About this Guide

Introduction

The Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide provides the information you need for understanding and troubleshooting the operation of the SBC.

Supported Platforms

Release Version S-C6.2.0 is supported on the Acme Packet 4500 and Acme Packet 3800 series platforms.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acme Packet 4500 System Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 4500 system.</td>
</tr>
<tr>
<td>Acme Packet 3800 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 3800 system.</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Contains information about the current documentation set release, including new features and management changes.</td>
</tr>
<tr>
<td>ACLI Configuration Guide</td>
<td>Contains information about the administration and software configuration SBC.</td>
</tr>
<tr>
<td>ACLI Reference Guide</td>
<td>Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.</td>
</tr>
<tr>
<td>Maintenance and Troubleshooting Guide</td>
<td>Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.</td>
</tr>
</tbody>
</table>
### Revision History

This section contains a revision history for this document.

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 30, 2009</td>
<td>Rev. 0.00</td>
<td>Initial release</td>
</tr>
<tr>
<td>June 29, 2012</td>
<td>Rev. 1.00</td>
<td>Revises definition for “Recent” in Viewing SIP Performance Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in the Performance Management chapter</td>
</tr>
<tr>
<td>December 17, 2012</td>
<td>Rev 1.10</td>
<td>Corrects assorted typos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrects maximum ftp/ssh sessions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clarifies the need to save configs during HA upgrades from release versions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>prior to C6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrects verify-config error text when steering pool port start port is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>less than 1025</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adds conditions under which arp-check command does not issue request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removes extraneous reboot from 4500 HA upgrade procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adds virtual MAC address re-calculation procedure to 4250 - 4500 HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Upgrade procedure</td>
</tr>
<tr>
<td>January x, 2013</td>
<td>Rev 1.11</td>
<td>Corrects alarm ID range for gateway unreachable alarm</td>
</tr>
<tr>
<td>May 17, 2013</td>
<td>Rev 1.12</td>
<td>Added additional log file descriptions to the section, “Log Files”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in the Logs chapter</td>
</tr>
<tr>
<td>July 25, 2013</td>
<td>Rev 1.13</td>
<td>In Chapter 4, replaced the “Setting Timezone” section with the new</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information about timezones. Also replaced the “Displaying the System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timezone” section</td>
</tr>
<tr>
<td>October 2014</td>
<td>Rev 1.14</td>
<td>Corrected show power-supply output</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this Guide</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</td>
<td>iii</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>iii</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>iii</td>
</tr>
<tr>
<td>Revision History</td>
<td>iv</td>
</tr>
<tr>
<td><strong>1 Logs</strong></td>
<td>27</td>
</tr>
<tr>
<td>Introduction</td>
<td>27</td>
</tr>
<tr>
<td>About Logs</td>
<td>27</td>
</tr>
<tr>
<td>Logging Events</td>
<td>27</td>
</tr>
<tr>
<td>Event Categories</td>
<td>28</td>
</tr>
<tr>
<td>About Events</td>
<td>28</td>
</tr>
<tr>
<td>Types of Events</td>
<td>28</td>
</tr>
<tr>
<td>Process Log Events</td>
<td>28</td>
</tr>
<tr>
<td>System Log Events</td>
<td>29</td>
</tr>
<tr>
<td>Protocol Trace Events</td>
<td>29</td>
</tr>
<tr>
<td>Event Granularity</td>
<td>29</td>
</tr>
<tr>
<td>Event Severity</td>
<td>30</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>30</td>
</tr>
<tr>
<td>Alarms</td>
<td>30</td>
</tr>
<tr>
<td>Process Log Events</td>
<td>31</td>
</tr>
<tr>
<td>System Log Events</td>
<td>31</td>
</tr>
<tr>
<td>Traps</td>
<td>31</td>
</tr>
<tr>
<td>Alarms</td>
<td>31</td>
</tr>
<tr>
<td><strong>Working with Logs</strong></td>
<td>32</td>
</tr>
<tr>
<td>Writing to Logs</td>
<td>32</td>
</tr>
<tr>
<td>Manually Rotating Logs</td>
<td>32</td>
</tr>
<tr>
<td>Working with Logs Example</td>
<td>32</td>
</tr>
<tr>
<td>Displaying List of Log Files</td>
<td>33</td>
</tr>
<tr>
<td>Viewing Logs</td>
<td>33</td>
</tr>
</tbody>
</table>
Log Files ................................................................. 42
  log.sysmand. ..................................................... 42
  log.bootstrap .................................................... 42
  log.berp .......................................................... 42
  log.broker ....................................................... 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
  log.atcpApp ...................................................... 43
  log.atcp .......................................................... 43
  log.audit .......................................................... 43
  log.auditpusher .................................................. 43
  log.authd .......................................................... 43
  log.certd .......................................................... 43
  log.qos .............................................................. 43
  log.lrd ............................................................. 44
  log.iked ............................................................ 44
  log.bcm ............................................................ 44
  log.lrtd ............................................................ 44
  log.ebmd ........................................................... 44
  syslog .............................................................. 44
  Process Logs ....................................................... 45
  HA Switchover Log ............................................... 45
  Log Message Graphical Display on Net-Net SBC. ...................... 45
2 Fault Management .................................................. 47

Overview ........................................................................ 47
Accessing Fault Management Data .................................. 47

About Traps ..................................................................... 47
Standard Traps .................................................................. 48
Enterprise Traps ............................................................... 48

About Alarms .................................................................... 50
Overview ........................................................................ 50
Types of Alarms ............................................................... 50
About the Alarm Process .................................................. 50
About Alarms and the Health Score ................................... 51
ACLI Instructions and Examples ........................................ 51
  Displaying Alarms .......................................................... 51
  Clearing Alarms ............................................................. 52
  About the Alarm Display on the Chassis ......................... 52
Alarm Severity Levels ...................................................... 52
Net-Net SBC Response to Alarms ....................................... 53
Writing to syslog (acmelog) ............................................... 53
Sending SNMP Traps ....................................................... 53
About Dry Contacts ........................................................ 53
Displaying Alarms to the Chassis ....................................... 54

Hardware and Environmental Faults ................................. 54
Hardware Temperature Alarm .......................................... 54
Fan Speed Alarm ............................................................. 55
Environmental Sensor Alarm ............................................. 55
Media Link Alarms ........................................................... 56
Power Supply Alarms ........................................................ 56
  Voltage Alarms ............................................................... 57
  Physical Interface Card Alarms ........................................... 57
Viewing PROM Statistics (Net-Net SBC 1 only) .................. 58
Graphic Window Display ................................................ 59
Fan Stopped Alarm ........................................................... 59
Temperature High Alarm .................................................. 59

System Fault Statistics ..................................................... 60
System State ................................................................. 60
  Viewing System Uptime .................................................. 60
  Viewing System State .................................................... 60
System Resources ............................................................ 60
  Viewing CPU Usage ....................................................... 60
  CPU Utilization Alarm .................................................... 61
  Memory Usage .............................................................. 61
Physical Interface Faults ........................................... 130
  Viewing Network Interface Statistics ........................................... 130
  Viewing Media Interface Statistics ........................................... 131
  Viewing Network Interface Statistics ........................................... 132
  Viewing Physical Interface Statistics ........................................... 132
  Viewing Front Interface Physical Level Statistics ............................... 132
  Physical Interface Alarms .................................................. 133
Verifying an IP Address ..................................................... 136
  Specifying a Source Address for ICMP Pings ................................. 136
DNS Statistics ............................................................... 137
  Viewing DNS Statistics for Specific Cache Entries ............................ 137
  Clearing ENUM and DNS Statistics ........................................... 137
System Support Information for Troubleshooting ............................... 138
  Included Data ............................................................. 139
    Using the ACLI show support-info command ..................................... 139
SIP Interface Constraints Monitoring ........................................... 141
  All SIP Interfaces ......................................................... 141
  Single SIP Interface ....................................................... 141
Displaying and Clearing Registration Cache Entries ............................ 142
  Working with the SIP Registration Cache ...................................... 142
    Displaying the SIP Registration Cache ...................................... 142
    Clearing the SIP Registration Cache ...................................... 144
    Auditing the SIP Registration Cache ...................................... 144
  Working with the H.323 Registration Cache ................................... 145
    Displaying the H.323 Registration Cache ................................... 145
    Clearing the H.323 Registration Cache ................................... 146
    Auditing the H.323 Registration Cache ................................... 146
  Working with the MGCP Registration Cache .................................... 146
    Displaying the MGCP Registration Cache .................................... 146
    Clearing the MGCP Registration Cache .................................... 147
    Auditing the MGCP Registration Cache .................................... 148
Session Management for SIP, H.323, and IWF ................................ 148
  Displaying Sessions ......................................................... 148
    Example 1: Displaying All SIP Sessions .................................... 149
    Example 2: Displaying All H.323 Sessions .................................. 149
    Example 3: Displaying SIP Sessions for a Session Agent ..................... 150
    Example 3: Displaying H.323 Sessions for a Session Agent .................. 150
    Example 4: Displaying SIP Sessions for a Call ID ............................. 151
  Clearing Sessions .......................................................... 152
    Example 1: Clearing All SIP Sessions ..................................... 152
3 Performance Management .............................................. 155

Overview .............................................................. 155

Viewing System Information ....................................... 155

ACLI Credit Information ............................................. 155
User Privilege Mode .................................................. 155
System Uptime .......................................................... 155
Current Date and Time .............................................. 156
Software Release Current Version .............................. 156

Viewing System Resource Information .......................... 156

System Memory ........................................................ 156
Listing Memory Subcommands ..................................... 156
Application Object Allocation and Use. ......................... 157
Memory Buffer .......................................................... 158
Control and Maintenance Interfaces ............................ 158

Viewing Active Processes .......................................... 162

Accessing Process Subcommands ............................... 164
Viewing Statistics for all Processes ............................. 166
Viewing Totals for all Processes ................................ 181
Viewing Current Statistics ........................................ 182
Checking Remaining Space ....................................... 182

Viewing Redundancy Statistics ................................... 183

Accessing Redundancy Subcommands .......................... 183
Configuration Checkpoint Example ............................. 183
About High Availability Transactions ........................ 184
Viewing Border Element Redundancy Protocol Information 184
Viewing Redundancy Health ........................................ 185
HA States ................................................................. 185
Command Examples .................................................. 186
Active ................................................................. 186
Standby ................................................................. 186

Viewing Routing Statistics ......................................... 188

Viewing Routing Table Entries .................................. 188
Viewing Routing Stats ............................................... 188
Testing Routing Policies .......................................... 188
Test Policy Subcommands ....................................... 189
Testing Address Translations .................................. 189
Viewing QoS Based Routing Statistics ......................... 189
Local Route Table Statistics and Management .............................................. 191
  Setting the Log Level ................................................................. 191
  Updating the Local Cache ......................................................... 191
  Testing a Lookup in the Local Cache ........................................... 191
  Displaying a Route Entry in the Local Cache ................................. 191
  Displaying Statistics for a Local Route Tables ............................... 192
  Resetting ENUM Statistic Counters............................................. 192

Viewing SIP Protocol Performance Statistics ........................................ 192
  Accessing SIP Statistics .......................................................... 192
  Example ...................................................................................... 193
  Viewing SIP Status Information .................................................. 193
  Viewing SIP Performance Statistics .............................................. 195
    All ............................................................................................ 195
    Example ................................................................................... 198
    About the Information .............................................................. 198
  Viewing Statistics for Other SIP Methods ....................................... 199
  SIP Monitoring by Transaction Type ............................................. 199
    SIP Server Transactions .......................................................... 199
    SIP Client Transactions .......................................................... 200
  Viewing SIP Media Event Errors .................................................. 200
  Viewing SIP Session Agent Statistics .......................................... 203
    Viewing SIP Session Agent Group Statistics .......................... 204
  Viewing Session and Dialog States .............................................. 204
    Sessions ................................................................................... 205
    Dialogs .................................................................................... 205
  Viewing SIP Endpoint ................................................................. 205
  Viewing SIP Per User CAC Statistics ........................................... 206
    IP-Based CAC Information ....................................................... 206
    AoR-Based CAC Information ..................................................... 206
    Number of Calls Dropped because of Per User CAC Limits ....... 207
  Viewing Statistics for SIP Per User Subscribe Dialog Limit ............ 207
  Viewing IMS-AKA Statistics .......................................................... 207
  STUN Server Statistics and Protocol Tracing .................................. 208
    STUN Server Statistics ............................................................. 208
    STUN Protocol Tracing .............................................................. 209

H.323 Protocol Performance ............................................................. 209
  Viewing the H.323 Performance Statistics ...................................... 209
  About Status Statistics ............................................................... 210
  About Stack Statistics ............................................................... 210
  Viewing Current Configuration .................................................... 210
  Viewing Stack Information ......................................................... 211
  Viewing a List of Stacks .............................................................. 211
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Stack Details</td>
<td>211</td>
</tr>
<tr>
<td>Viewing Specific Stacks</td>
<td>212</td>
</tr>
<tr>
<td>Viewing Session Agent Stats</td>
<td>213</td>
</tr>
<tr>
<td>Viewing a List of Session Agents</td>
<td>213</td>
</tr>
<tr>
<td>Viewing Session Agent Stats</td>
<td>213</td>
</tr>
<tr>
<td>Viewing Specific Session Agent Statistics</td>
<td>214</td>
</tr>
<tr>
<td>Viewing Session Agent Configurations</td>
<td>215</td>
</tr>
<tr>
<td>Viewing Session Agent by Hostname</td>
<td>216</td>
</tr>
<tr>
<td>Viewing Session Agent Group Stats</td>
<td>218</td>
</tr>
<tr>
<td>Listing Session Agent Groups</td>
<td>218</td>
</tr>
<tr>
<td>Viewing Session Agent Group Stats</td>
<td>218</td>
</tr>
<tr>
<td>Viewing Session Agent Details</td>
<td>218</td>
</tr>
<tr>
<td>Viewing Specific Session Group Statistics</td>
<td>219</td>
</tr>
<tr>
<td>Viewing all Configurations</td>
<td>219</td>
</tr>
<tr>
<td>Viewing Specific Session Agent Group Statistics</td>
<td>219</td>
</tr>
<tr>
<td>Viewing Stats for Each Configured Stack</td>
<td>220</td>
</tr>
<tr>
<td>Viewing Statistics for Specific Stacks</td>
<td>220</td>
</tr>
<tr>
<td>Viewing H.323 Registrations</td>
<td>222</td>
</tr>
<tr>
<td>Viewing MGCP Performance Statistics</td>
<td>222</td>
</tr>
<tr>
<td>Listing the MGCP Performance Subcommands</td>
<td>222</td>
</tr>
<tr>
<td>Viewing MGCP Status Statistics</td>
<td>223</td>
</tr>
<tr>
<td>About State Statistics</td>
<td>223</td>
</tr>
<tr>
<td>About MGCP Transactions</td>
<td>224</td>
</tr>
<tr>
<td>All Available Information</td>
<td>224</td>
</tr>
<tr>
<td>Viewing MGCP Error Statistics</td>
<td>226</td>
</tr>
<tr>
<td>MGCP Message Monitoring</td>
<td>227</td>
</tr>
<tr>
<td>Other MGCP Stats</td>
<td>227</td>
</tr>
<tr>
<td>Viewing Accounting Data and Statistics</td>
<td>228</td>
</tr>
<tr>
<td>QoS Reporting</td>
<td>228</td>
</tr>
<tr>
<td>Viewing Network Management Control Statistics</td>
<td>229</td>
</tr>
<tr>
<td>Displaying Network Management Control Statistics</td>
<td>229</td>
</tr>
<tr>
<td>Resetting Network Management Control Statistics</td>
<td>229</td>
</tr>
<tr>
<td>Monitoring Your Net-Net System in Real-Time</td>
<td>230</td>
</tr>
<tr>
<td>Displaying the Statistics</td>
<td>230</td>
</tr>
<tr>
<td>Changing the Refresh Rate</td>
<td>230</td>
</tr>
<tr>
<td>Quitting the Display</td>
<td>230</td>
</tr>
<tr>
<td>Viewing Real-Time Media Statistics</td>
<td>230</td>
</tr>
<tr>
<td>Viewing Real-Time SIP Session Statistics</td>
<td>232</td>
</tr>
<tr>
<td>Viewing TLS Information</td>
<td>233</td>
</tr>
<tr>
<td>Clearing the Entire TLS Session Cache</td>
<td>233</td>
</tr>
<tr>
<td>Viewing TLS Session Cache State and Statistics</td>
<td>233</td>
</tr>
</tbody>
</table>
Viewing Certificates in PEM Form ................................................. 233
Viewing Net-Net SSM Status ..................................................... 234

**Viewing IPSec Statistics** .................................................. 234
  Security Association Entries .............................................. 234
  Security Policy Entries ................................................... 235
  IPSec Statistics ................................................................ 235
    Viewing Statistics for a Specific SA ................................. 235
    Viewing Statistic for Traffic to/from the GMAC Interface and the Security Processor ...... 235
    Viewing IPSec Interface Status ....................................... 235

**Viewing SSH Security Information** ................................... 236
  Viewing SSH Statistics ....................................................... 236
  Viewing a Brief SSH Statistics Output ................................. 236
  Viewing a Detailed SSH Statistics Output ......................... 236

4 System Management ......................................................... 239

**User Privilege Levels and Passwords: Without Data Storage Security** ....... 239
  User and Superuser Modes ................................................ 239
  Setting Passwords ........................................................... 239
    SSH Remote Connections .............................................. 240
  SSH RADIUS Authentication VSA Support ....................... 241
  SSHv2 Public Key Authentication .................................... 241
    ACLI Instructions and Examples: Viewing SSH Public Key Data. ....................... 241
    Importing a Public Key Record ..................................... 242
  Expanded Privileges .......................................................... 243
  User Sessions ................................................................. 243
  Concurrent Sessions ........................................................ 244

**Data Storage Security** ................................................... 244
  Considerations When Enabling Data Storage Security ............ 244
  About Net-Net SBC Password Features .............................. 244
    Password Secure Mode .................................................. 245
    Protected Configuration Password for TLS, IPSec, and HDR ........ 245
    Configuration Migration ............................................... 245
    Password Requirements ............................................... 245
    Note on Backwards Compatibility .................................. 246
  Password Reset and Recovery ......................................... 246
  Password Policy .............................................................. 246
  Upgrade to ACP ............................................................... 246
  SSH Password Considerations ........................................ 247
  ACLI Instructions and Examples ..................................... 247
    Enabling Password-Secure Mode for the First Time .......... 247
    Setting a Protected Configuration Password: Matching Configurations ........ 248
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting a Protected Configuration Password: Mismatched Configurations</td>
<td>249</td>
</tr>
<tr>
<td>Setting a Protected Configuration Password: Committing Changes</td>
<td>250</td>
</tr>
<tr>
<td>Changing Protected Configuration Password on a Standby System in an HA Node</td>
<td>251</td>
</tr>
<tr>
<td>Confirming Synchronous Protected Configuration Password and Configuration</td>
<td>252</td>
</tr>
<tr>
<td>Configuration Migration</td>
<td>252</td>
</tr>
<tr>
<td>Setting the Password Policy</td>
<td>253</td>
</tr>
<tr>
<td>System Time</td>
<td>253</td>
</tr>
<tr>
<td>Setting Time</td>
<td>253</td>
</tr>
<tr>
<td>Setting Timezone</td>
<td>254</td>
</tr>
<tr>
<td>About UTC Timezones</td>
<td>254</td>
</tr>
<tr>
<td>Using the Timezone-Set Wizard</td>
<td>256</td>
</tr>
<tr>
<td>Configuring Timezone using POSIX Format</td>
<td>259</td>
</tr>
<tr>
<td>Manually Setting Timezone</td>
<td>261</td>
</tr>
<tr>
<td>Displaying the System Timezone</td>
<td>264</td>
</tr>
<tr>
<td>NTP Synchronization</td>
<td>265</td>
</tr>
<tr>
<td>Setting NTP Synchronization</td>
<td>265</td>
</tr>
<tr>
<td>Monitoring NTP from the ACLI</td>
<td>265</td>
</tr>
<tr>
<td>System Task Management</td>
<td>267</td>
</tr>
<tr>
<td>Viewing Tasks</td>
<td>267</td>
</tr>
<tr>
<td>Setting Task Log Levels</td>
<td>267</td>
</tr>
<tr>
<td>Stopping a Task</td>
<td>269</td>
</tr>
<tr>
<td>Notifying Tasks</td>
<td>269</td>
</tr>
<tr>
<td>Tracing Sockets</td>
<td>269</td>
</tr>
<tr>
<td>Notify Subcommands</td>
<td>269</td>
</tr>
<tr>
<td>Viewing Power Supply and RAMdrive Status</td>
<td>271</td>
</tr>
<tr>
<td>Rebooting the Net-Net SBC</td>
<td>271</td>
</tr>
<tr>
<td>reboot activate</td>
<td>271</td>
</tr>
<tr>
<td>reboot force</td>
<td>271</td>
</tr>
<tr>
<td>reboot force activate</td>
<td>271</td>
</tr>
<tr>
<td>Reboot Safeguards</td>
<td>272</td>
</tr>
<tr>
<td>Reboot Status File</td>
<td>272</td>
</tr>
<tr>
<td>Warning on Reboot</td>
<td>272</td>
</tr>
<tr>
<td>System Watchdog Timer</td>
<td>272</td>
</tr>
<tr>
<td>Watchdog Timer Configuration</td>
<td>273</td>
</tr>
<tr>
<td>Availability</td>
<td>273</td>
</tr>
<tr>
<td>ACLI Example</td>
<td>273</td>
</tr>
<tr>
<td>Configuring the Front Panel Interface</td>
<td>273</td>
</tr>
<tr>
<td>admin-state</td>
<td>274</td>
</tr>
<tr>
<td>auto-negotiation</td>
<td>274</td>
</tr>
<tr>
<td>duplex-mode</td>
<td>274</td>
</tr>
</tbody>
</table>
speed ................................................................. 274

**ARP Information** ................................................. 274
  show arp ......................................................... 275
  arp-add ......................................................... 275
  arp-delete ..................................................... 275
  arp-check ....................................................... 275

**NAT Information** ................................................. 276
  show nat info .................................................. 276
  show nat by-addr ............................................... 276
  show nat by-index ............................................. 278
  show nat in-tabular .......................................... 278

**SNMP Community and Trap Receiver Management** ................. 280
  SNMP Community Table ........................................ 280
    show snmp-community-table .................................. 280
    reset snmp-community-table ................................ 280
  Trap Receiver .................................................. 280
    show trap-receiver ......................................... 280
    reset trap-receiver ........................................ 281

**Login Banner** .................................................... 281

**ACLI Audit Trail** ................................................ 281

5 **Inventory Management** ........................................ 283

  Accessing Inventory Management Data .......................... 283

**Hardware Inventory** ............................................ 283
  Components ...................................................... 283
    show prom-info mainboard .................................... 283
    show prom-info CPU .......................................... 284
    show prom-info PHY0 ......................................... 284
    show prom-info PHY1 ......................................... 284

