunnel-mode remote-ip-addr                         |
| ERROR: security-association [id] has invalid espudp local-ip-addr (must be non-zero)                                                                                 | Invalid espudp local-ip-addr                               |
| ERROR: security-association [id] has invalid espudp remote-ip-addr (must be non-zero)                                                                                | Invalid espudp remote-ip-addr                              |

| Error Text                                                                         | Reason for Error           |
|------------------------------------------------------------------------------------|----------------------------|
| ERROR: security-association [id] has invalid espudp local-port (must be non-zero)  | Invalid espudp local-port  |
| ERROR: security-association [id] has invalid espudp remote-port (must be non-zero) | Invalid espudp remote-port |

## Security-Policy

| Error Text                                                                                                            | Reason for Error                                           |
|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| ERROR: security-policy [id] has invalid local-ip-addr-match                                                           | Empty local-ip-addr-match                                  |
| ERROR: security-policy [id] has invalid local-ip-addr-match [x]                                                       | Invalid local-ip-addr-match                                |
| ERROR: security-policy [id] has invalid remote-ip-addr-match                                                          | Empty remote-ip-addr-match                                 |
| ERROR: security-policy [id] has invalid remote-ip-addr-match [x]                                                      | Invalid remote-ip-addr-match                               |
| ERROR: security-policy [id] is missing network-interface entry                                                        | Missing network-interface entry                            |
| ERROR: security-policy [id] priority [x] is identical to security-policy [id2]                                        | Duplication of the priorities                              |
| ERROR: security-policy [id] has reference to network-interface [xyz] which does not exist                             | Network-interface was not found in network-interface table |
| ERROR: security-policy [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface | Network-interface is not valid IPSEC media interface       |

## Session-Agent

| Error Text                                                                                | Reason for Error                                               |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist            | Realm was not found in realm table                             |
| ERROR: session-agent [id] has reference to egress-realm-id [xyz] which does not exist     | Realm was not found in realm table                             |
| ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist    | Translation id was not found in translation table              |
| ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist   | Translation id was not found in translation table              |
| ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist   | Manipulation id was not found in manipulation table            |
| ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist  | Manipulation id was not found in manipulation table            |
| ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist | Enforcement-profile was not found in enforcement-profile table |
| ERROR: session-agent [id] has reference to code-policy [xyz] which does not exist         | Codec-policy was not found in codec-policy table               |

| Error Text                                                                               | Reason for Error                                 |
|------------------------------------------------------------------------------------------|--------------------------------------------------|
| ERROR: session-agent [id] has reference to response-map [xyz] which does not exist       | Response-map was not found in response map table |
| ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist | Response-map was not found in response map table |

## Session-Group

| Error Text                                                                          | Reason for Error                                       |
|-------------------------------------------------------------------------------------|--------------------------------------------------------|
| ERROR: session-group [id] has reference to session-agent [xyz] which does not exist | Session agent was not found in the session agent table |

## Session-Translation

| Error Text                                                                                 | Reason for Error                                             |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ERROR: session-translation [id] has reference to rules-called [xyz] which does not exist   | Translation rule was not found in the translation rule table |
| ERROR: session-translations [id] has reference to rules-calling [xyz] which does not exist | Translation rule was not found in the translation rule table |

## SIP-Config

| Error Text                                                                                 | Reason for Error                                                                                       |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| ERROR: sip-config has reference to home-realm-id [xyz] which does not exist                | Realm was not found in the realm-config table                                                          |
| ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist              | Realm was not found in the realm-config table                                                          |
| ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist          | Enforcement profile was not found in enforcement profile table                                         |
| WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [sip-internal-realm] | Missing home-realm-id, defaulted to sip-internal-realm                                                 |
| WARNING: sip-config home-realm-id [xyz] does not have a sip-interface                      | Sip-interface missing for the home realm                                                               |
| WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects   | Nat-mode needs to be set to either Public or Private if there are sip-nat objects in the configuration |
| ERROR: sip-config object is disabled                                                       | Sip-config is disabled, but there are configured sip-interface objects                                 |

## SIP-Interface

| Error Text                                                                                                | Reason for Error                                                                                    |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ERROR: sip-interface [id] is missing realm-id entry                                                       | missing realm                                                                                       |
| ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist                            | realm was not found in realm-config table                                                           |
| ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist                   | in-manipulationid was not found in manipulation table                                               |
| ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist                  | out-manipulationid was not found in manipulation table                                              |
| ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist                 | enforcement profile was not found in enforcement profile table                                      |
| ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist                        | response-map was not found in response-map table                                                    |
| ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist                  | local-response-map was not found in response-map table                                              |
| ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist                     | constraint-name was not found in session constraint table                                           |
| ERROR: sip-interface [id] has no sip-ports                                                                | sip-ports are missing                                                                               |
| ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist     | tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)               |
| ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist | ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS) |
| WARNING: sip-interface [id] has no sip-ports, using SIP-NAT external-address                              | no sip-ports so SIP-NAT external-address is used                                                    |
| WARNING: sip-interface [id] has no valid sip-ports, using SIP-NAT external-address                        | no valid sip-ports so SIP-NAT external-address is used                                              |

## SIP-Manipulation

| Error Text                                                                                                         | Reason for Error                                                   |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| ERROR: sip-manipulation [id] has no header-rules defined                                                           | Missing header rules                                               |
| ERROR: sip-manipulation [id] with header-rule [xyz] is missing new-value entry                                     | Missing new-value entry (checked only for action type "sip-manip") |
| ERROR: sip-manipulation [id] with header-rule [xyz] has reference to new-value [zxy] which does not exist          | New-value entry missing from the sip-manipulation table            |
| ERROR: sip-manipulation [id] with header-rule [xyz] has new-value that refers to itself from sip-manipulation [di] | Looping reference between two objects                              |