**Software Inventory** ............................................. 285
  System image ................................................... 285
    Image Filename: Net-Net 4250 and Net-Net 4500 ............. 285
    Location ...................................................... 285
    show version image .......................................... 285
    bootparam .................................................... 286
  Version ........................................................ 286
    show version ................................................ 286

**Configuration Information** .................................... 287
  Overview ....................................................... 287
    Configuration Show Subcommands ............................ 287
Running configuration Commands ................................................. 288
  show running-config ......................................................... 289
  show running-configuration media-manager .......................... 289
  display-running-cfg-version ........................................... 289
Configuration Commands ............................................................. 289
  show configuration .......................................................... 290
  show configuration media-manager ...................................... 290
  display-current-cfg-version ............................................ 290
Realm Specific ........................................................................ 290
  realm-specifics <realm ID> .............................................. 291
Running Configuration Example .................................................... 292

Software License Inventory ........................................................... 308
  About Licenses ................................................................. 308
  Unlicensed Signaling Protocols .......................................... 309
  Viewing License Information ............................................ 310
    show features ............................................................ 310
    license show ............................................................. 310
    show sessions ............................................................ 311

6 Net-Net 4250 Upgrading ............................................................ 313
  Introduction ...................................................................... 313
  Preparing for Upgrade .......................................................... 313
    Transferring Files .......................................................... 313
      Uploading SBC Software Image .................................... 313
      Downloading Running Configuration ............................ 314
    System Configuration Files Release Compatibility .......... 314
    Upgrade Paths and Release 2.2 ..................................... 314
  ACLI Upgrade Preparation Command ...................................... 315
    ACLI Instructions and Examples ..................................... 315
      Loading a New Image ................................................ 315
      When There is Insufficient Space for a New Image .......... 316
  S-C6.1.0 to S-C6.2.0 Upgrade .................................................. 317
    Pre-Upgrade Checklist ................................................ 317
  Stand-alone Upgrade .......................................................... 317
    Upgrade Procedure ........................................................ 317
  HA Upgrade ................................................................. 318
    Upgrade Overview ........................................................ 318
    Upgrade Process .......................................................... 319
  C6.0 to S-C6.1.0 Upgrade ...................................................... 321
    Pre-Upgrade Checklist ................................................ 321
Stand-alone Upgrade .......................................................... 321
Upgrade Procedure .......................................................... 321
HA Upgrade ................................................................. 322
Upgrade Overview ............................................................ 322
Upgrade Process ............................................................. 323

C5.1 to C6.0 Upgrade .......................................................... 325
Pre-Upgrade Checklist ..................................................... 325
Stand-alone Upgrade ....................................................... 325
Upgrade Procedure ........................................................ 325
HA Upgrade ................................................................. 326
Upgrade Overview ............................................................ 326
Upgrade Process ............................................................. 327

C5.0 to C5.1 Upgrade .......................................................... 329
Pre-Upgrade Checklist ..................................................... 329
Stand-alone Upgrade ....................................................... 329
Upgrade Procedure ........................................................ 329
HA Upgrade ................................................................. 330
Upgrade Overview ............................................................ 330
Upgrade Process ............................................................. 331

4.1 to C5.0 Upgrade ........................................................... 332
Pre-Upgrade Checklist ..................................................... 333
Standalone Upgrade ....................................................... 333
Upgrade Procedure ........................................................ 333
HA Upgrade ................................................................. 334
Upgrade Overview ............................................................ 334
Upgrade Process ............................................................. 334

4.0 to 4.1 Upgrade ........................................................... 336
Pre-Upgrade Checklist ..................................................... 337
Standalone Upgrade ....................................................... 337
Upgrade Procedure ........................................................ 337
HA Upgrade ................................................................. 338
Upgrade Overview ............................................................ 338
Upgrade Process ............................................................. 338

2.x to 4.0 Upgrade ........................................................... 340
Pre-Upgrade Checklist ..................................................... 341
Standalone Upgrade ....................................................... 341
Upgrade Procedure ........................................................ 341
HA Upgrade ................................................................. 342
Upgrade Overview ............................................................ 342
Upgrade Process ............................................................. 342

2.0/2.1 to 2.2 Upgrade .......................................................... 344
7 Net-Net 4500 Upgrading ........................................... 375

Introduction ........................................................... 375

Notes on Boot Parameters ........................................ 375
Net-Net 3800 ............................................................. 375
Preparing for Upgrade ............................................... 375
Password Secure Mode ............................................... 375

Upgrading S-CX6.2.0 Software Images ............................. 375

Pre-Upgrade Checklist ............................................... 375
Stand-alone Upgrade ............................................... 376
Upgrade Procedure ................................................ 376
HA Upgrade ............................................................. 377
Upgrade Process .................................................... 377
HA Backout Procedure ............................................. 379

Upgrading S-CX6.1.0 Software Images ............................. 380

Pre-Upgrade Checklist ............................................... 380
Stand-alone Upgrade ............................................... 380
Upgrade Procedure ................................................ 381
HA Upgrade ............................................................. 381
Upgrade Process .................................................... 381
HA Backout Procedure ............................................. 384

Upgrading CX6.0.0 Software Images .............................. 385

Pre-Upgrade Checklist ............................................... 385
Stand-alone Upgrade ............................................... 385
Upgrade Procedure ................................................ 385
HA Upgrade ............................................................. 386
Upgrade Process .................................................... 386
HA Backout Procedure ............................................. 389

Moving a Configuration ............................................... 390

Backup Commands .................................................. 390
Creating a Backup on Your Net-Net 4250 ......................... 391
Listing Backups ...................................................... 391
Copying the Backup to Your Net-Net 4500 ....................... 391
Restoring Backups .................................................. 392

8 Working with Configurations ..................................... 395

Configuration Overview ........................................... 395

Configuration Process .............................................. 395
Verifying & Regenerating Configurations ......................... 396
Verifying Address Duplication ................................... 397
Network-Interface .................................................. 397
<table>
<thead>
<tr>
<th>Class-Policy</th>
<th>427</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-Config</td>
<td>427</td>
</tr>
<tr>
<td>ENUM-Config</td>
<td>427</td>
</tr>
<tr>
<td>Ext-Policy-Server</td>
<td>427</td>
</tr>
<tr>
<td>H323-Stack</td>
<td>428</td>
</tr>
<tr>
<td>Host-Route</td>
<td>428</td>
</tr>
<tr>
<td>IWF-Config</td>
<td>428</td>
</tr>
<tr>
<td>Local-Policy</td>
<td>428</td>
</tr>
<tr>
<td>Local-Routing-Config</td>
<td>429</td>
</tr>
<tr>
<td>MGCP-Config</td>
<td>429</td>
</tr>
<tr>
<td>Network-Interface</td>
<td>429</td>
</tr>
<tr>
<td>Phy-Interface</td>
<td>429</td>
</tr>
<tr>
<td>Public-Key</td>
<td>430</td>
</tr>
<tr>
<td>Realm-Config</td>
<td>430</td>
</tr>
<tr>
<td>Realm-Group</td>
<td>431</td>
</tr>
<tr>
<td>Redundancy</td>
<td>431</td>
</tr>
<tr>
<td>Security-Association</td>
<td>432</td>
</tr>
<tr>
<td>Security-Policy</td>
<td>433</td>
</tr>
<tr>
<td>Session-Agent</td>
<td>433</td>
</tr>
<tr>
<td>Session-Group</td>
<td>434</td>
</tr>
<tr>
<td>Session-Translation</td>
<td>434</td>
</tr>
<tr>
<td>SIP-Config</td>
<td>434</td>
</tr>
<tr>
<td>SIP-Interface</td>
<td>435</td>
</tr>
<tr>
<td>SIP-Manipulation</td>
<td>435</td>
</tr>
<tr>
<td>SIP-NAT</td>
<td>436</td>
</tr>
<tr>
<td>Static-Flow</td>
<td>436</td>
</tr>
<tr>
<td>Steering-Pool</td>
<td>436</td>
</tr>
<tr>
<td>Surrogate-Agent</td>
<td>437</td>
</tr>
<tr>
<td>System-Config</td>
<td>437</td>
</tr>
<tr>
<td>TLS-Profile</td>
<td>438</td>
</tr>
</tbody>
</table>
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.

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

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.

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

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-config->enable-snmp-monitor-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:

```
notify * rotate-logs
```

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:

```
notify mbcd log
```

2. Make some test calls.

3. Set message writing to the log off by entering the following command:

```
notify mbcd nolog
```

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:
```

<table>
<thead>
<tr>
<th>Access</th>
<th>Mode</th>
<th>Owner</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>512</td>
<td>Jul 4</td>
<td>18:02</td>
<td>.</td>
</tr>
<tr>
<td>drwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>512</td>
<td>Jul 6</td>
<td>09:50</td>
<td>.</td>
<td>..</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>820707</td>
<td>Jul 6</td>
<td>11:55</td>
<td>acmelog</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>3447</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.sysmand</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>3724</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.bootstrap</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>132</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.brokerd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>740</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.npsoft</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>369</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.berpd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>26660</td>
<td>Jul 6</td>
<td>11:46</td>
<td>log.cliWorker</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>3316</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.lemd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>852</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.atcpd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>733</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.atcpApp</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>2877</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.mbcd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>757</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.lid</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>1151</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.algd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>741</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.radd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>728</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.pusher</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>1448</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.ebmd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>671322</td>
<td>Jul 6</td>
<td>11:55</td>
<td>log.sipd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>681011</td>
<td>Jul 6</td>
<td>11:55</td>
<td>log.h323d</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>1169</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.h248d</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>18294</td>
<td>Jul 2</td>
<td>17:40</td>
<td>log.snmpd</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>1078</td>
<td>Jul 2</td>
<td>17:40</td>
<td>snmpd.log</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>190</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliSSH0</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>191</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliSSH1</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>192</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliSSH2</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>192</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliSSH3</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>192</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliSSH4</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>3043</td>
<td>Jul 6</td>
<td>11:38</td>
<td>log.acliConsole</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>2655</td>
<td>Jul 2</td>
<td>21:07</td>
<td>log.acliTelnet0</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>195</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliTelnet1</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>195</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliTelnet2</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>195</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliTelnet3</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>195</td>
<td>Jul 2</td>
<td>15:59</td>
<td>log.acliTelnet4</td>
</tr>
<tr>
<td>r</td>
<td>rwxrwxrwx</td>
<td>1</td>
<td>0</td>
<td>1000005</td>
<td>Jul 4</td>
<td>18:01</td>
<td>acmelog.1</td>
</tr>
</tbody>
</table>

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 15:25:28.170 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 15:25:28.223 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 15:25:28.431 bootstrap@ACMEPACKET:MINOR is Wancom: No matching if for 10.0.0.0
Jun 19 15:25:28.445 berpd@ACMEPACKET:MINOR berpd: redundancy is disabled
```
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.

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

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
```
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:

```plaintext
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,
algorithmdo=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='acliSSH0'/>
  <process name='brokerd'/>
  <process name='tCliWorker'/>
  <process name='lemd'/>
  <process name='atcpd'/>
  <process name='atcpApp'/>
  <process name='mbcd'/>
  <process name='lid'/>
  <process name='algd'/>
  <process name='radd'/>
  <process name='pusher'/>
  <process name='ebmd'/>
  <process name='sipd'/>
  <process name='h248d'/>
  <process name='snmpd'/>
  <process name='acliSSH1'/>
  <process name='acliSSH2'/>
```
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
Authorization: Digest
username="user",
realm="intern1",
nonce=5dd735490c78a0146ca06d50f47c0a50,
uri="/sysmand@acmesystem",
response=129b082a3ee110db86565932819d017b,
algorithm="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 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: 544
```

<sysmand>
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:

```plaintext
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

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.

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.

### 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 tCliWoker processes.

**log.atcpApp**

This log contains information about the asynchronous Transport Control Protocol (TCP).

**log.atcpd**

This log contains information about the asynchronous TCP daemon.

**log.audit**

This log contains information about any audits performed on the system.

**log.auditpusher**

This log contains information about the audits that were pushed on the system.

**log.authd**

This log contains information about authentication used on the system.

**log.certd**

This log contains information about certificate records used on the system.

**log.qos**

This log contains information about quality of service (qos) for call sessions.

**log.lid**

This log contains information about the lawful intercept daemon.
**log.iked**  
This log contains information about the secure Internet Key Exchange (IKE) daemon.

**log.bcm**  
This log contains information about the Business Call Management (BCM) logger used with the system to process call detail records (CDR).

**log.lrtd**  
This log contains information about the local routing table (LRT) daemon.

**log.ebmd**  
This log contains information about Common Open Policy Service (COPS) and Call Admission Control (CAC) on the system. It is information about the External Bandwidth Manager (Radius/Diameter).

**syslog**  
The term syslog 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.

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.

**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.

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.
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

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 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.

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkUp</td>
<td>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.</td>
</tr>
<tr>
<td>linkDown</td>
<td>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.</td>
</tr>
<tr>
<td>coldStart</td>
<td>The SNMPv2 agent is reinitializing itself and its configuration may have been altered. This trap is not associated with a Net-Net system alarm.</td>
</tr>
<tr>
<td>authenticationFailure</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Enterprise Traps

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

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apSyslogMessageGenerated</td>
<td>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.</td>
</tr>
<tr>
<td>apSysMgmtGroupTrap</td>
<td>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.</td>
</tr>
<tr>
<td>apLicenseApproachingCapacityNotification</td>
<td>Generated when the total number of active sessions on the system (across all protocols) is within 98 - 100% of the licensed capacity.</td>
</tr>
<tr>
<td>apLicenseNotApproachingCapacityNotification</td>
<td>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).</td>
</tr>
<tr>
<td>apEnvMonI2CFailNotification</td>
<td>Generated when the Inter-IC bus (I2C) state changes from normal (1) to not functioning (7).</td>
</tr>
<tr>
<td>apEnvMonStatusChangeNotification</td>
<td>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.</td>
</tr>
<tr>
<td>apSwCfgActivateNotification</td>
<td>Generated when an activate-config command is issued and the configuration has been changed at running time.</td>
</tr>
<tr>
<td>Trap Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>apSysMgmtPowerTrap</td>
<td>Generated if a power supply is powered down, powered up, inserted/present or removed/not present.</td>
</tr>
<tr>
<td>apSysMgmtTempTrap</td>
<td>Generated if the temperature falls below the monitoring level.</td>
</tr>
<tr>
<td>apSysMgmtFanTrap</td>
<td>Generated if a fan unit speed falls below the monitoring level.</td>
</tr>
<tr>
<td>apSysMgmtTaskSuspendTrap</td>
<td>Generated if a critical task running on the system enters a suspended state.</td>
</tr>
<tr>
<td>apSysMgmtRedundancyTrap</td>
<td>Generated if a state change occurs on either the primary or secondary system in a redundant (HA) pair.</td>
</tr>
<tr>
<td>apSysMgmtMediaPortsTrap</td>
<td>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.</td>
</tr>
<tr>
<td>apSysMgmtMediaBandwidthTrap</td>
<td>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.</td>
</tr>
<tr>
<td>apSysMgmtMediaOutOfRangeMemory</td>
<td>Generated if the media process cannot allocate memory.</td>
</tr>
<tr>
<td>apSysMgmtMediaUnknownRealm</td>
<td>Generated if the media process cannot find an associated realm for the media flow.</td>
</tr>
<tr>
<td>apSysMgmtRadiusDownTrap</td>
<td>Generated if all or some configured RADIUS accounting servers have timed out from a RADIUS server.</td>
</tr>
<tr>
<td>apSysMgmtGatewayUnreachableTrap</td>
<td>Generated if the gateway specified becomes unreachable by the system.</td>
</tr>
<tr>
<td>apSysMgmtH323InitFailTrap</td>
<td>Generated if the H.323 stack has failed to initialize properly and has been terminated.</td>
</tr>
<tr>
<td>apSysMgmtHardwareErrorTrap</td>
<td>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.</td>
</tr>
<tr>
<td>apSysMgmtDOSTrap</td>
<td>Generated when the IP address and the realm ID is denied of service.</td>
</tr>
<tr>
<td>apSysMgmtCfgSaveFailTrap</td>
<td>Generated if an error occurs while the system is trying to save the configuration to memory.</td>
</tr>
<tr>
<td>apSysMgmtSystemStateTrap</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• online(0)</td>
</tr>
<tr>
<td></td>
<td>• becoming-offline(1)</td>
</tr>
<tr>
<td></td>
<td>• offline(2)</td>
</tr>
<tr>
<td>apSysMgmtAuthenticationFailedTrap</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• administration and access level (SSH, user, enable)</td>
</tr>
<tr>
<td></td>
<td>• connection type (Telnet or console)</td>
</tr>
</tbody>
</table>
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# display-alarms
   3 alarms to show
   ID     Task     Severity        First Occurred          Last Occurred
   Count Description
   1     ingress realm 'test_client_realm' not found
   
   131075 36786224        3       2005-02-10 13:59:05     2005-02-10 13:59:05
   Count Description
   1     Slot 0 Port 0 DOWN
   
   Count Description
   1     health score is under threshold 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 toposmost 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.

<table>
<thead>
<tr>
<th>Alarm Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>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.</td>
</tr>
<tr>
<td>Critical</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
<th>Health Score Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEMPERATURE HIGH</td>
<td>65538</td>
<td>SD1:</td>
<td>Fans are obstructed or stopped. The room is abnormally hot.</td>
<td>Temperature: XX.XX°C (where XX.XX is the temperature in degrees)</td>
<td>• apSyslogMessageGenerated trap generated</td>
<td>CRITICAL: -100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CRITICAL: ≥70°C</td>
<td></td>
<td></td>
<td>• apEnvMonStatusChangeNotification</td>
<td>MAJOR: -50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAJOR: ≥60°C</td>
<td></td>
<td></td>
<td>• apSysMgmtTempTrap</td>
<td>MINOR: -25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MINOR: ≥50°C</td>
<td></td>
<td></td>
<td>• critical, major, minor dry contact</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SD2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CRITICAL: ≥75°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAJOR: ≥65°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MINOR: ≥55°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SD3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CRITICAL: ≥105°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAJOR: ≥100°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MINOR: ≥95°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
<th>Health Score Impact</th>
</tr>
</thead>
</table>
| 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 is the Revolutions per Minute (RPM) of each fan on the fan module | • apSyslogMessageGenerated trap generated  
• apEnvMonStatusChangeNotification  
• 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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
<th>Health Score Impact</th>
</tr>
</thead>
</table>
| 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! | • apSyslogMessageGenerated trap generated  
• critical, major, minor dry contact  
• syslog  
Acme Packet recommends you perform the following:  
• 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 |
媒体链接警报

媒体链接警报包括以下内容：

- **重大**
  
  如果Net-Net SBC的媒体链接从正常变为异常，它将被视为重大警报。此警报适用于Net-Net SBC的两个槽位1和2。主要出现在Net-Net SBC机箱的前面板上，类似以下内容：
  
  **重大警报**
  端口Gig Port 1 DOWN

- **轻微**
  
  如果Net-Net SBC的媒体链接从异常变为正常，它将被视为轻微警报。此警报适用于Net-Net SBC的两个槽位1和2。

**电源供应警报**

以下表格描述了电源供应警报

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLD POWER A FAILURE</td>
<td>65540</td>
<td>MINOR (-10)</td>
<td>Power supply A has failed.</td>
<td>Back Power Supply A has failed!</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• minor dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
<tr>
<td>PLD POWER A UP</td>
<td>65541</td>
<td>MINOR</td>
<td>Power supply A is now present and functioning.</td>
<td>Back Power Supply A is present!</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• minor dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
</tbody>
</table>

如果Net-Net系统以一个电源启动，系统健康得分为100，且将不会生成任何警报。如果另一个电源随后添加到同一Net-Net系统，同样的警报将被触发，但系统健康得分不会被减分。

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLD POWER B FAILURE</td>
<td>65542</td>
<td>MINOR (-10)</td>
<td>Power supply B has failed.</td>
<td>Back Power Supply B has failed!</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• minor dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
<tr>
<td>PLD POWER B UP</td>
<td>65543</td>
<td>MINOR</td>
<td>Power supply B is now present and functioning.</td>
<td>Back Power Supply B is present!</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• minor dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
</tbody>
</table>
### Voltage Alarms

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

<table>
<thead>
<tr>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>65544</td>
<td>MINOR</td>
<td>• Voltage 2.5V CPU has minor alarm&lt;br&gt;• Voltage 2.5V CPU has emergency alarm, the system should shutdown</td>
<td>apSyslogMessageGenerated trap generated&lt;br&gt;dry contact&lt;br&gt;syslog</td>
<td></td>
</tr>
<tr>
<td>65545</td>
<td>MINOR</td>
<td>• Voltage 3.3V has minor alarm&lt;br&gt;• Voltage 3.3V has emergency alarm, the system should shutdown</td>
<td>apSyslogMessageGenerated trap generated&lt;br&gt;dry contact&lt;br&gt;syslog</td>
<td></td>
</tr>
<tr>
<td>65546</td>
<td>MINOR</td>
<td>• Voltage 5V has minor alarm&lt;br&gt;• Voltage 5V has emergency alarm, the system should shutdown</td>
<td>apSyslogMessageGenerated trap generated&lt;br&gt;dry contact&lt;br&gt;syslog</td>
<td></td>
</tr>
<tr>
<td>65547</td>
<td>MINOR</td>
<td>• Voltage CPU has minor alarm&lt;br&gt;• Voltage CPU has emergency alarm, the system should shutdown</td>
<td>apSyslogMessageGenerated trap generated&lt;br&gt;dry contact&lt;br&gt;syslog</td>
<td></td>
</tr>
</tbody>
</table>

### Physical Interface Card Alarms

The following table describes the physical interface card alarms.

<table>
<thead>
<tr>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>65550</td>
<td>MAJOR</td>
<td>Physical interface card 0 was removed.</td>
<td>PHY card 0 has been removed.</td>
<td></td>
</tr>
<tr>
<td>65552</td>
<td>MAJOR</td>
<td>Physical interface card 0 was inserted.</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>65553</td>
<td>MAJOR</td>
<td>Physical interface card 1 was removed.</td>
<td>PHY card 1 has been removed.</td>
<td></td>
</tr>
<tr>
<td>65554</td>
<td>MAJOR</td>
<td>Physical interface card 1 was inserted.</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Id</th>
<th>Pri</th>
<th>Status</th>
<th>Total CPU</th>
<th>Avg</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>tAlarm</td>
<td>1be43bb0</td>
<td>60</td>
<td>DELAY</td>
<td>29.524</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tAndMgr</td>
<td>1335f370</td>
<td>95</td>
<td>PEND+T</td>
<td>11.450</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tNetTask</td>
<td>06acf730</td>
<td>50</td>
<td>READY</td>
<td>6.809</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tAtcpd</td>
<td>18ba1130</td>
<td>75</td>
<td>PEND+T</td>
<td>4.236</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tTfsPTask</td>
<td>06a0eaed</td>
<td>100</td>
<td>DELAY</td>
<td>2.956</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tSSH</td>
<td>1bfa58b0</td>
<td>55</td>
<td>PEND+T</td>
<td>2.419</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tNpwbTmr</td>
<td>1883ab0</td>
<td>0</td>
<td>DELAY</td>
<td>1.881</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tSysmand</td>
<td>1320a960</td>
<td>75</td>
<td>PEND+T</td>
<td>1.879</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tExcTask</td>
<td>027588e8</td>
<td>80</td>
<td>PEND+T</td>
<td>1.680</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tTaskCheck</td>
<td>132d09c0</td>
<td>100</td>
<td>DELAY</td>
<td>1.116</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tH323d</td>
<td>1ba661f0</td>
<td>80</td>
<td>PEND+T</td>
<td>1.086</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tSipd</td>
<td>1b970c50</td>
<td>80</td>
<td>PEND+T</td>
<td>1.032</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tArpMgr</td>
<td>188614e0</td>
<td>61</td>
<td>PEND</td>
<td>0.691</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tArpTmr</td>
<td>18861890</td>
<td>61</td>
<td>DELAY</td>
<td>0.490</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>tifXCheck</td>
<td>1be20bb0</td>
<td>60</td>
<td>DELAY</td>
<td>0.483</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
```
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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU UTILIZATION</td>
<td>131099</td>
<td>MINOR</td>
<td>CPU usage reached 90% or greater of its capacity.</td>
<td>CPU usage X% over threshold X%</td>
<td>sysMgmtGroupTrap trap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>minor dry contact syslog</td>
</tr>
</tbody>
</table>

### 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
alloc    225332816  4203   53612     -
internal  448       2     224     -
cumulative
alloc    228178000  17335  13162     -
peak
alloc    225504896  -     -     -
```

Memory Errors:
Links Repaired: 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-remaining boot
boot: 29759488/29760512 bytes (99%) remaining

ACMEPACKET# check-space-remaining code
code: 26351616/29760512 bytes (88%) remaining

ACMEPACKET# check-space-remaining ramdrv
ramdrv: 131218944/132104192 bytes (99%) remaining
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 minsize maxsize empty
Memory Utilization Alarm

The following table describes the memory utilization alarm.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEMORY UTILIZATION</td>
<td>131100</td>
<td>MAJOR</td>
<td>Memory usage reached 90% or greater of its capacity.</td>
<td>Memory usage X% over threshold X%</td>
<td>• apSysMgmtGroupTrap trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• minor dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LICENSE ALARM APPROACHING SESSION</td>
<td>327684</td>
<td>MAJOR</td>
<td>Total number of active sessions on the system (across all protocols) is within 98 to 100% of the Net-Net system’s licensed capacity.</td>
<td>Total number of sessions (&lt;#&gt;) is approaching licensed capacity (&lt;#&gt;)</td>
<td>• apLicenseApproachingCapacityNotification</td>
</tr>
</tbody>
</table>

Configuration Statistics

You can use the following commands to display configuration information:

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

```bash
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
  mbcd-log-level                 NOTICE
  red-flow-port                  1985
  red-mgcp-port                  1986
  red-max-trans                  10000
  red-sync-start-time            5000
  red-sync-comp-time             1000
  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:
### Viewing Realm-Specific Configuration

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

```plaintext
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm Identifier</td>
<td>testrealm</td>
</tr>
<tr>
<td>Address Prefix</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td></td>
</tr>
<tr>
<td>MM-In-Realm</td>
<td>disabled</td>
</tr>
<tr>
<td>MM-In-Network</td>
<td>enabled</td>
</tr>
<tr>
<td>MM-Same-Ip</td>
<td>enabled</td>
</tr>
<tr>
<td>MM-In-System</td>
<td>disabled</td>
</tr>
<tr>
<td>BW-CAC-Non-MM</td>
<td>disabled</td>
</tr>
<tr>
<td>MSM-Release</td>
<td>disabled</td>
</tr>
<tr>
<td>QOS-Enable</td>
<td>disabled</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>Ext-Policy-Svr</td>
<td>boffo.com</td>
</tr>
<tr>
<td>Max Latency</td>
<td>0</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>0</td>
</tr>
<tr>
<td>Max Packet Loss</td>
<td>0</td>
</tr>
<tr>
<td>Observation Window Size</td>
<td>0</td>
</tr>
<tr>
<td>Parent Realm</td>
<td></td>
</tr>
<tr>
<td>DNS Realm</td>
<td></td>
</tr>
<tr>
<td>Media Policy</td>
<td></td>
</tr>
<tr>
<td>In Translation ID</td>
<td></td>
</tr>
<tr>
<td>Out Translation ID</td>
<td></td>
</tr>
<tr>
<td>In Manipulation ID</td>
<td></td>
</tr>
<tr>
<td>Out Manipulation ID</td>
<td></td>
</tr>
<tr>
<td>Class Profile</td>
<td></td>
</tr>
<tr>
<td>Average Rate Limit</td>
<td>0</td>
</tr>
<tr>
<td>Access Control Trust Level</td>
<td>low</td>
</tr>
<tr>
<td>Invalid Signal Threshold</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Signal Threshold</td>
<td>0</td>
</tr>
<tr>
<td>Untrusted Signal Threshold</td>
<td>750</td>
</tr>
<tr>
<td>Deny Period</td>
<td>30</td>
</tr>
<tr>
<td>Symmetric Latching</td>
<td>disabled</td>
</tr>
<tr>
<td>PAI Strip</td>
<td>disabled</td>
</tr>
<tr>
<td>Trunk Context</td>
<td></td>
</tr>
<tr>
<td>Early Media Allow</td>
<td>reverse</td>
</tr>
<tr>
<td>Additional Prefixes</td>
<td>10.0.0.0/24</td>
</tr>
<tr>
<td>172.16.0.0</td>
<td></td>
</tr>
<tr>
<td>Restricted Latching</td>
<td>peer-ip</td>
</tr>
<tr>
<td>Restriction Mask</td>
<td>17</td>
</tr>
<tr>
<td>Accounting Enable</td>
<td>enabled</td>
</tr>
<tr>
<td>User CAC Mode</td>
<td>none</td>
</tr>
<tr>
<td>User CAC Bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>User CAC Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Net Management Control</td>
<td>disabled</td>
</tr>
<tr>
<td>Delay Media Update</td>
<td>disabled</td>
</tr>
<tr>
<td>Codec Policy</td>
<td></td>
</tr>
<tr>
<td>Codec Manip-In Realm</td>
<td>disabled</td>
</tr>
<tr>
<td>Last Modified Date</td>
<td>2006-07-06 12:43:39</td>
</tr>
</tbody>
</table>
```
• 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-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
    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
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
Configuration Save Failed Alarm

The following table lists the CFG ALARM SAVE FAILED alarm.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG ALARM SAVE FAILED</td>
<td>393217</td>
<td>MAJOR</td>
<td>The save-config command execution failed on a standby Net-Net SBC peer operating as part of an HA pair.</td>
<td>save-config failed on targetName/code full, config sync stopped!</td>
<td>• apply syslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or save-config failed on targetName/code full, config sync stopped! (where the targetName is the target name (tn) configured in the boot parameters)</td>
<td>• syslog</td>
</tr>
</tbody>
</table>

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 ?
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
```

### 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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTH SCORE</td>
<td>131101</td>
<td>MAJOR</td>
<td>Net-Net system's health score fell below 60.</td>
<td>Health score X is under threshold (where X is the health score)</td>
<td>• apSysMgmtGroupTrap</td>
</tr>
<tr>
<td>NAT TABLE UTILIZATION</td>
<td>131102</td>
<td>MINOR</td>
<td>NAT table usage reached 90% or greater of its capacity.</td>
<td>NAT table usage X% over threshold X%</td>
<td>• apSysMgmtGroupTrap</td>
</tr>
<tr>
<td>ARP TABLE UTILIZATION</td>
<td>131103</td>
<td>MINOR</td>
<td>ARP table usage reached 90% or greater of its capacity.</td>
<td>ARP table X% over threshold X%</td>
<td>• apSysMgmtGroupTrap</td>
</tr>
<tr>
<td>REDUNDANT SWITCH-TO-ACTIVE</td>
<td>131104</td>
<td>CRITICAL</td>
<td>A state transition occurred from Standby/Becoming Standby to BecomingActive.</td>
<td>Switchover, &lt;state to state&gt;, active peer &lt;name of HA peer&gt; has timed out or Switchover, &lt;state to state&gt;, active peer &lt;name of HA peer&gt; has unacceptable health (x) (where x is the health score) or Switchover, &lt;state to state&gt;, forced by command</td>
<td>• apSyslogMessageGenerated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• apSysMgmtRedundancyTrap</td>
</tr>
<tr>
<td>REDUNDANT SWITCH-TO-STANDBY</td>
<td>131105</td>
<td>CRITICAL</td>
<td>A state transition occurred from Active/BecomingActive to BecomingStandby/ RelinquishingActive.</td>
<td>Switchover, &lt;state to state&gt;, peer &lt;name of HA peer&gt; is healthier (x) than us (x) (where x is the health score) or Switchover, &lt;state to state&gt;, forced by command</td>
<td>• apSyslogMessageGenerated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• apSysMgmtRedundancyTrap</td>
</tr>
<tr>
<td>REDUNDANT TIMEOUT</td>
<td>131106</td>
<td>MAJOR</td>
<td>An HA Net-Net system peer was not heard from within a time period.</td>
<td>Peer &lt;name of HA peer&gt; timed out in state x, my state is x (where x is the state (for example, BecomingStandby))</td>
<td>• apSyslogMessageGenerated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• apSysMgmtRedundancyTrap</td>
</tr>
</tbody>
</table>
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.

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

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. Note that the command does not send an ARP request if the specified address is already in the ARP table or is in a different subnet.

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: Sending ARP REQ port=0, vlan=6, source_ipa=192.168.200.10, target_ipa=192.168.100.1
```
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

<table>
<thead>
<tr>
<th>destination</th>
<th>gateway</th>
<th>flags</th>
<th>Refcnt</th>
<th>Use</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.30.0.1</td>
<td>00:0f:23:4a:d8:80</td>
<td>405</td>
<td>1</td>
<td>0</td>
<td>wancom0</td>
</tr>
</tbody>
</table>

--- 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
```
The following table describes the ARP table utilization alarm.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP TABLE UTILIZATION</td>
<td>131103</td>
<td>MINOR</td>
<td>ARP table usage reached 90% or greater of its capacity.</td>
<td>ARP table X% over threshold X%</td>
<td>· apSysMgmtGroupTrap trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>· syslog</td>
</tr>
</tbody>
</table>

**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 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 `<filename>`.
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# monitor sessions
09:10:26-172
```

<table>
<thead>
<tr>
<th>SIP Status</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dialogs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CallID Map</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rejections</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ReINVITEs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Pending</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Server Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Resp Contexts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Saved Contexts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sockets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Req Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNS Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNS Sockets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNS Results</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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
- Req 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        ---- Lifetime ----
                  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
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 ----------
Realm         Used   Free  No Ports    Flows Ingrss Egress  Total  Insuf BW
acme             0      0         0        0     0K     0K     0K         0
h323172          2  29999         0        0     0K     0K     0K         0
sip172           2  29999         0        0     0K     0K     0K         0
sip192           0  30001         0        0     0K     0K     0K         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

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                -- 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          1141    1234    5748    2503147    8440     2974
Flow-Rel Released   0       0       0          0       0
MSM-Release         0       0       0          0       0
Rel-Port             -       -       0      14796    4156
Rel-Hairpin         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:

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBCD ALARM OUT OF MEMORY</td>
<td>262145</td>
<td>CRITICAL: for flow</td>
<td>No further memory can be allocated for MBCD.</td>
<td>Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.</td>
<td>apSyslogMessageGenerated (ap-slog.mib)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAJOR: for media (if server cannot allocate a new context)</td>
<td></td>
<td></td>
<td>apSysMgmtMediaOutOfMemory</td>
</tr>
<tr>
<td>MBCD ALARM UNKNOWN REALM</td>
<td>262147</td>
<td>MAJOR: if media server is adding a new flow</td>
<td>Media server is unable to find realm interface.</td>
<td>Realm type (ingress, egress, hairpin) X, not found</td>
<td>apSyslogMessageGenerated (ap-slog.mib)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>apSysMgmtUnknownRealm</td>
</tr>
</tbody>
</table>
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:

```
acmpacket# 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 ()
0x00a69ea4 sip_proxy_daemon(int, char **, semaphore *)+ae8: Process::Run(int, int) ()
```

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  0x3df00b50  12240   392   440  11800
```

MBCD ALARM OUT OF BANDWIDTH

262149  CRITICAL: failure rate = 100%
MAJOR: failure rate > or = 50%
The realm is out of bandwidth.
Out of bandwidth
• 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
• apSyslogMessageGenerated (ap-slog.mib)
• apSysMgmtMediaPortsTrap
<table>
<thead>
<tr>
<th>Task</th>
<th>Type</th>
<th>Address</th>
<th>Size</th>
<th>Usage</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>tCliSSH1</td>
<td>aclI (tag) CLI</td>
<td>0x3df66f80</td>
<td>65488</td>
<td>1920</td>
<td>9888</td>
</tr>
<tr>
<td>tCliSSH2</td>
<td>aclI (tag) CLI</td>
<td>0x3df67460</td>
<td>65488</td>
<td>1920</td>
<td>9888</td>
</tr>
<tr>
<td>tCliSSH3</td>
<td>aclI (tag) CLI</td>
<td>0x3df67940</td>
<td>65488</td>
<td>1920</td>
<td>9888</td>
</tr>
<tr>
<td>tCliSSH4</td>
<td>aclI (tag) CLI</td>
<td>0x3df67e20</td>
<td>65488</td>
<td>1920</td>
<td>9888</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df68460</td>
<td>65488</td>
<td>6056</td>
<td>21432</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df68840</td>
<td>65488</td>
<td>1968</td>
<td>19672</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df68c20</td>
<td>65488</td>
<td>1968</td>
<td>9936</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df69000</td>
<td>65488</td>
<td>1968</td>
<td>9936</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df693e0</td>
<td>65488</td>
<td>1968</td>
<td>9936</td>
</tr>
<tr>
<td>tCliTelnet</td>
<td>cliInterface</td>
<td>0x3df697c0</td>
<td>65488</td>
<td>1968</td>
<td>9936</td>
</tr>
<tr>
<td>tWbTask</td>
<td>wdbTask</td>
<td>0x3df1bff0</td>
<td>8144</td>
<td>280</td>
<td>352</td>
</tr>
<tr>
<td>tNetTask</td>
<td>netTask</td>
<td>0x3df1abd0</td>
<td>12240</td>
<td>224</td>
<td>1136</td>
</tr>
<tr>
<td>tTelnetd</td>
<td>telnetd</td>
<td>0x3df1bb90</td>
<td>65488</td>
<td>408</td>
<td>1136</td>
</tr>
<tr>
<td>tNet</td>
<td>SSH_startSer</td>
<td>0x3df68100</td>
<td>65488</td>
<td>424</td>
<td>760</td>
</tr>
<tr>
<td>tFtp6d</td>
<td>0x00000433fc</td>
<td>0x3df1bb90</td>
<td>65488</td>
<td>408</td>
<td>1136</td>
</tr>
<tr>
<td>tBrokerd</td>
<td>brokerd(char)</td>
<td>0x3df24fc0</td>
<td>65488</td>
<td>1648</td>
<td>10920</td>
</tr>
<tr>
<td>tNpFrmRx</td>
<td>app_snd_tas</td>
<td>0x3df47440</td>
<td>20432</td>
<td>348</td>
<td>696</td>
</tr>
<tr>
<td>tNpFrmRx</td>
<td>app_frame_rx</td>
<td>0x3df47820</td>
<td>20432</td>
<td>304</td>
<td>736</td>
</tr>
<tr>
<td>tNpCellRx</td>
<td>app_cell_rx</td>
<td>0x3df47b80</td>
<td>20432</td>
<td>304</td>
<td>376</td>
</tr>
<tr>
<td>tNpDmaTx</td>
<td>app_idma_en</td>
<td>0x3df48140</td>
<td>20432</td>
<td>304</td>
<td>2440</td>
</tr>
<tr>
<td>tNpwbNpmRx</td>
<td>npwbNpmRxTas</td>
<td>0x3df4c840</td>
<td>20432</td>
<td>312</td>
<td>4592</td>
</tr>
<tr>
<td>tIpFrag</td>
<td>0x0001ce1634</td>
<td>0x3df5af40</td>
<td>20432</td>
<td>272</td>
<td>344</td>
</tr>
<tr>
<td>tAlarm</td>
<td>0x0001450910</td>
<td>0x3df66220</td>
<td>40912</td>
<td>336</td>
<td>1376</td>
</tr>
<tr>
<td>tNpDmaRx</td>
<td>app_idma_fra</td>
<td>0x3df47e60</td>
<td>20432</td>
<td>280</td>
<td>2392</td>
</tr>
<tr>
<td>tArpMgr</td>
<td>arp_manager</td>
<td>0x3df5a0c0</td>
<td>20432</td>
<td>336</td>
<td>4968</td>
</tr>
<tr>
<td>tARPd</td>
<td>arp_manager</td>
<td>0x3df5a3a0</td>
<td>20432</td>
<td>304</td>
<td>392</td>
</tr>
<tr>
<td>tPktCapMgr</td>
<td>pktcpt_main</td>
<td>0x3df55b80</td>
<td>20432</td>
<td>344</td>
<td>616</td>
</tr>
<tr>
<td>tFlowGdTmr</td>
<td>npApp_fg_main</td>
<td>0x3df5b320</td>
<td>20432</td>
<td>208</td>
<td>568</td>
</tr>
<tr>
<td>tSysmand</td>
<td>sysmand</td>
<td>0x3df234c0</td>
<td>163792</td>
<td>2968</td>
<td>17880</td>
</tr>
<tr>
<td>tAtcpd</td>
<td>atcpd(char)</td>
<td>0x3df566a0</td>
<td>65488</td>
<td>1928</td>
<td>12488</td>
</tr>
<tr>
<td>tMbcd</td>
<td>mbcd_daemon()</td>
<td>0x3df5ec60</td>
<td>65488</td>
<td>2784</td>
<td>17400</td>
</tr>
<tr>
<td>tEbdmd</td>
<td>ebmd_daemon()</td>
<td>0x3df622c0</td>
<td>65488</td>
<td>3744</td>
<td>15864</td>
</tr>
<tr>
<td>tLid</td>
<td>li_daemon(char)</td>
<td>0x3df5f540</td>
<td>65488</td>
<td>1992</td>
<td>14880</td>
</tr>
<tr>
<td>tAlgD</td>
<td>algd_daemon()</td>
<td>0x3df603a0</td>
<td>65488</td>
<td>2088</td>
<td>15656</td>
</tr>
<tr>
<td>tSipd</td>
<td>sipd(char)</td>
<td>0x3df62e20</td>
<td>98256</td>
<td>2488</td>
<td>17488</td>
</tr>
<tr>
<td>tH323d</td>
<td>h323d(char)</td>
<td>0x3df63980</td>
<td>65488</td>
<td>2360</td>
<td>14720</td>
</tr>
<tr>
<td>tH248d</td>
<td>h248d(char)</td>
<td>0x3df64360</td>
<td>65488</td>
<td>1864</td>
<td>10920</td>
</tr>
<tr>
<td>tRadd</td>
<td>radd(char)</td>
<td>0x3df60d80</td>
<td>65488</td>
<td>1456</td>
<td>12016</td>
</tr>
<tr>
<td>tPusher</td>
<td>pusher(char)</td>
<td>0x3df61960</td>
<td>65488</td>
<td>2096</td>
<td>12656</td>
</tr>
<tr>
<td>tEvtMtrTask</td>
<td>evtMtr</td>
<td>0x3df1c5a0</td>
<td>4048</td>
<td>360</td>
<td>432</td>
</tr>
<tr>
<td>tAndMgr</td>
<td>AND_start</td>
<td>0x3df46100</td>
<td>40912</td>
<td>536</td>
<td>2216</td>
</tr>
<tr>
<td>tSnmpd</td>
<td>snmpd</td>
<td>0x3df64bc0</td>
<td>65488</td>
<td>1360</td>
<td>15216</td>
</tr>
<tr>
<td>tLemd</td>
<td>lemd(char)</td>
<td>0x3df5c940</td>
<td>65488</td>
<td>2448</td>
<td>21592</td>
</tr>
<tr>
<td>tAtcpApp</td>
<td>atcpAppTask()</td>
<td>0x3df5e000</td>
<td>65488</td>
<td>1392</td>
<td>11952</td>
</tr>
<tr>
<td>tDumper</td>
<td>tDumperMain</td>
<td>0x3df241a0</td>
<td>16336</td>
<td>240</td>
<td>600</td>
</tr>
</tbody>
</table>
System Task Suspended Alarm

The following table describes the system task suspended alarm information.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM TASK SUSPENDED</td>
<td>131108</td>
<td>CRITICAL</td>
<td>A Net-Net system task (process) suspends or fails.</td>
<td>Task X suspended, which decremented health by 75% (where X is the task/process name)</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• major dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• reboot (if the Net-Net system is configured to do so)</td>
</tr>
</tbody>
</table>

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            -            -         -            -
```
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 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-Service : 0
Total Length : 76
Identification : 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 provides 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 that 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 ACL1 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 ACLI` 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

```

**Viewing System ACL Statistics**  
You can display statistics for system ACLs using the `show ip stats` ACLI 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
```

 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 link
```
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 system 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 -- -------- Lifetime --------
  Active  High  Total  Total  PerMax  High
```
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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 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 | • 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 
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 Exp 0 0 0
Exp Media Drops 0 0 0

Fault Management
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
```

<table>
<thead>
<tr>
<th>Process Status</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>17</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>47</td>
<td>47</td>
<td>0</td>
<td>81</td>
<td>81</td>
<td>49</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5306</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>5</td>
<td>12365</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>1</td>
<td>5298</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>13</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.547</td>
<td>529790</td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.547</td>
<td>529790</td>
<td></td>
</tr>
</tbody>
</table>

MGCP DNS Failure Alarm

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

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGCP ALARM DNS FAILURE</td>
<td>327683</td>
<td>WARNING</td>
<td>Cannot authenticate the RSIP and need to drop the packet.</td>
<td>Endpoint &lt;endpoint&gt; from source &lt;sourceHostname&gt; could not be authenticated.</td>
<td>• apSyslogMessageGenerated trap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• critical dry contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
</tbody>
</table>

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 ntfy and press <Enter>.