## SIP-NAT

| Error Text                                                                                                | Reason for Error                                             |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| ERROR: sip-nat [id] is missing home-address entry                                                         | Missing home-address                                         |
| ERROR: sip-nat [id] has invalid home-address [x] entry                                                    | Invalid home-address entry                                   |
| ERROR: sip-nat [id] is missing ext-address entry                                                          | Missing ext-address                                          |
| ERROR: sip-nat [id] has invalid ext-address [x] entry                                                     | Invalid ext-address entry                                    |
| ERROR: sip-nat [id] is missing ext-proxy-address entry                                                    | Missing ext-proxy-address                                    |
| ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry                                               | Invalid ext-proxy-address entry                              |
| ERROR: sip-nat [id] is missing user-nat-tag entry                                                         | Missing user-nat-tag                                         |
| ERROR: sip-nat [id] is missing host-nat-tag entry                                                         | Missing host-nat-tag                                         |
| ERROR: sip-nat [id] is missing domain-suffix entry                                                        | Missing domain-suffix                                        |
| ERROR: sip-nat [id] is missing realm-id entry                                                             | Missing realm entry                                          |
| ERROR: sip-nat [id] does not match sip-interface realm [xyz]                                              | Sip-interface name was not found in realm table              |
| ERROR: sip-nat [id] does not have a sip-interface                                                         | Sip-interface is missing                                     |
| WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]                                               | Duplicated user-nat-tag                                      |
| WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]                                               | Duplicated host-nat-tag                                      |
| WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y] | Sip-nat ext-address needs to be the same as sip-port address |
| ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]                                             | Duplicated home-address                                      |

## Static-Flow

| Error Text                                                                       | Reason for Error                              |
|----------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: static-flow [id] is missing in-realm-id entry                             | Missing in-realm-id                           |
| ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist  | Realm was not found in the realm-config table |
| ERROR: static-flow [id] is missing out-realm-id entry                            | Missing out-realm-id                          |
| ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist | Realm was not found in the realm-config table |
| ERROR: ext-policy-server [id] has illegal protocol value [xyz]                   | Invalid protocol entry                        |

## Steering-Pool

| Error Text                                                             | Reason for Error                                |
|------------------------------------------------------------------------|-------------------------------------------------|
| ERROR: steering-pool [id] has invalid start-port [x]                   | Invalid start-port value (smaller than 1025)    |
| ERROR: steering-pool [id] has start-port [x] greater than end-port [y] | Start-port value is greater than end-port value |

| Error Text                                                                              | Reason for Error                                                 |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------|
| ERROR: steering-pool [id] is missing realm entry                                        | Missing realm entry                                              |
| ERROR: steering-pool [id] has reference to realm [xyz] which does not exist             | Realm [xyz] was not found in realm-config table                  |
| ERROR: steering-pool [id] has reference to network-interface [xyz] which does not exist | Network-interface [xyz] was not found in network-interface table |

## Surrogate-Agent

| Error Text                                                                    | Reason for Error                              |
|-------------------------------------------------------------------------------|-----------------------------------------------|
| ERROR: surrogate-agent [id] is missing realm entry                            | Missing realm entry                           |
| ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist | Realm was not found in the realm-config table |
| ERROR: surrogate-agent [id] is missing customer-next-hop entry                | Missing customer-next-hop entry               |
| ERROR: surrogate-agent [id] is missing register-contact-user entry            | Missing register-contact-user entry           |
| ERROR: surrogate-agent [id] is missing register-contact-host entry            | Missing register-contact-host entry           |

## System-Config

| Error Text                                                                                                      | Reason for Error                                                        |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| ERROR: system-config has reference to default-gateway [xyz] which does not exist                                | gateway was not found in the network-interface table or boot parameters |
| ERROR: system-config collect has sample-interval [x] greater than push-interval                                 | sample-interval greater than push-interval                              |
| ERROR: system-config collect has start-time [x] greater than end-time [y]                                       | Start-time greater than end-time                                        |
| ERROR: system-config collect has group [xyz] with sample-interval [x] greater than collection push-interval [y] | Group [xyz] has incorrect sample interval                               |
| ERROR: system-config collect has group [xyz] with start-time [x] greater than end-time [y]                      | Group [xyz] has incorrect sample interval                               |
| ERROR: system-config collect has no push-receivers defined                                                      | No push-receivers defined                                               |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have user-name set             | No user-name set                                                        |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have password set              | No password set                                                         |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have address set               | No address set                                                          |
| ERROR: system-config collect has reference to push-receiver [xyz] which does not have data-store set            | No data-store set                                                       |

**TLS-Profile**

| Error Text                                                                                                                       | Reason for Error                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates                       | End-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD |
| ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.     | Bad private key for the cert-record                                                                                             |
| ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist                                       | Certificate record was not found in cert-record table                                                                           |
| ERROR: tls-profile [id] has an end-entity-certificate records without any end entity certificate                                 | End certificate missing from all end-entity-certificate records or none of them where imported to the SD                        |
| ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length                                           | Found an empty trusted-ca-record in the list                                                                                    |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates                      | Trusted-ca-records entry missing certificate                                                                                    |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] with PKCS7 structure which does not have any certificates | Trusted-ca-records entry with PKCS7 structure missing certificate                                                               |
| ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not exist                                      | Certificate record was not found in cert-record table                                                                           |
| ERROR: tls-profile [id] has no trusted-ca-certificates, but mutual-authentication is enabled                                     | No trusted certificates, but enabled mutual-authentication                                                                      |