```
ACMEPACKET# show algd ntfy
```

### 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 ....

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Offer Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SDP Answer Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Media Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Application Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Exp Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Early Media Exps</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Exp Media Drops</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Expired Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multiple OK Drops</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multiple OK Terms</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Failure Drops</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Non-ACK 2xx Drops</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Invalid Requests</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Invalid Responses</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Invalid Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAC Session Drop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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                5                  5                  5
High                  5                  6                  3
Total                 0                  0                  0
PerMax                0                  0                  0
High                  0                  0                  0
Services              5                  5                  5
Messages              0                  0                  0
Transactions          0                  0                  0
Timed Objects         7                  14                 11
Total Buffers         5                  5                  5
Alloc Buffers         3                  7                  4
Memory Chunks         48                 82                 79
TOQ Entries           2                  58301              19
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                8.133/529935
CPU Usage             0.0
```

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:

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
- **Refreshe**—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:
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
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**

```
Session Stats

-------- Lifetime --------
Current Total PerMax
Inbound Sessions          0   0   0
Per RValue Stats

-------- Lifetime --------
Active High Total Total PerMax High
RValue = ets.2
Incoming Sessions          0   0   0          0   0   0
Outgoing Sessions          0   0   0          0   0   0
InbSessions Rej            -   -   0          0   0   -
OutbSessions Rej           -   -   0          0   0   -

RValue = ets.5
Incoming Sessions          0   0   0          0   0   0
Outgoing Sessions          0   0   0          0   0   0
InbSessions Rej            -   -   0          0   0   -
OutbSessions 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 Lifetime High
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 NOTIFY

   NOTIFY (15:53:42-57)

   MESSAGE/EVENT               RECENT     TOTAL     PERMAX    RECENT     TOTAL     PERMAX
   ---------------------------------------------------------------------------------------
   NOTIFY Requests             0          49         19         0          0         0
   Retransmissions            0          0          0          0          0         0
   100 Trying                 0          49         19         0          0         0
   180 Ringing                0          38         19         0          0         0
   200 OK                     0          38         19         0          0         0
   503 Service Unavail        0          11         11         0          0         0
   Response Retrans           0          9          5          0          0         0
   Transaction Timeouts       -          -          -          0          0         0
   Locally Throttled          -          -          -          0         24         24

   Avg Latency=0.000 for 0
   Max Latency=0.000
   BurstRate Incoming=11 Outgoing=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 NOTIFY

   NOTIFY (15:53:42-57)

   MESSAGE/EVENT               RECENT     TOTAL     PERMAX    RECENT     TOTAL     PERMAX
   ---------------------------------------------------------------------------------------
   NOTIFY Requests             0          50         31         0          0         0
   Retransmissions            0          3          3          0          0         0
   200 OK                     0          25         18         0          0         0
   503 Service Unavail        0          25         24         0          0         0
   Transaction Timeouts       -          -          -          0          0         0
   Locally Throttled          -          -          -          0         24         24

   Avg Latency=0.000 for 0
   Max Latency=0.000
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 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
```

Viewing SIP PUBLISH Statistics

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

```
summer# show sipd publish
PUBLISH (10:26:43.199)

Message/Event          Recent  Total  PerMax  Recent  Total  PerMax
------------           -------  ------  -------  -------  ------  -------
PUBLISH Requests       1       1       1       0       0       0
Retransmissions       0       0       0       0       0       0
405 Not Allowed       1       1       1       0       0       0
Transaction Timeouts  -       -       -       0       0       0
Locally Throttled     -       -       -       0       0       0
```

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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Display</td>
<td>General accounting setup (as established in the accounting configuration element), including:</td>
</tr>
<tr>
<td></td>
<td>• Information about the state of the RADIUS client</td>
</tr>
<tr>
<td></td>
<td>• Accounting strategy used (Hunt, Failover, RoundRobin, FastestRTT, or FewestPending)</td>
</tr>
<tr>
<td></td>
<td>• IP address and port on which the Net-Net server is listening</td>
</tr>
<tr>
<td></td>
<td>• Maximum message delay in seconds</td>
</tr>
<tr>
<td></td>
<td>• Number of configured accounting servers</td>
</tr>
<tr>
<td>Waiting Queue</td>
<td>Amount of accounting (RADIUS) messages waiting to be sent.</td>
</tr>
<tr>
<td></td>
<td>Waiting queue capacity is 4,096 messages.</td>
</tr>
<tr>
<td>&lt;IP Address:Port&gt;</td>
<td>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_Atmpt, INIT).</td>
</tr>
</tbody>
</table>

• 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
    AccessRe transmissions    : 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
    AccessRe transmissions    : 9
    AccessAccepts            : 0
    Timeouts                 : 10
    AccessRejects            : 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

..............................................................
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
..............................................................
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

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

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
</table>
| RADIUS ACCOUNTING CONNECTION DOWN | 327681   | CRITICAL       | 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. | • 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 an IP address and realm ID is denied of service, it 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:vlan 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
```

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:vlan 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
```
ACMEPACKET# show acl trusted
trusted entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask prot type
index recv drop
Total number of trusted entries = 0
Trusted Entries not allocated due to ACL constraints: 0

ACMEPACKET# show acl all
deny entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask prot type
index
Total number of deny entries = 0

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

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:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask prot type
index
Total number of deny entries = 0

trusted entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask prot type
index recv drop
Total number of trusted 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:

<table>
<thead>
<tr>
<th></th>
<th># of entries</th>
<th>% utilization</th>
<th>Reserved Entry Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denied</td>
<td>0</td>
<td>0.0%</td>
<td>200</td>
</tr>
<tr>
<td>Trusted</td>
<td>0</td>
<td>0.0%</td>
<td>200</td>
</tr>
<tr>
<td>Media</td>
<td>0</td>
<td>0.0%</td>
<td>3884</td>
</tr>
<tr>
<td>Untrusted</td>
<td>0</td>
<td>0.0%</td>
<td>100</td>
</tr>
</tbody>
</table>
```

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

---

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
```
### Fault Management

**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

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Exceeded</td>
<td>0</td>
</tr>
<tr>
<td>Num Exceeded</td>
<td>0</td>
</tr>
<tr>
<td>Reg Rate Exceeded</td>
<td>0</td>
</tr>
</tbody>
</table>

### Outbound Sessions

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Exceeded</td>
<td>0</td>
</tr>
<tr>
<td>Num Exceeded</td>
<td>0</td>
</tr>
<tr>
<td>Reg Rate Exceeded</td>
<td>0</td>
</tr>
</tbody>
</table>

### Trans Timeout

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>40928</td>
</tr>
</tbody>
</table>

### Requests Sent

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>519695</td>
</tr>
</tbody>
</table>

### Requests Complete

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>478367</td>
</tr>
</tbody>
</table>

### Seizure

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>239762</td>
</tr>
</tbody>
</table>

### Answer

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>234661</td>
</tr>
</tbody>
</table>

### ASR Exceeded

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

### Messages Received

<table>
<thead>
<tr>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1431343</td>
</tr>
</tbody>
</table>

**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 outbound 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
recursion         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:              recursion
11:00:07-32
----- Inbound -----  ---- Outbound ----- -- Latency --
Session 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
150.150.150.35    I     0   0.0      0       1   0.0      0  0.000  0.000     1
SAG:              recursion
150.150.150.16    I     0   0.0      0       0   0.0      0  0.005  0.005     1
SAG:              recursion
150.150.150.35    I     0   0.0      0       1   0.0      0  0.000  0.000     1
Totals:          recursion
11:00:21-16
----- Inbound -----  ---- Outbound ----- -- Latency --
SAG              Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max
recursion         I     0   0.0      0       1   0.1      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:
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.
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  1     11     11     11
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# show h323 agentconfig
session-agent
    hostname test hostname.com
    ip-address 192.168.200.13
```
<table>
<thead>
<tr>
<th>Port</th>
<th>5060</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>enabled</td>
</tr>
<tr>
<td>App-Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>App-Type</td>
<td>H323-GW</td>
</tr>
<tr>
<td>Transport-Method</td>
<td>UDP</td>
</tr>
<tr>
<td>Realm-ID</td>
<td>h323192</td>
</tr>
</tbody>
</table>

**Description**

**Carriers**

- Allow-Next-Hop-LP: enabled
- Constraints: disabled

**Max Sessions**

- 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
- redirect-action: enabled
- loose-routing: enabled
- send-media-session: enabled
- response-map

**Ping Method**

- ping-method: 0
- ping-interval: 0
- ping-in-service-response-codes
- ping-out-service-response-codes
- media-profiles
- in-translationid
- out-translationid
- trust-me: disabled
- request-uri-headers
- stop-recurse
- local-response-map
- ping-to-user-part
- ping-from-user-part
- li-trust-me: disabled
- in-manipulationid
- out-manipulationid
- p-asserted-id
- trunk-group

**Max Register-Sustain-Rate**

- max-register-sustain-rate: 0

**Early Media Allow**

- early-media-allow: 0
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 -----  ---- Outbound ----- -- Latency -- ------- Max -------
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                 testhostname.com
hostname                       testhostname.com
ip-address                     5060
port                           SIP
state                          enabled
app-protocol                   SIP
app-type                       UDP
realm-id                       description
carriers                       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                     None
```
### Viewing H.323 Session Agent Group Configuration
Display information about the session agent group configuration by using the `show h323d groupconfig` command. For example:

ACMEPACKET# show h323d groupconfig

<table>
<thead>
<tr>
<th>session-group</th>
<th>group-name</th>
<th>description</th>
<th>state</th>
<th>app-protocol</th>
<th>strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323Group</td>
<td>h323</td>
<td></td>
<td>enabled</td>
<td>H323</td>
<td>Hunt</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>SAG</th>
<th>Active Rate</th>
<th>ConEx</th>
<th>Active Rate</th>
<th>ConEx</th>
<th>Avg</th>
<th>Max</th>
<th>InBurst</th>
<th>OutBurst</th>
</tr>
</thead>
<tbody>
<tr>
<td>H323Group</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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 ---- Inbound ----- ---- Outbound ----- -- Latency -- ------- Max -------
Realm        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 --- Steering Ports --- ----------- Bandwidth Usage -----------
Realm         Used   Free  No Ports    Flows Ingrss Egress Total Insuf BW
acme             0      0         0        0     0K     0K     0K         0
h323172          0  30001         0        0     0K     0K     0K         0
sip172           2  29999         0        0     0K     0K     0K         0
sip192           2  29999         0        0     0K     0K     0K         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
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.

### Viewing MBCD Statistics for a Specific Realm

- **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

For example:

```plaintext
acmePacket# show mbcd realms sip172
18:47:31.2881 Realm=sip172

<table>
<thead>
<tr>
<th></th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PerMax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ports Used</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>Free Ports</td>
<td>29999</td>
<td>30017</td>
</tr>
<tr>
<td>No Ports Avail</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Ingress Band</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>Egress Band</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>BW Allocations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Band Not Avail</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Total Bandwidth</td>
<td>OK</td>
<td>0</td>
</tr>
</tbody>
</table>

Steering Ports: 100% Success
Viewing MBCD Task Errors

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

For example:

```
ACMEPACKET# show mbcd errors
11:42:37-198
MBC Errors/Events                ---- Lifetime ----
                                      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 Notify Failed                   0       0       0
Unacknowledged Notify               0       0       0
Invalid Realm                       0       0       0
No Ports Available                  0       0       0
Insufficient Bandwidth              0       0       0
Stale Ports Reclaimed               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
-- Period -- ------- Lifetime -------
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 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
realm1 10 10 0 0 0

Media Alarms
The following table lists information about the different media alarms.

Table 1:

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBCD ALARM OUT OF MEMORY</td>
<td>262145</td>
<td>CRITICAL</td>
<td>No further memory can be allocated for MBCD.</td>
<td>Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.</td>
<td>apSyslogMessageGenerated, apSysMgmtMediaOutofMemory trap generated</td>
</tr>
<tr>
<td>MBCD ALARM INTERNAL</td>
<td>262146</td>
<td>MINOR</td>
<td>An internal software error.</td>
<td>Internal Error. No agent for socket &lt;IPPort&gt;.</td>
<td>None</td>
</tr>
<tr>
<td>MBCD ALARM UNKNOWN REALM</td>
<td>262147</td>
<td>MAJOR</td>
<td>Media server is unable to find realm interface.</td>
<td>Realm type (ingress, egress, hairpin) X, not found</td>
<td>apSyslogMessageGenerated, apSysMgmtUnknownRealm</td>
</tr>
<tr>
<td>MBCD ALARM OUT OF BANDWIDTH</td>
<td>262149</td>
<td>CRITICAL</td>
<td>The realm is out of bandwidth.</td>
<td>Out of bandwidth</td>
<td>apSyslogMessageGenerated, apSysMgmtMediaBandwidth Trap</td>
</tr>
<tr>
<td>MBCD ALARM OUT OF PORTS</td>
<td>262150</td>
<td>CRITICAL</td>
<td>The realm is out of steering ports.</td>
<td>Out of steering ports</td>
<td>apSyslogMessageGenerated, apSysMgmtMediaPortsTrap</td>
</tr>
</tbody>
</table>

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:vlan 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.

- **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>`

---

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

**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
```

120 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide  Version S-C6.2.0
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

Viewing NAT Information In Tabular

acmepacket# show nat in-tabular

<table>
<thead>
<tr>
<th>NAT</th>
<th>SA_key</th>
<th>DA_key</th>
<th>SP_key</th>
<th>DP_key</th>
<th>VLAN_key</th>
</tr>
</thead>
<tbody>
<tr>
<td>ING</td>
<td>PROTO</td>
<td>WEIGHT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0xac100056, dip=0x00000000, SP=0x0000, DP=0x0000, VLAN=0, intf=64, proto=0, weight=0x10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0x7f000064, dip=0x00000000, SP=0x0000, DP=0x0000, VLAN=999, intf=64, proto=0, weight=0x10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0000, VLAN=0, intf=6, proto=6, weight=0x9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0000, VLAN=0, intf=6, proto=17, weight=0x9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0x00000000, dip=0x7f000064, SP=0x0000, DP=0x13c4, VLAN=999, intf=0, proto=17, weight=0xd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addr</td>
<td>sip=0x00000000, dip=0xac100058, SP=0x0000, DP=0x13c4, VLAN=0, intf=0, proto=17, weight=0xd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 Info

<table>
<thead>
<tr>
<th>IFD Index</th>
<th>IFD Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00034000</td>
<td>Static = No</td>
</tr>
<tr>
<td></td>
<td>Word 0 = Valid, Word 1 = Valid</td>
</tr>
<tr>
<td></td>
<td>Enabled for CPU Traffic = Yes</td>
</tr>
<tr>
<td></td>
<td>ABJ Mode = Enabled,</td>
</tr>
<tr>
<td></td>
<td>EPD Mode = Disabled</td>
</tr>
<tr>
<td></td>
<td>Enabled for Data Traffic = Yes</td>
</tr>
<tr>
<td></td>
<td>IFD enabled = Disabled,</td>
</tr>
<tr>
<td></td>
<td>IFD assigned = Unassigned</td>
</tr>
<tr>
<td></td>
<td>IQD Assigned = No</td>
</tr>
<tr>
<td></td>
<td>Thresholding Enabled,</td>
</tr>
<tr>
<td></td>
<td>TG Index = 0x0</td>
</tr>
<tr>
<td></td>
<td>WRED Disabled.</td>
</tr>
</tbody>
</table>

## OFD Index Info

<table>
<thead>
<tr>
<th>OFD Index</th>
<th>Oft Dest ID Queue Index Scheduling Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00034000</td>
<td>0x00034000 0x00000000 0x00000000 0x00000001</td>
</tr>
<tr>
<td></td>
<td>Word 0 = Valid,</td>
</tr>
<tr>
<td></td>
<td>Word 1 = Valid</td>
</tr>
<tr>
<td></td>
<td>Word 2 = Valid,</td>
</tr>
<tr>
<td></td>
<td>Word 3 = Valid</td>
</tr>
<tr>
<td></td>
<td>Packet Mode = Yes</td>
</tr>
<tr>
<td></td>
<td>SPWRR Parameters</td>
</tr>
<tr>
<td></td>
<td>Delta = 0x000000000001</td>
</tr>
<tr>
<td></td>
<td>Credit Min Exponent = 0x0000000</td>
</tr>
<tr>
<td></td>
<td>Pipe Index Pipe Scheduler Parameters</td>
</tr>
<tr>
<td></td>
<td>0x00008000</td>
</tr>
<tr>
<td></td>
<td>Packet Max Mode Set = Enabled</td>
</tr>
<tr>
<td></td>
<td>Delta = 0x000000000007</td>
</tr>
<tr>
<td></td>
<td>Credit Min Exponent = 0x0000000000000000</td>
</tr>
<tr>
<td></td>
<td>Credit Min Mantissa = 0x0000000000000000</td>
</tr>
<tr>
<td></td>
<td>Credit Max Exponent = 0x00000000000000007</td>
</tr>
<tr>
<td></td>
<td>Credit Max Mantissa = 0x0000000000000018</td>
</tr>
<tr>
<td></td>
<td>Total Dropped = 0x0</td>
</tr>
<tr>
<td></td>
<td>Total Received = 0x5</td>
</tr>
</tbody>
</table>

## SA_prefix Info

<table>
<thead>
<tr>
<th>SA_prefix</th>
<th>01.000.011.012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol flow_key</td>
<td>6</td>
</tr>
<tr>
<td>Ingress flow_key</td>
<td>0</td>
</tr>
<tr>
<td>Ingress slot</td>
<td>0</td>
</tr>
<tr>
<td>Ingress port</td>
<td>0</td>
</tr>
<tr>
<td>VLAN flow_key</td>
<td>0</td>
</tr>
<tr>
<td>Protocol flow_key</td>
<td>0</td>
</tr>
<tr>
<td>SA_prefix</td>
<td>01.000.011.012</td>
</tr>
<tr>
<td>DA prefix</td>
<td>32</td>
</tr>
<tr>
<td>SP prefix</td>
<td>16</td>
</tr>
<tr>
<td>DP prefix</td>
<td>0</td>
</tr>
<tr>
<td>VLAN_prefix</td>
<td>0</td>
</tr>
<tr>
<td>Protocol flow_key</td>
<td>6</td>
</tr>
<tr>
<td>Ingress_flow_key</td>
<td>0</td>
</tr>
<tr>
<td>Ingress_slot</td>
<td>0</td>
</tr>
<tr>
<td>Ingress_port</td>
<td>0</td>
</tr>
<tr>
<td>XSA data_entry</td>
<td>000.000.000.000</td>
</tr>
<tr>
<td>XDA data_entry</td>
<td>192.168.050.001</td>
</tr>
<tr>
<td>XSP data_entry</td>
<td>0</td>
</tr>
<tr>
<td>XDP data_entry</td>
<td>0</td>
</tr>
<tr>
<td>Egress data_entry</td>
<td>0</td>
</tr>
<tr>
<td>Egress slot</td>
<td>0</td>
</tr>
</tbody>
</table>
### IFD Index Information

<table>
<thead>
<tr>
<th>IFD Index</th>
<th>IFD Info</th>
<th>Input Admission Params</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000002</td>
<td>Static = No</td>
<td>Word 0 = Valid, Word 1 = Valid</td>
</tr>
</tbody>
</table>

- **EPD Mode**: Disabled
- **IFD enabled for CPU Traffic**: Yes
- **ABJ Mode**: Enabled
- **IFD enabled for Data Traffic**: Yes
- **Thresholding Enabled**: Yes
- **IQD Assigned**: No
- **TG Index**: 0x0
- **WRED**: Disabled.

### OFD Index Information

<table>
<thead>
<tr>
<th>OFD Index</th>
<th>Oft</th>
<th>DestID</th>
<th>QueueIndex</th>
<th>Scheduling Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00004002</td>
<td>0x00004002</td>
<td>0x00000000</td>
<td>0x00000001</td>
<td>Word 0 = Valid, Word 1 = Valid</td>
</tr>
</tbody>
</table>

- **Word 2 = Valid, Word 3 = Valid**
- **Word 4 = Invalid**
- **Packet Mode**: Yes
- **Shaping Parameters**:
  - **Sustained Cell Rate Exp**: 0x00000005
  - **Sustained Cell Rate Mantissa**: 0x000000e8
  - **Peak Cell Rate Exp**: 0x00000000
  - **Peak Cell Rate Mantissa**: 0x00000000
  - **Max Burst Threshold Exp**: 0x00000000
  - **Max Burst Threshold Mantissa**: 0x00000000
- **Latency Sensitive**: Disabled
**Pipe Index**  
Pipe Scheduler Parameters  
0x00008000  
Packet Max Mode Set = Enabled  
Delta = 0x00000001  
mtick = 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:

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
</table>
| NAT TABLE UTILIZATION       | 131102  | MINOR          | NAT table usage reached 90% or greater of its capacity. | NAT table usage X% over threshold X% | 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
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 timestamp 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
```
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.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GATEWAY UNREACHABLE</td>
<td>dynamicID</td>
<td>MAJOR</td>
<td>The Net-Net SBC lost ARP connectivity to the front interface gateway.</td>
<td>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)</td>
<td>• apSysMgmtGatewayUnreachableTrap generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• syslog</td>
</tr>
</tbody>
</table>

The value of this alarm changes based on a number of factors. The total alarm ID range falls between 196608 and 262143. 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 0xffffff00 Subnetmask 0xffffff00
  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 0xffffffff Subnetmask 0xffffffff
  Metric is 0
  Maximum Transfer Unit size is 32768
```
69 packets received; 69 packets sent
0 multicast packets received
0 multicast 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 MULTICAST TRAILERS ARP RUNNING INET_UP
  Type: SOFTWARE_LOOPBACK
  inet: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  inet6: ::1 prefixlen 128
  Maximum Transfer Unit size is 1536
  198 packets received; 198 packets sent
  0 multicast packets received
  0 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
eth (unit number 0):
  Flags: (0x78843) UP BROADCAST MULTICAST ARP RUNNING INET_UP
  Type: ETHERNET_CSMACD
  inet: 172.30.1.186
  Broadcast address: 172.30.255.255
  Netmask 0xffff0000 Subnetmask 0xffff0000
  Ethernet address is 00:08:25:a0:78:50
  Maximum Transfer Unit size is 1500
  123096284 octets received
  12747 octets sent
  23 unicast packets received
  198 unicast packets sent
  96295 multicast packets received
  0 multicast 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
sp (unit number 0):
  Flags: (0x68043) UP BROADCAST MULTICAST ARP RUNNING INET_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 protos
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: 0xffffffff
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: 0xffffffff
Gateway: 0.0.0.0
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:
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

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Vlan</th>
<th>IPAddress</th>
<th>Mask</th>
<th>Gateway Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0:</td>
<td>4</td>
<td>192.168.200</td>
<td>10 255.255.255</td>
<td>0 192.168.200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>192.168.200</td>
<td>10 255.255.255</td>
<td>0 192.168.200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/3:</td>
<td>0</td>
<td>63.67.143.8</td>
<td>8 255.255.255</td>
<td>0 63.67.143.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Viewing Physical Interface Statistics**

ACMEPACKET# show media physical

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>MAC Address</th>
<th>Encap</th>
<th>Connection ID</th>
<th>Frames Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1:</td>
<td>0: 8:25:1: 0:53</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
<tr>
<td>2/3:</td>
<td>0: 8:25:1: 0:54</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

**Viewing Front Interface Physical Level Statistics**

ACMEPACKET# show media phy-stats 0 0

*** RECEIVE STATISTICS ***

<table>
<thead>
<tr>
<th>Statistics Counter Name</th>
<th>Count (hex)</th>
<th>Count (decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx bytes recd - Upper 32 bits</td>
<td>0x0000</td>
<td>0x002E</td>
</tr>
<tr>
<td>Rx bytes recd - Lower 32 bits</td>
<td>0x8132</td>
<td>0x6E69</td>
</tr>
<tr>
<td>Rx 64 (Bad + Good)</td>
<td>0x0005</td>
<td>0x3392</td>
</tr>
<tr>
<td>Rx 65 to 127 (Bad + Good)</td>
<td>0x006F</td>
<td>0x6F88</td>
</tr>
<tr>
<td>Rx 128 to 255 (Bad + Good)</td>
<td>0x368A</td>
<td>0x844C</td>
</tr>
<tr>
<td>Rx 256 to 511 (Bad + Good)</td>
<td>0x0004</td>
<td>0x531C</td>
</tr>
<tr>
<td>Rx 512 to 1023 (Bad + Good)</td>
<td>0x0000</td>
<td>0x02D0</td>
</tr>
<tr>
<td>Rx 1024 to 1518 (Bad + Good)</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx 1519 to 1530 (Bad + Good)</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx &gt; 1530 (Good)</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx Error Oversized &gt; 1530</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx Good Undersized &lt; 64</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx Error Undersized &lt; 64</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
<tr>
<td>Rx Unicast Frames In (Good)</td>
<td>0x3732</td>
<td>0x8CF4</td>
</tr>
<tr>
<td>Rx Multicast Frames In (Good)</td>
<td>0x0000</td>
<td>0x93A2</td>
</tr>
<tr>
<td>Rx Broadcast Frames In (Good)</td>
<td>0x0000</td>
<td>0x5C8B</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm ID</th>
<th>Alarm Severity</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINK UP ALARM GIGPORT</td>
<td>131073</td>
<td>MINOR</td>
<td>Gigabit Ethernet interface 1 goes up.</td>
<td>Slot 1 port 0 UP</td>
<td>• linkup trap generated • syslog</td>
</tr>
<tr>
<td>LINK UP ALARM GIGPORT</td>
<td>131074</td>
<td>MINOR</td>
<td>Gigabit Ethernet interface 2 goes up.</td>
<td>Slot 2 port 0 UP</td>
<td>• linkup trap generated • syslog</td>
</tr>
</tbody>
</table>
FAULT MANAGEMENT

Link Down Alarm

**GIGPORT**
- Gigabit Ethernet interface 1 goes down.
- Slot 1 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

**GIGPORT**
- Gigabit Ethernet interface 2 goes down.
- Slot 2 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

**VXINTF**
- Control interface 0 goes up.
- Port 0 Up
- LinkUp trap generated
- syslog

**VXINTF**
- Control interface 1 goes up.
- Port 1 Up
- LinkUp trap generated
- syslog

**VXINTF**
- Control interface 2 goes up.
- Port 2 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 1, port 0 goes down.
- Slot 1 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

**FEPORT**
- Fast Ethernet slot 2, port 0 goes down.
- Slot 2 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

**FEPORT**
- Fast Ethernet slot 1, port 1 goes up.
- Slot 1 port 1 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 2, port 1 goes up.
- Slot 2 port 1 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 1, port 2 goes up.
- Slot 1 port 2 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 2, port 2 goes up.
- Slot 2 port 2 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 1, port 3 goes up.
- Slot 1 port 3 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 2, port 3 goes up.
- Slot 2 port 3 Up
- LinkUp trap generated
- syslog

**FEPORT**
- Fast Ethernet slot 1, port 0 goes down.
- Slot 1 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

**FEPORT**
- Fast Ethernet slot 2, port 0 goes down.
- Slot 2 port 0 Down
- LinkDown trap generated
- minor dry contact
- syslog

---

**Alarm Name** | **Alarm ID** | **Alarm Severity** | **Cause(s)** | **Example Log** | **Actions**
--- | --- | --- | --- | --- | ---
**LINK DOWN ALARM VXINTF** | 131080 | MAJOR | Control interface 0 goes down. | Port 0 DOWN | LinkDown trap generated
 | 131081 | MAJOR | Control interface 1 goes down. | Port 1 DOWN | LinkDown trap generated
 | 131082 | MAJOR | Control interface 2 goes down. | Port 2 DOWN | LinkDown trap generated
 | 131083 | MAJOR | Fast Ethernet slot 1, port 0 goes up. | Slot 1 port 0 UP | LinkUp trap generated
 | 131084 | MAJOR | Fast Ethernet slot 2, port 0 goes up. | Slot 2 port 0 UP | LinkUp trap generated
 | 131085 | MINOR | Fast Ethernet slot 1, port 1 goes up. | Slot 1 port 1 UP | LinkUp trap generated
 | 131086 | MINOR | Fast Ethernet slot 2, port 1 goes up. | Slot 2 port 1 UP | LinkUp trap generated
 | 131087 | MINOR | Fast Ethernet slot 1, port 2 goes up. | Slot 1 port 2 UP | LinkUp trap generated
 | 131088 | MINOR | Fast Ethernet slot 2, port 2 goes up. | Slot 2 port 2 UP | LinkUp trap generated
 | 131089 | MINOR | Fast Ethernet slot 1, port 3 goes up. | Slot 1 port 3 UP | LinkUp trap generated
 | 131090 | MINOR | Fast Ethernet slot 2, port 3 goes up. | Slot 2 port 3 UP | LinkUp trap generated
 | 131091 | MAJOR | Fast Ethernet slot 1, port 0 goes down. | Slot 1 port 0 DOWN | LinkDown trap generated
 | 131092 | MAJOR | Fast Ethernet slot 2, port 0 goes down. | Slot 2 port 0 DOWN | LinkDown trap generated

T34 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide Version S-C6.2.0
<table>
<thead>
<tr>
<th>ALARM</th>
<th>CODE</th>
<th>LEVEL</th>
<th>DESCRIPTION</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| FEPORT | 131093| MAJOR | Fast Ethernet slot 1, port 1 goes down. | • linkDown trap generated  
• minor dry contact  
• syslog |
| FEPORT | 131094| MAJOR | Fast Ethernet slot 2, port 1 goes down. | • linkDown trap generated  
• minor dry contact  
• syslog |
| FEPORT | 131095| MAJOR | Fast Ethernet slot 1, port 2 goes down. | • linkDown trap generated  
• minor dry contact  
• syslog |
| FEPORT | 131096| MAJOR | Fast Ethernet slot 2, port 2 goes down. | • 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
```

Specify 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:**

1. 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
1
```

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.sipp.com
Query-->  Q: A abc.sipp.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.

<table>
<thead>
<tr>
<th>Data Group</th>
<th>Included Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>General System Commands</td>
<td>• show clock&lt;br&gt;• show version image&lt;br&gt;• show version boot&lt;br&gt;• show prom-info all&lt;br&gt;• display-alarms&lt;br&gt;• show uptime&lt;br&gt;• show process&lt;br&gt;• show arp&lt;br&gt;• show sessions&lt;br&gt;• show features&lt;br&gt;• show memory&lt;br&gt;• show buffer&lt;br&gt;• show health&lt;br&gt;• show running-config</td>
</tr>
<tr>
<td>Physical Interface Commands</td>
<td>• show interface&lt;br&gt;• show media physical&lt;br&gt;• show media phy-stats&lt;br&gt;• show media host-stats&lt;br&gt;• show media classify&lt;br&gt;• show media network&lt;br&gt;• show media frame-stats&lt;br&gt;• show media tm-stats</td>
</tr>
<tr>
<td>SIP Commands</td>
<td>• show reg&lt;br&gt;• show sipd all&lt;br&gt;• show sipd agent&lt;br&gt;• stack sipd</td>
</tr>
<tr>
<td>H323 Commands</td>
<td>• show h323&lt;br&gt;• show h323 h323stats&lt;br&gt;• show h323 agentstats&lt;br&gt;• show h323 stackCallstats&lt;br&gt;• show h323 stackPvtStats&lt;br&gt;• show h323 stackDisconnectInstate&lt;br&gt;• show h323 stacklist&lt;br&gt;• stack h323d</td>
</tr>
<tr>
<td>MGCP Commands</td>
<td>• show algd all&lt;br&gt;• show algd rsip&lt;br&gt;• show algd errors&lt;br&gt;• stack algd</td>
</tr>
<tr>
<td>Call Media Commands</td>
<td>• show mbcd all&lt;br&gt;• show mbcd realms&lt;br&gt;• stack mbcd</td>
</tr>
</tbody>
</table>

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> binary`

       **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> dir`
   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          I     0   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 -- -------- 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       -
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
You can add the `detail` argument to view this command’s output with detailed information:

```plaintext
ACMEPACKET> show registration sipd by-user user@acme.com detail
```

```
Registration Cache (Detailed View)       TUE JUL 11:32:21 UTC 2007
User: sip:user@acme.com

Contact Information:
Contact Name: sip: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: sip:user-acc-m2vmeht2n09kb@127.0.0.15:5060;transport=udp
Realm: access, IP: 172.30.80.4:5060
SD Contact: sip:user-p3rrurjvp0lvf@127.0.0.10:5060
Realm: backbone

ACMEPACKET>
```

The following is a sample of the `show registration sipd by-realm` command’s output:

```plaintext
ACMEPACKET# show registration sipd by-realm access
```

```
Registration Cache             WED JUN 25 2008  09:12:03
Realm         User                             Registered at
--------------- -------------------------------- ------------------
access         sip:16172345687@192.168.12.200              2008-06-25-09:00:32
access         sip: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 sip:16172345687@192.168.12.200 2008-06-25-09:00:32
0.0.0.0 sip: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-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 sip:3397654323@192.168.12.200 2008-06-25-09:00:40

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):
```

Version S-C6.2.0
Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide 145
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.

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:aain/*@mtal.cablelabs.com
Registration Cache                               WED MAR 17:58:01 2007
```
You can add the `detail` argument to view this command’s output with detailed information:

```
ACMEPACKET# show registration mgcp by-endpoint mgcp-150:aaln/1@mta1.cablelabs.com detail
```

```
Registration Cache (Detailed View) THU JUN 14:03:42 2007

Endpoint: mgcp-150:aaln/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:aaln/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: aaln/1

External Key: mgcp-150:mta1.cablelabs.com
Name Format: aaln/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 an 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 iwft 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 iwft 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.

```plaintext
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) SD0d9601-05d11dd13301cad1523806354168b28b-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=5D6d9601-113783f0-1d0010ac-13c4-12557b-426bb44b-12557b
  To-URI              <sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SD0d9699-0000012000088798
  Contact-URI        <sip:1180000@127.0.0.100:5060;transport=UDP>
```

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.

```plaintext
ACMEPACKET# show h323d sessions all

Displaying Sessions 'all' expression ''
This may take up to 30 seconds

CallID(S) SD0d9601-05d11dd13301cad1523806354168b28b-v3000i1 ()
CallID(C) 80834d3a4200001f0110090e2f3cc51b
IWF Call Leg is SERVER
From (Server)
```
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 sipd sessions by-agent 127.0.0.11

Displaying Sessions 'by-agent' expression '127.0.0.11'
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>
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=113783f0-1d0010ac-13c4-12557b-426bb44b-12557b
To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SD06d9699-0000012000088798
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=SD06d9699-113783f0-1d0010ac-13c4-12557b-426bb44b-12557b
To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=0000012000088798
Contact-URI <sip:2180000@127.0.0.11:5060;transport=UDP>
```

Displayed 1 out of total of 1 Sessions (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 sessions by-agent 192.168.200.29

Displaying Sessions 'by-agent' expression '192.168.200.29'
```

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-callId A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192.168.11.101
```

This may take up to 30 seconds

```
<call-id>                     Call-Id
< sessions by-callId A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192.168.11.101

Displaying Sessions 'by-callId' expression '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"<sip:333@192.168.12.200:5060>;tag=43629539029921
  To-URI <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
  Contact-URI <sip:333@192.168.11.101:5060>
To (Client)
  Realm core
  From-URI "poza"<sip:333@192.168.12.200:5060>;tag=43629539029921
  To-URI <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
  Contact-URI <sip:1234-dcgvufb35n8e8@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"<sip:333@192.168.12.200:5060>;tag=43629539029921
  To-URI <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
  Contact-URI <sip:333-3sd0uq3ad3a65@192.168.12.100:5060;transport=udp>
```
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)  SDpmd9601-8a9346384f02a41972cf4e65d7692be-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-13c4-12568b-3ce7f7a6-12568b
  To-URI      <sip:1180000@127.0.0.100;5060;transport=UDP>;tag=SDpmd9699-000022c000a0e38
  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=SDpmd9601-113783f0-1d0010ac-13c4-12568b-3ce7f7a6-12568b
  To-URI      <sip:1180000@192.168.200.29:1720;acme_sa=192.168.200.29;acme_realm=acme_real m=acme_iwf_iftrusted>;tag=0000022c000a0e38
  Contact-URI <sip:1180000@127.0.0.1:5070;acme_sa=192.168.200.29;acme_realm=acme_iwf_iftrusted>
Clear Call [y/n]? y
*** Call Cleared ***

Clear 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

Cal ID(S)  SD70bp801-c3ab2f185aa73aca37d1fc619ec16a2f-v3000i11 ()
Cal ID(C)  c080c5f0c600001f0112090e2f3cc51b
IWF Call Leg is = SERVER
From (Server)
  Realm
  From-URI
  <sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SD70bp801-1138cd28-1d0b10ac-13c4-1257b5-1a5eebc4-1257b5
  To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
To (Client)
  Realm
  From-URI
  <sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SD70bp801-1138cd28-1d0b10ac-13c4-1257b5-1a5eebc4-1257b5
  To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
Clear Call [y/n]?: y
*** Call Cleared ***

Retrying the command

Cleared 1 Sessions

ACMEPACKET#
3 Performance Management

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
alloc     211642160  3398   62284        -
internal  448         2   224        -
cumulative
alloc     212286912  5105  41584        -
peak
alloc     211643792   -    -        -
```

Memory Errors:

- Links Repaired: 0
- Padding Modified: 0
- Nodes Removed: 0
- Removal Failures: 0
- Fatal Errors: 0

**Listing Memory Subcommands**

You can access a list of available `show memory` subcommands.

```
ACMEPACKET# show memory ?
application   application memory usage statistics
l2            layer 2 cache status
l3            layer 3 cache status
usage         memory usage statistics
```
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
```

<table>
<thead>
<tr>
<th>Memory Statistics</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>27</td>
<td>27</td>
<td>0</td>
<td>29</td>
<td>28</td>
<td>27</td>
</tr>
<tr>
<td>Messages</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>23768</td>
<td>298</td>
<td>27</td>
</tr>
<tr>
<td>Services</td>
<td>133</td>
<td>133</td>
<td>0</td>
<td>142</td>
<td>139</td>
<td>134</td>
</tr>
<tr>
<td>Sockets</td>
<td>120</td>
<td>120</td>
<td>0</td>
<td>129</td>
<td>126</td>
<td>121</td>
</tr>
<tr>
<td>Buffers</td>
<td>338</td>
<td>338</td>
<td>0</td>
<td>350</td>
<td>325</td>
<td>338</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>22</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>16164</td>
<td>16164</td>
<td>0</td>
<td>16486</td>
<td>16218</td>
<td>16176</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>25</td>
<td>25</td>
<td>1893</td>
<td>4178055</td>
<td>1334</td>
<td>37</td>
</tr>
<tr>
<td>SIP Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MBC Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pipe Messages</td>
<td>30</td>
<td>30</td>
<td>0</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Message Blocks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The following table lists and defines the subcommands of the `show memory` application command.

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>Process object statistics</td>
</tr>
<tr>
<td>Message</td>
<td>Message class and all derived classes statistics</td>
</tr>
<tr>
<td>Services</td>
<td>Service class and all derived classes statistics</td>
</tr>
<tr>
<td>Sockets</td>
<td>ServiceSocket class and all derived classes statistics</td>
</tr>
<tr>
<td>Buffers</td>
<td>Malloced buffers in various classes statistics</td>
</tr>
<tr>
<td>Transactions</td>
<td>All classes derived from the transactions template statistics</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>TimedObject class and all derived classes statistics</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>Timed out queue (TOQEntry) class statistics</td>
</tr>
<tr>
<td>SIP Messages</td>
<td>Sip request (SipReq) and SIP response (SipResp) entry classes statistics</td>
</tr>
<tr>
<td>MBC Messages</td>
<td>MbcpMessage class statistics</td>
</tr>
<tr>
<td>Pipe Messages</td>
<td>Pipe message class statistics</td>
</tr>
</tbody>
</table>
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 | minsize| maxsize| 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 INET_UP INET6_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 0xffff0000 Subnetmask 0xffff0000
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: 0xffff0000
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: 0xffffff000
  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
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 Port Vlan Interface IP          Gateway          Admin Oper
Num Num ID Name       Address             Address          State State
----- ---- ---- ---------- ------------------- ---------------- ----- -
----- ---- ---- ---------- ------------------- ---------------- ----- -
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
238 packets received; 238 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 INET_UP INET6_UP
Type: ETHERNET_CSMACD
inet6: fe80::208:25ff:fe02:2280%wancom0 scopedid 0x2 prefixlen 64
inet: 172.30.1.186
Broadcast address: 172.30.255.255
Netmask 0xffff0000 Subnetmask 0xffff0000
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 unicast packets received
129 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
21 unknown protos
0 collisions; 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 0xffffffff
  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 protos
  0 collisions; 0 dropped
  0 output queue drops
  0          0          192.168.50.1/24          192.168.0.1      up    down
  1          0          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       | T ID   | PRI| STATUS   | PC     | SP     | ERRNO|
|----------+-------------+--------+---+----------+--------+--------+-----+
| tJobTask | 1934484     | 6704870| 0  | PEND     | 19e33dc| 6707ed0| 0    |
| tExcTask | 1933408     | 26c6458| 0  | PEND     | 19e33dc| 26ca1f0| 0    |
| tLogTask | 6704d30     | 19e0ac8| 0  | PEND     | 671e3e0| 0      | 0    |
| tNbioLog | 19354e8     | 670eb0c| 0  | PEND     | 19e33dc| 671e9f0| 0    |
| tWatchDog| 435fc       | 698b9c0| 0  | DELAY    | 19e2c0 | 69df68 | 0    |
| tNpwbTmr | 160a690     | 18793830| 0 | DELAY    | 19e2c0 | 187c6f40| 0    |
| ubsec_bh_h>167b8f0| 13155990| 1 PEND| 19e33dc| 13168f40| 0    |
| tClisSHO | Z4ac1p11ta | 1be38940| 1 PEND| 19e33dc| 1324e820| 44    |
```

---

162 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide Version S-C6.2.0
<table>
<thead>
<tr>
<th>Process Name</th>
<th>User</th>
<th>PID</th>
<th>State</th>
<th>Priority</th>
<th>RSS (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tFlowGdTmr</td>
<td>nPA</td>
<td>17151</td>
<td>PEND+T</td>
<td>62</td>
<td>19e33dc 18a2dec0 0</td>
</tr>
<tr>
<td>tSysmand</td>
<td>sysmand</td>
<td>32382</td>
<td>PEND+T</td>
<td>75</td>
<td>19e33dc 13178910 3d0004</td>
</tr>
<tr>
<td>tAtcpd</td>
<td>_Z5atcpdPcP9</td>
<td>181</td>
<td>PEND+T</td>
<td>75</td>
<td>19e33dc 18aebcd0 3d0004</td>
</tr>
<tr>
<td>tSecured</td>
<td>_Z7manualPc</td>
<td>32374</td>
<td>PEND+T</td>
<td>75</td>
<td>19e33dc 1b4ac1c0 3d0004</td>
</tr>
<tr>
<td>tMbcd</td>
<td>_Z11mbcPcP9s</td>
<td>2371</td>
<td>PEND+T</td>
<td>78</td>
<td>19e33dc 1b35cac0 3d0004</td>
</tr>
<tr>
<td>tEbmd</td>
<td>_Z11ebmdPcP9s</td>
<td>32365</td>
<td>PEND+T</td>
<td>78</td>
<td>19e33dc 1b867820 3d0004</td>
</tr>
<tr>
<td>tLid</td>
<td>_Z9lidaemon</td>
<td>32361</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b5ae8b0 3d0004</td>
</tr>
<tr>
<td>tAlg0</td>
<td>_Z11algPcP9s</td>
<td>32359</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b60a0a0 3d0004</td>
</tr>
<tr>
<td>tSipd</td>
<td>_Z4sipdPcP9s</td>
<td>2335</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b87b7b8 3d0004</td>
</tr>
<tr>
<td>tLtnd</td>
<td>_Z4ltndPcP9s</td>
<td>32350</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b949c80 3d0004</td>
</tr>
<tr>
<td>tH323d</td>
<td>_Z5h323dPcP9</td>
<td>2345</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b9a1c0a 3d0004</td>
</tr>
<tr>
<td>tH248d</td>
<td>_Z5h248dPcP9</td>
<td>32339</td>
<td>PEND+T</td>
<td>80</td>
<td>19e33dc 1b9d66c0 3d0004</td>
</tr>
<tr>
<td>tRadd</td>
<td>_Z4raddPcP9s</td>
<td>32334</td>
<td>PEND+T</td>
<td>82</td>
<td>19e33dc 1b617d30 3d0004</td>
</tr>
<tr>
<td>tPusher</td>
<td>_Z6pushePcP</td>
<td>32333</td>
<td>PEND+T</td>
<td>82</td>
<td>19e33dc 1b8357e0 3d0004</td>
</tr>
<tr>
<td>tAndMrc</td>
<td>AND_start</td>
<td>105</td>
<td>PEND+T</td>
<td>95</td>
<td>19e0ac8 132bde60 3d0004</td>
</tr>
<tr>
<td>tCollect</td>
<td>_Z7collectPc</td>
<td>2395</td>
<td>PEND+T</td>
<td>97</td>
<td>19e33dc 18abbdd0 3d0004</td>
</tr>
<tr>
<td>tSnmpd</td>
<td>snmpd</td>
<td>32322</td>
<td>PEND+T</td>
<td>97</td>
<td>19e33dc 1baf2d40 3d0004</td>
</tr>
<tr>
<td>tLemd</td>
<td>_Z4lemdPcP9s</td>
<td>32321</td>
<td>PEND+T</td>
<td>99</td>
<td>19e33dc 18a7fb80 3d0004</td>
</tr>
<tr>
<td>tAtcppApp</td>
<td>_Z11atcppAppP9</td>
<td>32317</td>
<td>PEND+T</td>
<td>99</td>
<td>19e33dc 18b10d30 3d0004</td>
</tr>
<tr>
<td>tTffsTask</td>
<td>flPollTask</td>
<td>6982a60</td>
<td>READY</td>
<td>100</td>
<td>19ea2c0 6986f60 0 0</td>
</tr>
<tr>
<td>tDumper</td>
<td>tDumperMain</td>
<td>13229260</td>
<td>PEND</td>
<td>100</td>
<td>19e33dc 1322ef20 0 0</td>
</tr>
<tr>
<td>tTaskCheck</td>
<td>taskCheckMain</td>
<td>132295f0</td>
<td>DELAY</td>
<td>100</td>
<td>19ea2c0 1323f30 160068</td>
</tr>
<tr>
<td>tCliWorker</td>
<td>Z13cliWorker</td>
<td>0</td>
<td>PEND</td>
<td>100</td>
<td>19e33dc 18a51f20 0 0</td>
</tr>
<tr>
<td>tPanel</td>
<td>26510</td>
<td>6984010</td>
<td>PEND</td>
<td>251</td>
<td>19e0ac8 698ef18 0 0</td>
</tr>
<tr>
<td>tIdle</td>
<td>2e93bc</td>
<td>6984c10</td>
<td>READY</td>
<td>255</td>
<td>2e93c0 6995f90 0 0</td>
</tr>
</tbody>
</table>

## Accessing Process Subcommands

Display the help text for the `show processes` command to access the following subcommands:

```
ACMEPACKET# show processes ?
```
The following table lists and defines the subcommands and additional capabilities of the `show processes` command.

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmand</td>
<td>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.</td>
</tr>
<tr>
<td>lemd</td>
<td>Statistics for the local element management (lemd) process, which is responsible for maintaining and providing local and remote access to data (including configuration and policy data) stored in the system.</td>
</tr>
<tr>
<td>brokerd</td>
<td>Statistics for the brokerd process, which is a log concentrator and sequencer used for forwarding path and hardware monitor tasks.</td>
</tr>
<tr>
<td>mbcd</td>
<td>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.</td>
</tr>
</tbody>
</table>
Display the statistics for all processes by using the `show processes all` command.

ACMEPACKET# show processes all

<table>
<thead>
<tr>
<th>12:05:39-79</th>
<th>Process Svs</th>
<th>Rcvd</th>
<th>Sent</th>
<th>Events</th>
<th>Alarm</th>
<th>Slog</th>
<th>Plog</th>
<th>CPU Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:05:09-150 (sysmand)</td>
<td>ID=13155d60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Status:</td>
<td>Active:</td>
<td>Period:</td>
<td>Total:</td>
<td>PerMax:</td>
<td>High:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services:</td>
<td>29</td>
<td>29</td>
<td>0</td>
<td>29</td>
<td>29</td>
<td>29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages:</td>
<td>0</td>
<td>1</td>
<td>12</td>
<td>35909</td>
<td>322</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactions:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Objects:</td>
<td>31</td>
<td>31</td>
<td>0</td>
<td>31</td>
<td>31</td>
<td>31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Buffers:</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alloc Buffers:</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>95</td>
<td>33</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Chunks:</td>
<td>83</td>
<td>84</td>
<td>12</td>
<td>35947</td>
<td>390</td>
<td>84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOQ Entries:</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>5326</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations:</td>
<td>16</td>
<td>44721</td>
<td>310</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received:</td>
<td>12</td>
<td>35853</td>
<td>296</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Sent:</td>
<td>0</td>
<td>45</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Message:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Events:</td>
<td>1</td>
<td>5324</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Logs:</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs:</td>
<td>0</td>
<td>58</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate:</td>
<td>0.0</td>
<td>0.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage:</td>
<td>0.0</td>
<td>11.868/531797</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ACMEPACKET# show processes all

| 08:23:17-37 (acliSSH0) | ID=1b38940 |       |       |        |       |       |       |         |
| Process Status: | Active: | Period: | Total: | PerMax: | High: |       |       |         |
|                   |       |       |       |         |         |         |         |         |

**Viewing Statistics for all Processes**

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>algd</td>
<td>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.</td>
</tr>
<tr>
<td>sipd</td>
<td>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.</td>
</tr>
<tr>
<td>current</td>
<td>Current statistics for all processes.</td>
</tr>
<tr>
<td>total</td>
<td>Total statistics for all processes.</td>
</tr>
<tr>
<td>all</td>
<td>All statistics for all processes.</td>
</tr>
<tr>
<td>cpu</td>
<td>Percentage of CPU utilization by all processes.</td>
</tr>
<tr>
<td>Component</td>
<td>Activity</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
</tr>
<tr>
<td>Process Logs</td>
<td>6</td>
</tr>
<tr>
<td>Load Rate</td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td></td>
</tr>
</tbody>
</table>

**17:19:33-113 (brokerd) ID=1326356e0**

**Process Status**

<table>
<thead>
<tr>
<th>Component</th>
<th>Activity</th>
<th>High</th>
<th>Total</th>
<th>PerMax</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>11</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>8</td>
<td>41</td>
<td>31</td>
<td>41</td>
<td>31</td>
</tr>
<tr>
<td>Messages Received</td>
<td>3</td>
<td>20</td>
<td>16</td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Load Rate</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td></td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**09:32:34-194 (cliWorker) ID=18a40470**

**Process Status**

<table>
<thead>
<tr>
<th>Component</th>
<th>Activity</th>
<th>High</th>
<th>Total</th>
<th>PerMax</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### PERFORMANCE MANAGEMENT

### Memory Chunks

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>6</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>78</td>
<td>78</td>
<td>91</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### CPU Usage

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### Load Rate

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### Messages Received

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### Messages Sent

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### Load Rate

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>

### CPU Usage

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>35</td>
<td>3</td>
<td>115198</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Process Status</th>
<th>- Period -</th>
<th>- Lifetime -</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>346</td>
<td>1068224</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>342</td>
<td>1059436</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>35.711/531883</td>
</tr>
</tbody>
</table>

12:06:39-140 (atcpApp) ID=18b0c290

<table>
<thead>
<tr>
<th>Process Status</th>
<th>- Period -</th>
<th>- Lifetime -</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>3</td>
<td>8867</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

Version S-C6.2.0
Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide 169
### Performance Management

<table>
<thead>
<tr>
<th>Load Rate</th>
<th>0.0</th>
<th>0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.247/531905</td>
</tr>
</tbody>
</table>

12:07:39-100 (mbcd) ID=1b34afe0

<table>
<thead>
<tr>
<th>Process Status</th>
<th>-- Period --</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td><strong>High</strong></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td>Services</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>16012</td>
<td>16012</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>54</td>
<td>54</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>5</td>
<td>21279</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>5</td>
<td>23049</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>38</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>1.144/531917</td>
</tr>
</tbody>
</table>

12:07:39-100 (lid) ID=1b59db10

<table>
<thead>
<tr>
<th>Process Status</th>
<th>-- Period --</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td><strong>High</strong></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>2</td>
<td>8867</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.206/531930</td>
</tr>
</tbody>
</table>

12:07:39-100 (algd) ID=1b69e570

<table>
<thead>
<tr>
<th>Process Status</th>
<th>-- Period --</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td><strong>High</strong></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>2</td>
<td>8867</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.206/531930</td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>47</td>
<td>47</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>3</td>
<td>12415</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>1</td>
<td>5320</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.550/531940</td>
</tr>
</tbody>
</table>

12:07:39-100 (radd) ID=1b6e6790

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>14</td>
<td>14</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td>16</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5321</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>3</td>
<td>14185</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>1</td>
<td>5318</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.358/531957</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.358/531957</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Process Status**

12:07:39-100 (pusher) | ID=1b824c60

<table>
<thead>
<tr>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>11</td>
<td>11</td>
<td>0</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>2</td>
<td>8868</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.232/531987</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.232/531987</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12:08:39-160 (ebmd) | ID=1b856ba0

<table>
<thead>
<tr>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>56</td>
<td>56</td>
<td>0</td>
<td>102</td>
<td>102</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>10654</td>
<td>18</td>
</tr>
<tr>
<td>Operations</td>
<td>4</td>
<td>12417</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Period</td>
<td>Lifetime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>2</td>
<td>10640</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.445/532002</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12:09:19-100 (sipd) ID=1b89dfd0

<table>
<thead>
<tr>
<th>Process Status</th>
<th>- Period -</th>
<th>Lifetime -</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Transactions</td>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>82</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>Operations</td>
<td>3</td>
<td>8868</td>
</tr>
</tbody>
</table>

12:08:39-160 (lrtd) ID=1b938740

<table>
<thead>
<tr>
<th>Process Status</th>
<th>- Period -</th>
<th>Lifetime -</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>15</td>
<td>18</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>3</td>
<td>8868</td>
</tr>
</tbody>
</table>

Version S-C6.2.0 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide 173
<table>
<thead>
<tr>
<th>System Logs</th>
<th>0</th>
<th>7</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.247/532030</td>
<td></td>
</tr>
</tbody>
</table>

### System Logs (h323d) ID=1b990570

<table>
<thead>
<tr>
<th>Time</th>
<th>12:09:49-130</th>
<th>ID=1b990570</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Status</td>
<td>--- Period --- Lifetime ---</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>133</td>
<td>133</td>
</tr>
<tr>
<td>Timed Events</td>
<td>19</td>
<td>79802</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>4</td>
<td>17792</td>
</tr>
<tr>
<td>Process Logs</td>
<td>4</td>
<td>17798</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.247/532030</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>8.668/532048</td>
</tr>
</tbody>
</table>

### System Logs (h248d) ID=1b9c56c0

<table>
<thead>
<tr>
<th>Time</th>
<th>12:09:39-120</th>
<th>ID=1b9c56c0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Status</td>
<td>--- Period --- Lifetime ---</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Timed Events</td>
<td>19</td>
<td>79802</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>4</td>
<td>17792</td>
</tr>
<tr>
<td>Process Logs</td>
<td>4</td>
<td>17798</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.301/532093</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>8.668/532048</td>
</tr>
</tbody>
</table>

### System Logs (secured) ID=1ba472c0

<table>
<thead>
<tr>
<th>Time</th>
<th>12:10:39-180</th>
<th>ID=1ba472c0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Status</td>
<td>--- Period --- Lifetime ---</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Timed Events</td>
<td>19</td>
<td>79802</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>4</td>
<td>17792</td>
</tr>
<tr>
<td>Process Logs</td>
<td>4</td>
<td>17798</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.301/532093</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>8.668/532048</td>
</tr>
</tbody>
</table>
## Process Status

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>43</td>
<td>43</td>
<td>65</td>
<td>45</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>4</td>
<td>8871</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.258/532104</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.244/532118</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12:10:39-180 (snmpd) | ID=1bae1760

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>4</td>
<td>4</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>16</td>
<td>16</td>
<td>22</td>
<td>18</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>4</td>
<td>8871</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.258/532104</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.244/532118</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

08:23:17-37 (acliSSH1) | ID=1be88cd0

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
<td>Total</td>
<td>PerMax</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>-------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Process Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.000/532127</td>
<td>0.000/532143</td>
<td>0.000/532143</td>
</tr>
</tbody>
</table>

08:23:17-37 (ac1iSSH2) ID=1be89c70
08:23:17-37 (ac1iSSH3) ID=1be9c010
### Performance Management

<table>
<thead>
<tr>
<th>Metric</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial Message Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Message Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.000/532143</td>
<td></td>
</tr>
</tbody>
</table>

08:23:17-37 (acliSSH3) ID=1be9c010

<table>
<thead>
<tr>
<th>Process Status</th>
<th>-- Period --</th>
<th>--------</th>
<th>Lifetime --------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.0</td>
<td>0.000/532170</td>
</tr>
</tbody>
</table>

08:23:17-37 (acliSSH4) ID=1be9c010

<table>
<thead>
<tr>
<th>Process Status</th>
<th>-- Period --</th>
<th>--------</th>
<th>Lifetime --------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>
### Process Logs

<table>
<thead>
<tr>
<th></th>
<th>12:14:39-120 (acliConsole) ID=1bedb940</th>
<th>12:05:39-179 (acliTelnet0) ID=1bef1ce0</th>
<th>14:04:54-134 (acliTelnet1) ID=1bf07ca0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Load Rate</strong></td>
<td>0.0</td>
<td>0.4</td>
<td>19.778</td>
</tr>
<tr>
<td><strong>CPU Usage</strong></td>
<td>0.000/532344</td>
<td>0.450/532357</td>
<td>19.778/532371</td>
</tr>
<tr>
<td><strong>Process Status</strong></td>
<td>-- Period -- -------- Lifetime --------</td>
<td>-- Period -- -------- Lifetime --------</td>
<td>-- Period -- -------- Lifetime --------</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>3</td>
<td>4</td>
<td>42</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>3</td>
<td>4</td>
<td>42</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>3</td>
<td>4</td>
<td>42</td>
</tr>
<tr>
<td><strong>PerMax</strong></td>
<td>3</td>
<td>4</td>
<td>42</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>3</td>
<td>4</td>
<td>42</td>
</tr>
</tbody>
</table>

<p>| <strong>Services</strong>   | 3                                     | 4                                     | 42                                    |
| <strong>Messages</strong>   | 0                                     | 0                                     | 0                                     |
| <strong>Transactions</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Timed Objects</strong> | 5                                     | 5                                     | 5                                     |
| <strong>Total Buffers</strong> | 5                                     | 5                                     | 5                                     |
| <strong>Alloc Buffers</strong> | 2                                     | 2                                     | 2                                     |
| <strong>Memory Chunks</strong> | 15                                    | 15                                    | 15                                    |
| <strong>TOQ Entries</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Operations</strong> | 3                                     | 10517                                 | 177                                   |
| <strong>Messages Received</strong> | 0                                     | 1                                     | 1                                     |
| <strong>Messages Sent</strong> | 0                                     | 16                                    | 6                                     |
| <strong>Partial Message</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Partial Msg Expired</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Partial Msg Dropped</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Timed Events</strong> | 0                                     | 0                                     | 0                                     |
| <strong>Alarms</strong>     | 0                                     | 0                                     | 0                                     |
| <strong>System Logs</strong> | 0                                     | 18                                    | 6                                     |
| <strong>Process Logs</strong> | 0                                     | 18                                    | 6                                     |
| <strong>Load Rate</strong>  | 0.0                                   | 0.0                                   | 0.0                                   |
| <strong>CPU Usage</strong>  | 0.000/532344                          | 0.450/532357                          | 19.778/532371                         |</p>
<table>
<thead>
<tr>
<th>Process</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>4</td>
<td>662</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>Process Logs</td>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.129</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.129/532384</td>
</tr>
</tbody>
</table>

08:23:17-37 (acliTelnet2) ID=1bf1ec90
<table>
<thead>
<tr>
<th>Process</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Process Logs</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.000/532397</td>
</tr>
</tbody>
</table>

08:23:17-37 (acliTelnet3) ID=1bf4b4c0
<table>
<thead>
<tr>
<th>Process</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Messages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory Chunks</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Partial Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Partial Msg Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Process Logs</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.0</td>
<td>0.000/532435</td>
</tr>
</tbody>
</table>

08:23:17-37 (acl iTelnet4) | ID=1bf62090

| Process Status | ... | Period | ... | Lifetime | ... |
| 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 | 1 | 1 | 1 |
| Messages Received | 0 | 0 | 0 | 0 | 0 | 0 |
| Messages Sent | 3 | 3 | 3 | 3 | 3 | 3 |
| Partial Message | 0 | 0 | 0 | 0 | 0 | 0 |
| Partial Msg Expired | 0 | 0 | 0 | 0 | 0 | 0 |
| Partial Msg Dropped | 0 | 0 | 0 | 0 | 0 | 0 |
| Timed Events | 0 | 0 | 0 | 0 | 0 | 0 |
| Alarms | 0 | 0 | 0 | 0 | 0 | 0 |
| System Logs | 6 | 6 | 6 | 6 | 6 | 6 |
| Process Logs | 6 | 6 | 6 | 6 | 6 | 6 |
| Load Rate | 0.0 | 0.0 | 0.0 |
| CPU Usage | 0.0 | 0.000/532454 |

08:24:43-23 (tTaskCheck) | ID=132295f0

| Process Status | ... | Period | ... | Lifetime | ... |
| 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 | 1 | 1 | 1 |
### 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 Alarm Slog Plog CPU Max
sysmmand  29 35961 45 5340 0 11 58 0.0 0
acliSSH0   4   0   3   0   0 6 6 0.0 0
brokerd    2  20   4   0   3 4 4 0.0 0
cliWorke    2   0   2   0   5 6 0.0 0
lemd        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   7 8 0.0 0
mbcd        9   1  30 23112 0 32 38 0.0 0
lid          3   1   6   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   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
lrd          4   1   5   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   8 10 0.0 0
snmpd       4   1   7   0   9 9 0.0 0
acliSSH1    4   0   3   0   6 6 0.0 0
acliSSH2    4   0   3   0   6 6 0.0 0
acliSSH3    4   0   3   0   6 6 0.0 0
acliSSH4    4   0   3   0   6 6 0.0 0
acliCons    3   1  16   0   18 18 0.0 0
acliTeln    4  22  92   3   73 73 0.0 0
acliTeln    4   6  20   0   16 16 0.0 0
acliTeln    4   0   3   0   6 6 0.0 0
acliTeln    4   0   3   0   6 6 0.0 0
acliTeln    4   0   3   0   6 6 0.0 0
taskChe     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**

<table>
<thead>
<tr>
<th>Process</th>
<th>Svcs</th>
<th>TOQ</th>
<th>Ops</th>
<th>Rcvd</th>
<th>Sent</th>
<th>Events</th>
<th>Alarm</th>
<th>Slog</th>
<th>Plog</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmand</td>
<td>29</td>
<td>2</td>
<td>15</td>
<td>11</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aclSSH0</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>brokerd</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>cliWorke</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lemd</td>
<td>5</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>collect</td>
<td>3</td>
<td>0</td>
<td>34</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>atcpd</td>
<td>5</td>
<td>1</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>atcpApp</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mbcd</td>
<td>9</td>
<td>2</td>
<td>7</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lid</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>algd</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>radd</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pusher</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ebmd</td>
<td>5</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>sipd</td>
<td>5</td>
<td>2</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>lrtd</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>h323d</td>
<td>6</td>
<td>3</td>
<td>16</td>
<td>0</td>
<td>5</td>
<td>22</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>h248d</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>secured</td>
<td>5</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>snmpd</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aclSSH1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclSSH2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclSSH3</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclSSH4</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclConn</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aclTeln</td>
<td>4</td>
<td>0</td>
<td>48</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aclTeln</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>aclTeln</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclTeln</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>aclTeln</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>tTaskChe</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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-remaining boot

boot: 20127744/29760512 bytes (67%) remaining

ACMEPACKET# check-space-remaining code

code: 23214080/29760512 bytes (78%) remaining

ACMEPACKET# check-space-remaining ramdrv
```
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 ?
```

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       -- Period --       -- Lifetime --
                                  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      0       0       0
Server Trans                  1        44      593     78      27      0
Client Trans                  0        0       0      0       0       0
Redundancy Transactions      ----       --     ----       ----       ----       ----
Recent                        44      593     78
Requests received             44      593     78
```
### 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.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued entries</td>
<td>Number of transactions the active Net-Net SBC has not yet sent to its standby Net-Net SBC peer.</td>
</tr>
<tr>
<td>Red Records</td>
<td>Total number of HA transactions created. This set of statistics should be the same as those for Queued entries.</td>
</tr>
<tr>
<td>Records Dropped</td>
<td>Number of HA transaction records that were lost (i.e., dropped) because the standby Net-Net SBC fell behind in synchronization.</td>
</tr>
<tr>
<td>Server Trans</td>
<td>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.</td>
</tr>
<tr>
<td>Client Trans</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Viewing Border Element Redundancy Protocol Information

You can view Border Element Redundancy Protocol statistics by using the `show berp` 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.

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.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>HA Net-Net SBC is booting and looking for its configured peers.</td>
</tr>
<tr>
<td>BecomingActive</td>
<td>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.</td>
</tr>
<tr>
<td>Active</td>
<td>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.</td>
</tr>
<tr>
<td>RelinquishingActive</td>
<td>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).</td>
</tr>
<tr>
<td>BecomingStandby</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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.
```

**Standby**

The following example shows a becoming standby Net-Net SBC.

```
ACMEPACKET# show health

Media Synchronized true
SIP Synchronized disabled
MGCP Synchronized true
Config Synchronized true
Active Peer Address 0.0.0.0
```
Redundancy Protocol Process (v2):

<table>
<thead>
<tr>
<th>State</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>100</td>
</tr>
<tr>
<td>Lowest Local Address</td>
<td>11.0.0.1:9090</td>
</tr>
</tbody>
</table>

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 table lists the health statistics along with a brief description.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Synchronized</td>
<td>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 displayed message is displayed in the show health output.</td>
</tr>
<tr>
<td>SIP Synchronized</td>
<td>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.</td>
</tr>
<tr>
<td>MGCP Synchronized</td>
<td>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.</td>
</tr>
<tr>
<td>Config Synchronized</td>
<td>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.</td>
</tr>
<tr>
<td>Active Peer Address</td>
<td>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)</td>
</tr>
</tbody>
</table>
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
Destination/Pfx    Gateway         Flags    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
routing:
  0 bad routing redirect
  3 dynamically created route
  1 new gateway due to redirects
  9 destinations found unreachable
  2 use of a wildcard 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-profiles                list of media profiles
show                          shows local policy test results
source-realm                  Source realm
time-of-day                   enables/disables time of day
to-address                    To address
exit                          end test
```
The following table lists the test-policy specification formats.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-realm</td>
<td>A string that indicates the name set in the source-realm field of a configured local-policy element. If you enter a &quot;*&quot; in this specification, any configured source realms will be matched. An empty source-realm value indicates that only the &quot;global&quot; realm will be tested.</td>
</tr>
<tr>
<td>time-of-day</td>
<td>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.</td>
</tr>
<tr>
<td>carriers</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Test Policy Subcommands**

The following table lists and describes the test-policy subcommands.

<table>
<thead>
<tr>
<th>test-policy Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from-address</td>
<td>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:<a href="mailto:19785551212@netnetsystem.com">19785551212@netnetsystem.com</a>).</td>
</tr>
<tr>
<td>to-address</td>
<td>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:<a href="mailto:19785551212@netnetsystem.com">19785551212@netnetsystem.com</a>).</td>
</tr>
<tr>
<td>show</td>
<td>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.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the test-policy session.</td>
</tr>
</tbody>
</table>

**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
- calling-address
- show
- translation-id
- exit

**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 -- ------- Lifetime -------
Realm              Active  Rate   High  Total      Total PerMax   High
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 -- ------- Lifetime -------
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       -
Seizure                -       -       4          4       4       -
Answer                 -       -       4          4       4       -
ASR Exceeded           -       -       0          0       0       -
Requests Received      -       -       0          0       0       -
QoS Major Exceeded    -       -       2          2       2       -
QoS Critical 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.lrtd 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 lrtd 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 lrtd, followed by the log level you want to set. Then press <Enter>.

ACMEPACKET# notify lrtd 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 lrtd refresh, followed by the name of the local routing policy you want updated.

ACMEPACKET# notify lrtd 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 lr= 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 lr=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
Performance Management

UserName <123>
User Type = E164
Next Hop = !:^.*$!sip:123@192.168.1.191!
Next Hop 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
- Not Found—Number of note 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 -- -------- Lifetime --------
                      Active | High | Total | Total | PerMax | High
Sessions             0      | 0     | 0      | 0      | 0      | 0
Subscriptions        0      | 0     | 0      | 0      | 0      | 0
Dialogs              0      | 0     | 0      | 0      | 0      | 0
Call ID Map          0      | 0     | 0      | 0      | 0      | 0
Rejections           -      | -     | 0      | 0      | 0      | 0
ReINVITEs            -      | -     | 0      | 0      | 0      | 0
Media Sessions       0      | 0     | 0      | 0      | 0      | 0
Media Pending        0      | 0     | 0      | 0      | 0      | 0
Client 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      | 0
DNS Trans            0      | 0     | 0      | 0      | 0      | 0
DNS Sockets          0      | 0     | 0      | 0      | 0      | 0
DNS Results          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 -- -------- Lifetime --------
                      Active | High | Total | Total | PerMax | High
Sessions             0      | 0     | 0      | 0      | 0      | 0
Subscriptions        0      | 0     | 0      | 0      | 0      | 0
Dialogs              0      | 0     | 0      | 0      | 0      | 0
Call ID Map          0      | 0     | 0      | 0      | 0      | 0
Rejections           -      | -     | 0      | 0      | 0      | 0
ReINVITEs            -      | -     | 0      | 0      | 0      | 0
Media Sessions       0      | 0     | 0      | 0      | 0      | 0
Media Pending        0      | 0     | 0      | 0      | 0      | 0
Client 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      | 0
DNS Trans            0      | 0     | 0      | 0      | 0      | 0
DNS Sockets          0      | 0     | 0      | 0      | 0      | 0
DNS Results          0      | 0     | 0      | 0      | 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.
Session Rate = 0.0
Load Rate = 0.0

The following table lists the SIP status statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialogs</td>
<td>Number of SIP signaling connections between the Net-Net SBC and a SIP UA</td>
</tr>
<tr>
<td></td>
<td>(for example, a call leg)</td>
</tr>
<tr>
<td>Sessions</td>
<td>Number of sessions established by an INVITE request. A session consists of</td>
</tr>
<tr>
<td></td>
<td>all dialogs created by one INVITE transaction.</td>
</tr>
<tr>
<td>Sockets</td>
<td>Number of active SIP communication ports (the number of open UDP and TCP</td>
</tr>
<tr>
<td></td>
<td>sockets)</td>
</tr>
<tr>
<td>DNS Transactions</td>
<td>Number of outstanding DNS requests</td>
</tr>
</tbody>
</table>
Viewing SIP Performance Statistics

The following example shows the subcommands available for the `show sipd` command.

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 -- Period -- -------- Lifetime --------
      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  2351
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 Exp      0    0    0
Exp Media Drops       0    0    0
15:10:31-138
MGCP ACL Status -- Period -- -------- Lifetime --------
```
### PERFORMANCE MANAGEMENT

<table>
<thead>
<tr>
<th>Total Entries</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>3475</td>
<td>3475</td>
<td>3247</td>
<td>3475</td>
<td>2390</td>
<td>3475</td>
</tr>
</tbody>
</table>

| Trusted       | 2351   | 2351 | 2351  | 1897         | 2351 |

| Blocked       | 0      | 0    | 0     | 0            | 0    |

### ACL Operations

<table>
<thead>
<tr>
<th>ACL Requests</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2351</td>
<td>2351</td>
<td>1897</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bad Messages</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Promotions</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2351</td>
<td>2351</td>
<td>1897</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Demotions</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

--- < NO DATA AVAILABLE >----(RSIP)

### Traffic Metrics

**RQNT incoming:**

<table>
<thead>
<tr>
<th>Requests received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>9904</td>
<td>9924</td>
<td>8252</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>9653</td>
<td>9653</td>
<td>8156</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>232</td>
<td>252</td>
<td>154</td>
<td></td>
</tr>
</tbody>
</table>

**RQNT outgoing:**

<table>
<thead>
<tr>
<th>Requests sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>9672</td>
<td>9672</td>
<td>8174</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>9653</td>
<td>9653</td>
<td>8156</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**NTFY incoming:**

<table>
<thead>
<tr>
<th>Requests received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>5741</td>
<td>5741</td>
<td>5053</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>5350</td>
<td>5350</td>
<td>4665</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>366</td>
<td>366</td>
<td>366</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overload 403 sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>366</td>
<td>366</td>
<td>366</td>
<td></td>
</tr>
</tbody>
</table>

**NTFY outgoing:**

<table>
<thead>
<tr>
<th>Requests sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>5352</td>
<td>5352</td>
<td>4667</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>5350</td>
<td>5350</td>
<td>4665</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**CRCX incoming:**

<table>
<thead>
<tr>
<th>Requests received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2356</td>
<td>2356</td>
<td>1902</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2351</td>
<td>2351</td>
<td>1897</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**CRCX outgoing:**

<table>
<thead>
<tr>
<th>Requests sent</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2356</td>
<td>2356</td>
<td>1902</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>2351</td>
<td>2351</td>
<td>1897</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**MDCX incoming:**

<table>
<thead>
<tr>
<th>Requests received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>4761</td>
<td>4761</td>
<td>3987</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors received</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
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
INVITE (15:53:43-122)

--------------- Server --------------  -------------- Client --------------
Message/Event     Recent  Total   PerMax  Recent  Total   PerMax
---------------     ------  ------   ------  ------  ------   ------
INVITE Requests   469     11132   428     469     11132   428
Retransmissions   0       0       0       0       0       0
100 Trying        469     11132   428     468     10965   428
180 Ringing       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
Transaction Timeouts -   -   -   -   -   -

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 current time period—in one-second increments, and always is between 100 and 199 and never below 100, constituting a 100-200 second recent period. This is done in order to keep the statistics from zeroing out between transition periods.

• 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

<table>
<thead>
<tr>
<th>SIP Server Trans</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Period</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>All States</td>
<td>0</td>
<td>346</td>
<td>2213</td>
<td>67975</td>
<td>3729</td>
</tr>
<tr>
<td>&lt;Initial&gt;</td>
<td>0</td>
<td>1</td>
<td>2213</td>
<td>67975</td>
<td>3729</td>
</tr>
<tr>
<td>&lt;Trying&gt;</td>
<td>0</td>
<td>48</td>
<td>1504</td>
<td>44773</td>
<td>2431</td>
</tr>
<tr>
<td>&lt;Proceeding&gt;</td>
<td>0</td>
<td>9</td>
<td>709</td>
<td>23202</td>
<td>1310</td>
</tr>
<tr>
<td>&lt;Cancelled&gt;</td>
<td>0</td>
<td>2</td>
<td>75</td>
<td>1370</td>
<td>182</td>
</tr>
<tr>
<td>&lt;Established&gt;</td>
<td>0</td>
<td>2</td>
<td>545</td>
<td>20201</td>
<td>971</td>
</tr>
<tr>
<td>&lt;Completed&gt;</td>
<td>0</td>
<td>148</td>
<td>959</td>
<td>23202</td>
<td>1309</td>
</tr>
<tr>
<td>&lt;Confirmed&gt;</td>
<td>0</td>
<td>157</td>
<td>716</td>
<td>23202</td>
<td>1309</td>
</tr>
<tr>
<td>&lt;Terminated&gt;</td>
<td>0</td>
<td>1</td>
<td>545</td>
<td>20201</td>
<td>972</td>
</tr>
</tbody>
</table>
```

ACMEPACKET#

The following table lists the specifics along with a brief description.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All States</td>
<td>Total number of all server transactions.</td>
</tr>
<tr>
<td>Initial</td>
<td>State when the server transaction is created after a request is received.</td>
</tr>
<tr>
<td>Trying</td>
<td>Number of times the 100 Trying message has been sent, meaning that a request has been received and action is being taken.</td>
</tr>
<tr>
<td>Proceeding</td>
<td>Number of times a server transaction has been constructed for a request.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>Number of INVITE transactions for which the Net-Net system receives a CANCEL.</td>
</tr>
<tr>
<td>Established</td>
<td>Situation in which the server sends a 2xx response to an INVITE.</td>
</tr>
<tr>
<td>Completed</td>
<td>Number of times that the server has received a 300 to 699 status code and therefore entered the completed state.</td>
</tr>
<tr>
<td>Confirmed</td>
<td>Number of times that an ACK was received while the server was in the completed state and therefore transitioned to the confirmed state.</td>
</tr>
<tr>
<td>Terminated</td>
<td>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.</td>
</tr>
</tbody>
</table>
Display statistics for SIP client transactions by using the `show sipd client` command.

ACMEPACKET# `show sipd client`

15:40:09-69

```
SIP Client Trans          -- Period -- -------- Lifetime --------
                           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
<Canceled>               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.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All States</td>
<td>Total number of all client transactions.</td>
</tr>
<tr>
<td>Initial</td>
<td>State before a request is sent out.</td>
</tr>
<tr>
<td>Trying</td>
<td>Number of times the <code>trying</code> state was entered due to the receipt of a request.</td>
</tr>
<tr>
<td>Calling</td>
<td>Number of times that the <code>calling</code> state was entered due to the receipt of an INVITE request.</td>
</tr>
<tr>
<td>Proceeding</td>
<td>Number of times that the <code>proceeding</code> state was entered due to the receipt of a provisional response while in the <code>calling</code> state.</td>
</tr>
<tr>
<td>Early Media</td>
<td>Number of times that the <code>proceeding</code> state was entered due to the receipt of a provisional response that contained SDP while in the <code>calling</code> state.</td>
</tr>
<tr>
<td>Completed</td>
<td>Number of times that the <code>completed</code> state was entered due to the receipt of a 300 to 699 status code when either in the <code>calling</code> or <code>proceeding</code> state.</td>
</tr>
<tr>
<td>SetMedia</td>
<td>Number of transactions in which the Net-Net system is setting up NAT and steering ports (setting up the steering of the RTP flow).</td>
</tr>
<tr>
<td>Established</td>
<td>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.</td>
</tr>
<tr>
<td>Terminated</td>
<td>Number of times that the <code>terminated</code> state was entered due to the receipt of a 2xx message.</td>
</tr>
</tbody>
</table>

**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 | 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 on the current log level setting) of the appropriate severity which will indicate the nature of the error.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Offer Errors</td>
<td>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.</td>
</tr>
<tr>
<td>SDP Answer Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Drop Media Errors</td>
<td>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 mbcd errors.</td>
</tr>
<tr>
<td>Transaction Errors</td>
<td>Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session.</td>
</tr>
<tr>
<td>Missing Dialog</td>
<td>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.</td>
</tr>
<tr>
<td>Application Errors</td>
<td>Number of miscellaneous errors that occur in the SIP application that are otherwise uncategorized.</td>
</tr>
<tr>
<td>Media Exp Events</td>
<td>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 mbcd errors.</td>
</tr>
<tr>
<td>Early Media Exp</td>
<td>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 subaq-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.</td>
</tr>
<tr>
<td>Exp Media Drops</td>
<td>Number of flow timer expiration notifications from MBCD which resulted in the SIP application terminating the dialog/session.</td>
</tr>
<tr>
<td>Multiple OK Drops</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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          Active | Period | Lifetime
Sessions                   0 | 0 | 0 | 0 | 0 | 0
  Initial                  0 | 0 | 0 | 0 | 0 | 0
  Early                   0 | 0 | 0 | 0 | 0 | 0
  Established              0 | 0 | 0 | 0 | 0 | 0
  Terminated              0 | 0 | 0 | 0 | 0 | 0
Dialogs                   0 | 0 | 0 | 0 | 0 | 0
  Early                  0 | 0 | 0 | 0 | 0 | 0
  Confirmed              0 | 0 | 0 | 0 | 0 | 0
  Terminated            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] ID=4 exp=28
UA-ctnt='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] ID=4 exp=20
UA-ctnt='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'
```
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 ACLI `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: 0078555-47260002-3dde9eed-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 *
```

### 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
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
```
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 mbcd 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 mbcd 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.

<table>
<thead>
<tr>
<th>STUN Server Display Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>The number of STUN servers (the same as the number of realms configured with a STUN server).</td>
</tr>
<tr>
<td>Server Ports</td>
<td>Number of ports per STUN server; there will be four ports per STUN server.</td>
</tr>
<tr>
<td>Binding Requests</td>
<td>Number of STUN Binding Request messages received by all STUN servers.</td>
</tr>
<tr>
<td>Binding Responses</td>
<td>Number of STUN Binding Response messages sent by all STUN servers.</td>
</tr>
</tbody>
</table>
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 mbcd log` or `notify mbcd debug` commands, you enable protocol tracing for STUN. Using `notify mbcd debug` sets the STUN log level to TRACE. You can turn off tracing using the `notify mbcd nolog` or `notify mbcd nodebug` commands. Using `notify mbcd 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
```

<table>
<thead>
<tr>
<th>Session Stats</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Calls</td>
<td>135</td>
<td>176</td>
<td>1001</td>
<td>77258</td>
<td>785</td>
<td>196</td>
</tr>
<tr>
<td>Outgoing Calls</td>
<td>135</td>
<td>176</td>
<td>1001</td>
<td>77258</td>
<td>785</td>
<td>196</td>
</tr>
<tr>
<td>Connected Calls</td>
<td>135</td>
<td>172</td>
<td>977</td>
<td>74390</td>
<td>727</td>
<td>196</td>
</tr>
<tr>
<td>Incoming Channels</td>
<td>251</td>
<td>319</td>
<td>1953</td>
<td>148780</td>
<td>1454</td>
<td>358</td>
</tr>
<tr>
<td>Outgoing Channels</td>
<td>251</td>
<td>319</td>
<td>1953</td>
<td>148780</td>
<td>1454</td>
<td>358</td>
</tr>
<tr>
<td>Contexts</td>
<td>135</td>
<td>179</td>
<td>1001</td>
<td>77258</td>
<td>785</td>
<td>197</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H323D Status</th>
<th>Current</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued Messages</td>
<td>238</td>
<td>16000</td>
</tr>
<tr>
<td>TPKT Channels</td>
<td>542</td>
<td>4004</td>
</tr>
<tr>
<td>UDP Channels</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack</th>
<th>State</th>
<th>Type</th>
<th>Mode</th>
<th>Registered Gatekeeper</th>
</tr>
</thead>
</table>

---

<table>
<thead>
<tr>
<th>STUN Server Display Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding Errors</td>
<td>Number of STUN Binding Error messages sent by all STUN servers.</td>
</tr>
<tr>
<td>Messages Dropped</td>
<td>Number of messages dropped by all STUN servers.</td>
</tr>
</tbody>
</table>
The following table lists the session statistics along with a brief description.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Calls</td>
<td>Number of H.323 calls coming into the Net-Net SBC.</td>
</tr>
<tr>
<td>Outgoing Calls</td>
<td>Number of H.323 calls going out of the Net-Net SBC.</td>
</tr>
<tr>
<td>Connected Calls</td>
<td>Number of H.323 calls that are currently connected via the Net-Net SBC.</td>
</tr>
<tr>
<td>Incoming Channels</td>
<td>Number of incoming channels that have been established on the Net-Net SBC</td>
</tr>
<tr>
<td>Outgoing Channels</td>
<td>Number of outgoing channels that have been established on the Net-Net SBC</td>
</tr>
<tr>
<td>Contexts</td>
<td>Number of contexts (i.e., the number of calls traversing the Net-Net SBC)</td>
</tr>
</tbody>
</table>

About Status Statistics

The following table lists the current H.323 process status statistics along with a brief description:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued Messages</td>
<td>Number of messages queued.</td>
</tr>
<tr>
<td>TPKT Channels</td>
<td>Number of Transport Packet (TPKT) channels open(ed).</td>
</tr>
<tr>
<td>UDP Channels</td>
<td>Number of User Datagram Protocol (UDP) channels open(ed).</td>
</tr>
</tbody>
</table>

**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
```
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
 prefixes
 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
 q931-max-calls 200
 h245-tunneling disabled
 fs-in-first-msg disabled
 call-start-fast enabled
 call-start-slow disabled
 media-profiles
 prefix
 process-registration disabled
 allow-anonymous all
 proxy-mode       H225
 h245-stage       connect
```

codec-fallback disabled
last-modified-date 2006-07-07 07:49:57
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
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-c-start-port           0
dynamic-c-number-ports         0
rfc2833-mode                   transparent
filename                       ps
tcp-keepalive                  disabled
```

```
212 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide Version S-C6.2.0
```
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 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.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbound</strong></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Number of active sessions sent to each session agent listed in the Session Agent column of this command’s output.</td>
</tr>
<tr>
<td>Rate</td>
<td>Average rate of session invitations (per second) sent to each session agent listed in the Session Agent column of this command’s output.</td>
</tr>
</tbody>
</table>
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]

                  Period       Lifetime
                 --  --------  --------
Active            0       0       0
High              0       0       0
Total             0       0       0
PerMax            0       0       0
High              0       0       0

Inbound Sessions
                  0       0       0
Rate Exceeded    -       -       0
Num Exceeded     -       -       0
Reg Rate Exceeded-       -       0
Outbound Sessions
                  199     245     196
Rate Exceeded    -       -       0
Num Exceeded     -       -       0
Reg Rate Exceeded-       -       0
Out of Service   -       -       0
Trans Timeout    -       -       0
Requests Sent    -       -       2092
Requests Complete-       -       196
Seizure          -       -       196
Answer           -       -       199
ASR Exceeded     -       -       199
```

### Statistic Description

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConEx</td>
<td>Number of times that the constraints established in the constraints fields of the <code>session-agent</code> element have been exceeded. The constraints fields of the <code>session-agent</code> element include the following: <code>max-sessions</code>, <code>max-outbound-sessions</code>, <code>max-burst-rate</code>, <code>max-sustain-rate</code>, <code>burst-rate-window</code>, and <code>sustain-rate-window</code>.</td>
</tr>
<tr>
<td>Latency</td>
<td></td>
</tr>
<tr>
<td>Avg</td>
<td>Average latency for packets traveling to and from each session agent listed in the <code>Session Agent</code> column of this command's output.</td>
</tr>
<tr>
<td>Max</td>
<td>Maximum latency for packets traveling to and from each session agent listed in the <code>Session Agent</code> column of this command's output.</td>
</tr>
<tr>
<td>Max Burst</td>
<td>Total number of session invitations sent to or received from the session agent within the amount of time configured in the <code>burst-rate-window</code> field of the <code>session-agent</code> element.</td>
</tr>
</tbody>
</table>
The following table lists the statistics and a brief description.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbound Sessions</strong></td>
<td></td>
</tr>
<tr>
<td>Rate Exceeded</td>
<td>Number of times the session or burst rate was exceeded for inbound sessions.</td>
</tr>
<tr>
<td>Num Exceeded</td>
<td>Number of times the time constraints were exceeded for inbound sessions.</td>
</tr>
<tr>
<td><strong>Outbound Sessions</strong></td>
<td></td>
</tr>
<tr>
<td>Rate Exceeded</td>
<td>Number of times the session or burst rate was exceeded for outbound sessions.</td>
</tr>
<tr>
<td>Num Exceeded</td>
<td>Number of times the time constraints were exceeded for outbound sessions.</td>
</tr>
<tr>
<td>Burst</td>
<td>Number of times the burst rate was exceeded for this session agent.</td>
</tr>
<tr>
<td>Out of Service</td>
<td>Number of times this session agent went out of service.</td>
</tr>
<tr>
<td>Trans Timeout</td>
<td>Number of transactions that timed out for this session agent.</td>
</tr>
<tr>
<td>Requests Sent</td>
<td>Number of messages sent via the session agent.</td>
</tr>
<tr>
<td>Requests Complete</td>
<td>Number of requests that have been completed for this session agent.</td>
</tr>
<tr>
<td>Messages Received</td>
<td>Number of messages received by this session agent.</td>
</tr>
</tbody>
</table>

**Viewing Session Agent Configurations**

Display the configuration for all configured H.323 session agents by using the `show h323d agentconfig` command.

```
ACMEPACKET(session-agent)# show h323 agentconfig
```

```
hostname testhostname.com
ip-address 192.168.200.13
port 5060
state enabled
app-protocol SIP
app-type H323-GW
transport-method UDP
realm-id h323192
description
 carriers
 allow-next-hop-lp 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
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-translationid
out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
p-asserted-id
trunk-group tname1:tgcontext1
tname2: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 test hostname.com
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>192.168.200.13</td>
</tr>
<tr>
<td>port</td>
<td>5060</td>
</tr>
<tr>
<td>state</td>
<td>enabled</td>
</tr>
<tr>
<td>app-protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>app-type</td>
<td>H323-GW</td>
</tr>
<tr>
<td>transport-method</td>
<td>UDP</td>
</tr>
<tr>
<td>realm-id</td>
<td>h323192</td>
</tr>
<tr>
<td>description</td>
<td></td>
</tr>
<tr>
<td>carriers</td>
<td></td>
</tr>
<tr>
<td>allow-next-hop-lp</td>
<td>enabled</td>
</tr>
<tr>
<td>constraints</td>
<td>disabled</td>
</tr>
<tr>
<td>max-sessions</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-sessions</td>
<td>4</td>
</tr>
<tr>
<td>max-outbound-sessions</td>
<td>5</td>
</tr>
<tr>
<td>max-burst-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-burst-rate</td>
<td>10</td>
</tr>
<tr>
<td>max-outbound-burst-rate</td>
<td>1</td>
</tr>
<tr>
<td>max-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-inbound-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>max-outbound-sustain-rate</td>
<td>0</td>
</tr>
<tr>
<td>min-seizures</td>
<td>5</td>
</tr>
<tr>
<td>min-asr</td>
<td>0</td>
</tr>
<tr>
<td>time-to-resume</td>
<td>0</td>
</tr>
<tr>
<td>ttr-no-response</td>
<td>0</td>
</tr>
<tr>
<td>in-service-period</td>
<td>0</td>
</tr>
<tr>
<td>burst-rate-window</td>
<td>0</td>
</tr>
<tr>
<td>sustain-rate-window</td>
<td>0</td>
</tr>
<tr>
<td>req-uri-carrier-mode</td>
<td>None</td>
</tr>
<tr>
<td>proxy-mode</td>
<td>Redirect</td>
</tr>
<tr>
<td>redirect-action</td>
<td>enabled</td>
</tr>
<tr>
<td>loose-routing</td>
<td>enabled</td>
</tr>
<tr>
<td>send-media-session</td>
<td>enabled</td>
</tr>
<tr>
<td>response-map</td>
<td></td>
</tr>
<tr>
<td>ping-method</td>
<td></td>
</tr>
<tr>
<td>ping-interval</td>
<td>0</td>
</tr>
<tr>
<td>ping-in-service-response-codes</td>
<td></td>
</tr>
<tr>
<td>out-service-response-codes</td>
<td></td>
</tr>
<tr>
<td>media-profiles</td>
<td></td>
</tr>
<tr>
<td>in-translationid</td>
<td></td>
</tr>
<tr>
<td>out-translationid</td>
<td></td>
</tr>
<tr>
<td>trust-me</td>
<td>disabled</td>
</tr>
<tr>
<td>request-uri-headers</td>
<td></td>
</tr>
<tr>
<td>stop-recursse</td>
<td></td>
</tr>
<tr>
<td>local-response-map</td>
<td></td>
</tr>
<tr>
<td>ping-to-user-part</td>
<td></td>
</tr>
<tr>
<td>ping-from-user-part</td>
<td></td>
</tr>
<tr>
<td>li-trust-me</td>
<td>disabled</td>
</tr>
<tr>
<td>in-manipulationid</td>
<td></td>
</tr>
<tr>
<td>out-manipulationid</td>
<td></td>
</tr>
<tr>
<td>p-asserted-id</td>
<td></td>
</tr>
<tr>
<td>trunk-group</td>
<td></td>
</tr>
<tr>
<td>tgname1:tgcontext1</td>
<td></td>
</tr>
<tr>
<td>tname2:tgcontext2</td>
<td></td>
</tr>
<tr>
<td>max-register-sustain-rate</td>
<td>0</td>
</tr>
</tbody>
</table>
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        sg1
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 NetNet 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

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

Totals:
SGTest          D   120   0.0      0     359   0.0      0  0.000  0.000     5   0     0

ACMEPACKET#
```

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     5   0     0

192.168.200.61 I  120  0.0  0  359  0.0  0  0.000  0.000  5  0  0  0

Totals:
SGTest          D   120   0.0      0     359   0.0      0  0.000  0.000     5   0     0

ACMEPACKET#
```
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

<table>
<thead>
<tr>
<th>SAG</th>
<th>Active</th>
<th>Rate</th>
<th>ConEx</th>
<th>Active</th>
<th>Rate</th>
<th>ConEx</th>
<th>Avg</th>
<th>Max</th>
<th>Burst</th>
</tr>
</thead>
<tbody>
<tr>
<td>testgroup</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
<td>0</td>
</tr>
</tbody>
</table>

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#

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
```

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 agentconfig 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
```
Display information for each of the configured H.323 stacks by using the `show h323d h323stats` command.

```
ACMEPACKET# show h323d h323stats
```

<table>
<thead>
<tr>
<th>STACK</th>
<th>H.225 : Sent</th>
<th>Recd</th>
<th>H.245 : Msg</th>
<th>Ack</th>
<th>Rej</th>
<th>Rel</th>
<th>RAS : Req</th>
<th>Ack</th>
<th>Rej</th>
<th>maxCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>h323172</td>
<td>585622</td>
<td>764844</td>
<td>976289</td>
<td>1171626</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>h323192</td>
<td>586040</td>
<td>585622</td>
<td>976087</td>
<td>1171626</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The display identifies the H.323 stack by its name and then provides the data described in the following table.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.225</td>
<td>Number of H.225 messages sent and received by this H.323 stack</td>
</tr>
<tr>
<td>H.245</td>
<td>Number of H.245 requests, acknowledgements, rejections, and releases sent and received by this H.323 stack</td>
</tr>
<tr>
<td>RAS</td>
<td>Number of RAS requests, acks, and rejects sent and received by this H.323 stack</td>
</tr>
</tbody>
</table>

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.

```
amepacket# show h323d h323stats h323172
```

<table>
<thead>
<tr>
<th>STACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>h323172</td>
</tr>
</tbody>
</table>

**H.225 STATISTICS**

<table>
<thead>
<tr>
<th>MESSAGE TYPE</th>
<th>SENT</th>
<th>RECD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>200118</td>
<td>0</td>
</tr>
<tr>
<td>Call Proceeding</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alerting</td>
<td>0</td>
<td>200112</td>
</tr>
<tr>
<td>Connect</td>
<td>0</td>
<td>200109</td>
</tr>
<tr>
<td>Progress</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Facility</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Release Complete</td>
<td>199906</td>
<td>191628</td>
</tr>
<tr>
<td>Status</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Status Inquiry</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Notify</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Info</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**H.245 STATISTICS (Total)**

<table>
<thead>
<tr>
<th>MESSAGE TYPE</th>
<th>MSG</th>
<th>ACK</th>
<th>REJ</th>
<th>REL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Slave</td>
<td>200110</td>
<td>400218</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Terminal Capability</td>
<td>400218</td>
<td>400218</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OpenLogical Channel</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CloseLogical Channel</td>
<td>399812</td>
<td>399812</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Statistic</td>
<td>Type</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.225 STATISTICS</td>
<td></td>
<td>Statistics about the H.225.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MESSAGE TYPE</td>
<td>Type of messages sent and received by this H.323 stack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENT</td>
<td>For each type of message specified in the MESSAGE TYPE column, how many of the message types were sent by this H.323 stack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECD</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.245 STATISTICS Total</td>
<td></td>
<td>Statistics about the H.245.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MESSAGE TYPE</td>
<td>Type of H.245 messages sent and received by this H.323 stack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSG</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REJ</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 ?
```

<table>
<thead>
<tr>
<th>Statistic Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REL</td>
<td>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.</td>
</tr>
<tr>
<td>RAS STATISTICS FOR MESSAGES</td>
<td>There are two sections of RAS statistics: one for SENT (or issued) and one for RECD (or received.</td>
</tr>
<tr>
<td>MESSAGE TYPE</td>
<td>Type of RAS messages sent and received by this H.323 stack.</td>
</tr>
<tr>
<td>REQ</td>
<td>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.</td>
</tr>
<tr>
<td>CON</td>
<td>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.</td>
</tr>
<tr>
<td>REJ</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>State</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGCP Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CA Endpoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GW Endpoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Server Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pending MBCD</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MGCP ALGs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

-------- Gateway --------- ------- Call Agent --------

<table>
<thead>
<tr>
<th>MGCP Transactions</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Duplicates received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Retransmissions sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

ACMEPACKET#
```

About State Statistics

The State section displays information about MGCP sessions, connections, and transactions, which are defined in the following table.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGCP Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Media Sessions</td>
<td>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).</td>
</tr>
<tr>
<td>Client Trans</td>
<td>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.</td>
</tr>
<tr>
<td>Server Trans</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>Number of requests received by the Net-Net SBC from the gateway and call agent.</td>
</tr>
<tr>
<td>Responses sent</td>
<td>Number of responses sent back by the Net-Net SBC to the gateway and call agent in response to the requests received.</td>
</tr>
<tr>
<td>Duplicates Received</td>
<td>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.</td>
</tr>
<tr>
<td>Requests Sent</td>
<td>Number of requests sent by the Net-Net SBC to the gateway and call agent.</td>
</tr>
<tr>
<td>Responses Received</td>
<td>Number of responses received from the gateway and call agent in response to the requests sent by the Net-Net SBC.</td>
</tr>
<tr>
<td>Retransmissions Sent</td>
<td>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.</td>
</tr>
</tbody>
</table>

- **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, NFTYs, CRCXs, MDCXs, DLCXs, and AUEPs

```
ACMEPACKET# show algd all
14:15:22-168

State

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Period</th>
<th>PerMax</th>
<th>High</th>
<th>Lifetime</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGCP Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CA Endpoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GW Endpoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Sessions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Server Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pending MBCD</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MGCP ALGs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

--------- Gateway ---------

MGCP Transactions

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Period</th>
<th>Total</th>
<th>PerMax</th>
<th>Lifetime</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Duplicates received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses received</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Retransmissions sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

----------- Call Agent -----------

MGCP Media Events

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Lifetime</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling SDP Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Called SDP Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Media Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Application Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Exp Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Early Media Exps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Exp Media Drops</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

--------- Lifetime ---------

MGCP ACL Status

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Period</th>
<th>PerMax</th>
<th>High</th>
<th>Lifetime</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Trusted</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Blocked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

ACL Operations

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Requests</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Promotions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Demotions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---< NO DATA AVAILABLE >---(RSIP)
---< NO DATA AVAILABLE >---(RQNT)
---< NO DATA AVAILABLE >---(NFTY)
---< NO DATA AVAILABLE >---(CRCX)
---< NO DATA AVAILABLE >---(MDCX)
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 on 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.

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling SDP Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Called SDP Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Drop Media Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Transaction Errors</td>
<td>Number of errors in continuing the processing of the MGCP transaction associated with setting up or tearing down of the media session.</td>
</tr>
<tr>
<td>Application Errors</td>
<td>Number of miscellaneous errors that occur in the MGCP ALG application that are otherwise uncategorized.</td>
</tr>
</tbody>
</table>
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 rsip
20:43:05-195

Media Exp Events

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSIP incoming:</td>
<td>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 mbcd errors display.</td>
</tr>
<tr>
<td>RSIP outgoing:</td>
<td></td>
</tr>
</tbody>
</table>

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             ------ Lifetime -----  
                   Current      Total     PerMax
Incoming Calls              0          0          0
Rejected Calls              0          0          0
Diverted Calls              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
```

230 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide  Version S-C6.2.0
<table>
<thead>
<tr>
<th></th>
<th>7430</th>
<th>7518</th>
<th>7828</th>
<th>3346410</th>
<th>11604</th>
<th>8002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used Ports</td>
<td>572</td>
<td>724</td>
<td>7724</td>
<td>3338980</td>
<td>11132</td>
<td>8000</td>
</tr>
<tr>
<td>Port Sorts</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>14796</td>
<td>4156</td>
<td></td>
</tr>
<tr>
<td>MBC Trans</td>
<td>1141</td>
<td>1234</td>
<td>5748</td>
<td>2503147</td>
<td>8440</td>
<td>2974</td>
</tr>
<tr>
<td>MBC Ignored</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ARP Trans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

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  Lifetime
Active      High    Total  Total  PerMax  High
Sessions    0   0   0     0   0   0
Subscriptions 0   0   0     0   0   0
Dialogs     0   0   0     0   0   0
CallID Map  0   0   0     0   0   0
Rejections   -  -   0     0   0   0
ReINVITES   -  -   0     0   0   0
Media Sessions 0   0   0     0   0   0
Media Pending 0   0   0     0   0   0
Client 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   0
DNS Trans   0   0   0     0   0   0
DNS Sockets 0   0   0     0   0   0
DNS Results 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
```

```
BEGIN PKCS7-----
MIIDRwYJKoZIhvcNAQcCoI1ODDCzA2QCAQExADADBgEAlIDjEDCCAYAwggKjQoAMC
AQICCAI1EAAeXMA0GCSqGSIb3DQEBBQUAMHAXCzAIBoGVBAYTA1VTMRWmEQYDV
VOQIDwpDVxpm9ybmihMHREwDQYJKoZIhvcNAQcCoIBAQQDAgMB0GCSqGSIb3DQ
EBBQUAMHAXCzAIBoGVBAYTA1VTMRWmEQYDV
```

This is the certificate in PEM form.
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 ACLI `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] [brief | detail] [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
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
finger-print:
finger-print-raw:
```

**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@ac-linux.acmepacket.com"
finger-print:
finger-print-raw:
pub-key:
AAAAB3NzaC1yc2EAAAABAQwAAAEQAXApY5GYJKBi52URsdwOLrKtAlvDNzyK3HftqHsVWhWCEDmtdGcKqr+AAT4d/7jug+otJTg8xzlZZZcsL2Fbi056Wi431H6d8B1QCHSNQnLdUj3YfxbiiEOy++ElPiBAgifeEzjY7swCcnUdcgsU0DA27/HzSP/tdldvEAwtfef+Yu5uB07vpmSGlvzNhkpWhkZ4EyHvXQoafvbXpNnlO6j0JHvcli3yPvZ42zIL9fuwhm+hYKmpZ57NUnkoXpmC3VDEVqvd0GvzrBNjZ2RkJUqMq92kFnjXgEKLYTF3zp7/fArUn4crDxkzKPF170+sap05k1hDkx3UDWV8e1S0q=
Modulus (2048 bit):
00:c4:fc:b9:19:88:ca:06:2e:76:51:1b:1d:c0:e2:
eb:2a:80:0b:bc:33:73:c8:ad:c7:16:0b:6a:1:e:c5:
70:85:66:5c:10:0e:aa:4c:67:00:78:01:87:
32:fb:33:0e:20:40:82:27:3:c:ee:36:3b:3:00:
82:9d:47:5c:82:5c:03:03:6e:ff:1f:34:8b:fe:d6:
```
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 five 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.™ “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:

- \texttt{shell:priv-lvl=15} — User automatically logged in as an administrator
- \texttt{shell:priv-lvl=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 \texttt{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.

\textbf{To view information for public keys in brief format:}

1. In Superuser mode, type \texttt{show security ssh-pub-key brief}, and the log-in name for the public key you want to see. Then press <Enter>.

\begin{verbatim}
ACMEPACKET# show security ssh-pub-key brief jdoe
\end{verbatim}

Your display will resemble the following example:

\begin{verbatim}
login-name:
  jdoe
finger-print:
finger-print-raw:
\end{verbatim}

1. In Superuser mode, type \texttt{show security pub-key detail}, and the log-in name for the public key you want to see. Then press <Enter>.

\begin{verbatim}
ACMEPACKET# show security ssh-pub-key detail msmith
\end{verbatim}

Your display will resemble the following example:

\begin{verbatim}
login-name:
  msmith
comment:
\end{verbatim}
Importing a Public Key Record

This section shows you how to import a public key record. Note that the processes require 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-public-key import jdoe

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"
AAAAB3NzaC1yc2EAAAADAgAAAQEA7OBf08jJe7MSMgerjDTgZt5jMjS5v3v6AEN2pYiZiI7xZismmpooO19kkj56s/ljGStEzqXMHKHUr9mB
qvELQbqbowEi5sz2AP31GUpjQTCKZRF1XOQx8A44vHZCum9j/fNRSnWQ1mhHmaZMmF2L
hOr4j/NlvpvpsvprordlV6Fhtz5eriVgocxDrjNcVtsAMYLPdDl6e9XebOZQGS92TrPuK
/yzLj2G5NVfmx05i+FvdHz1vBdv505y2QPj/iiz1u3TA/307tyntB0b7beDylrg64Azc
G7E3AgI/H49LhBtIQ/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-public-key` commands.

```
ACMEPACKET# ssh-pub-key delete jdoe
SSH public key deleted successfully....
WARNING: Configuration changed, run 'save-config' command.
```

```
ACMEPACKET# ssh-pub-key delete jdoe
record (jdoe) 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.
2. 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 type    state
----- ---------- --------------------- ----- -------- ------- -----
0 0x0225c400                           0 00:03:42 console  priv
1 0x0225e260      10.0.200.40:4922     1 00:03:24 telnet  priv *
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
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 <Link>Note on Backwards Compatibility (246) 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 (245) 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 (245) 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 (245).

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 confirm to the <Link>Password Requirements (245) 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
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

Currently active (137) and saved configurations (138) do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET#

3. 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

4. Continue with the process described in the <Link>Setting a Protected Configuration Password: Matching Configurations (248).

---

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:**

1. Carry out the process described in the <Link>Setting a Protected Configuration Password: Matching Configurations (248).

2. 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
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 carrying out the <Link>Setting a Protected Configuration Password: Matching Configurations (248) 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`
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# verify-config
   Checking configuration data...
   OK: configuration password is in sync with the configuration data
   ```

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# backup-config copyConfig1
   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# delete-config
   ```

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-config copyConfig1
   Need to perform save-config and activate/reboot activate for changes to take effect...
   task done
   ```

6. Before activating the configuration, verify it.

   ```
   ACMEPACKET2# verify-config
   ```
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(security)# password-policy
   ACMEPACKET(system-config)#

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 systime-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# systime-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

The timezone on the Net-Net ESD must be set manually via the ACLI using one of two methods:

- using the `timezone-set` command at the root prompt. This command starts a timezone wizard that allows you to answer prompts specifically related to timezone settings. You can set your timezone location and the wizard automatically sets the daylight savings time for the location you select.

- at the path `system->timezone`. This parameter allows you to create a timezone name and apply specific instructions for daylight savings time (DST) and specify the number of minutes from Coordinated Universal Time (UTC). If you initiated the “timezone-set” wizard previous to accessing this parameter, the settings for `system->timezone` are already populated. You can change them if required.

It is recommended you set the timezone after first boot of the system.

About UTC Timezones

Coordinated Universal Time (UTC) is used as the official world reference for time. Coordinated Universal Time replaced the use of Greenwich Mean Time (GMT) in 1972. Sometimes time zones are represented similar to UTC - 5h or GMT - 5h. In this example, the (-5h) refers to that time zone being five hours behind UTC or GMT and so forth for the other time zones. UTC +5h or GMT +5h would refer to that time zone being five hours ahead of UTC of GMT and so forth for the other time zones.

The usage of UTC and GMT is based upon a twenty four hour clock, similar to military time, and is based upon the 0° longitude meridian, referred to as the Greenwich meridian in Greenwich, England.

UTC is based on cesium-beam atomic clocks, with leap seconds added to match earth-motion time, where as Greenwich Mean Time is based upon the Earth’s rotation and celestial measurements. UTC is also known as Zulu Time or Z time.

In areas of the United States that observe Daylight Saving Time, local residents move their clocks ahead one hour when Daylight Saving Time begins. As a result, their UTC or GMT offset would change from UTC -5h or GMT - 5h to UTC -4h or GMT - 4h. In places not observing Daylight Saving Time the local UTC or GMT offset will remain the same year round. Arizona, Puerto Rico, Hawaii, U.S. Virgin Islands and American Samoa do not observe Daylight Saving Time.

In the United States Daylight Saving Time begins at 2:00 a.m. local time on the second Sunday in March. On the first Sunday in November areas on Daylight Saving Time return to Standard Time at 2:00 a.m. The names in each time zone change along with Daylight Saving Time. Eastern Standard Time (EST) becomes Eastern Daylight Time (EDT), and so forth. A new federal law took effect in March 2007 which extends Daylight Saving Time by four weeks.

The United States uses nine standard time zones. From east to west they are Atlantic Standard Time (AST), Eastern Standard Time (EST), Central Standard Time (CST), Mountain Standard Time (MST), Pacific Standard Time (PST), Alaskan Standard Time (AKST), Hawaii-Aleutian Standard Time (HST), Samoa standard time (UTC-11) and Chamorro Standard Time (UTC+10). The following tables identify the standard time zone boundaries and the offsets.
### Standard Timezone Boundaries Table

<table>
<thead>
<tr>
<th>Coordinated Universal Time (UTC)</th>
<th>Greenwich Mean Time (GMT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTC/GMT +0</td>
<td>UTC/GMT +0</td>
</tr>
</tbody>
</table>

### Timezone Offsets Table

<table>
<thead>
<tr>
<th>Time Zone in United States</th>
<th>Examples of places in the United States using these Time Zones</th>
<th>United States GMT/UTC Offsets</th>
<th>UTC Offset Standard Time</th>
<th>UTC Offset Daylight Saving Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic</td>
<td>Puerto Rico, US Virgin Islands</td>
<td></td>
<td>UTC - 4h</td>
<td>N/A</td>
</tr>
<tr>
<td>Eastern</td>
<td>Connecticut, Delaware, Florida, Georgia, part of Indiana, part of Kentucky, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, part of Tennessee, Vermont, Virginia and West Virginia</td>
<td></td>
<td>UTC - 5h</td>
<td>UTC - 4h</td>
</tr>
<tr>
<td>Central</td>
<td>Alabama, Arkansas, Florida, Illinois, part of Indiana, Iowa, part of Kansas, part of Kentucky, Louisiana, part of Michigan, Minnesota, Mississippi, Missouri, Nebraska, North Dakota, Oklahoma, part of South Dakota, part of Tennessee, most of Texas, and Wisconsin</td>
<td></td>
<td>UTC - 6h</td>
<td>UTC - 5h</td>
</tr>
<tr>
<td>Mountain</td>
<td>Arizona*, Colorado, part of Idaho, part of Kansas, Montana, part of Nebraska, New Mexico, part of North Dakota, part of Oregon, part of South Dakota, part of Texas, Utah, and Wyoming</td>
<td></td>
<td>UTC - 7h</td>
<td>UTC - 6h</td>
</tr>
<tr>
<td>Pacific</td>
<td>California, part of Idaho, Nevada, most of Oregon, Washington</td>
<td></td>
<td>UTC - 8h</td>
<td>UTC - 7h</td>
</tr>
<tr>
<td>Alaska</td>
<td>Alaska and a portion of the Aleutian Islands that is east of 169 degrees 30 minutes west longitude observes the Alaska Time Zone.</td>
<td></td>
<td>UTC - 9h</td>
<td>UTC - 8h</td>
</tr>
<tr>
<td>Hawaii - Aleutian</td>
<td>Hawaii and a portion of the Aleutian Islands that is west of 169 degrees 30 minutes west longitude observes the Hawaii-Aleutian Standard Time Zone. Although Hawaii does not observe daylight saving time the Aleutian Islands do observe daylight saving time.</td>
<td></td>
<td>UTC - 10h</td>
<td>UTC - 9h</td>
</tr>
</tbody>
</table>
You can configure the timezone on the Net-Net ESD by running a `timezone-set` wizard from the root location via the ACLI. Use the following procedure to configure the Net-Net ESD timezone.

**Note:** The procedure described below may display different prompts depending on whether your system is running on VXWorks or LINUX.

**To configure the timezone:**

1. At the root prompt, enter `timezone-set` and press <Enter>.

```
ACMEPACKET# timezone-set
```

The following displays.

```
==========================================
Calling tzselect. Use ^D to cancel without save
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.

#?
==========================================
```

2. Enter the number corresponding to the continent or ocean you want to select, and press <Enter>.

   or

   Enter `none` to specify the time zone using the Portable Operating System Interface (POSIX) timezone format.

**Note:** For a procedure to configure timezones using POSIX format, see <Link>Configuring Timezone using POSIX Format</Link> (259).

```
#? 2
```

The following displays.

```
==========================================
Please select a country.
1) Anguilla
2) Antigua & Barbuda
3) Argentina
4) Aruba
5) Bahamas
6) Barbados
7) Belize
8) Bolivia
```

9) Bonaire Sint Eustatius & Saba
10) Brazil
11) Canada
12) Cayman Islands
13) Chile
14) Colombia
15) Costa Rica
16) Cuba
17) Curacao
18) Dominica
19) Dominican Republic
20) Ecuador
21) El Salvador
22) French Guiana
23) Greenland
24) Grenada
25) Guadeloupe
26) Guatemala
27) Guyana
28) Haiti
29) Honduras
30) Jamaica
31) Martinique
32) Mexico
33) Montserrat
34) Nicaragua
35) Panama
36) Paraguay
37) Peru
38) Puerto Rico
39) Sint Maarten
40) St Barthélemy
41) St Kitts & Nevis
42) St Lucia
43) St Martin (French part)
44) St Pierre & Miquelon
45) St Vincent
46) Suriname
47) Trinidad & Tobago
48) Turks & Caicos Is
49) United States
50) Uruguay
51) Venezuela
52) Virgin Islands (UK)
53) Virgin Islands (US)
#?
3. Enter the number corresponding to the country you want to select, and press <Enter>.

#? 49

The following displays.

==========================================
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Time - Navajo
21) Mountain Standard Time - Arizona
22) Pacific Time
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Metlakatla Time - Annette Island
30) Hawaii

#?
4. Enter the number corresponding to the time zone region you want to select, and press <Enter>.

#? 1

The following displays.

=================================================================
The following information has been given:

United States
Eastern Time

Therefore TZ='America/New_York' will be used.
Local time is now: Wed Mar 13 11:18:52 EDT 2013.
Is the above information OK?
1) Yes
2) No
#?
=================================================================

5. Enter 1 (Yes), and press <Enter>.
or
Enter 2 (No) to go back to Step 2 and enter the correct timezone information.

#? 1

The following displays.

=================================================================

You have completed the timezone-set wizard.

Configuring Timezone using POSIX Format

If you want to configure the timezone using POSIX format, you can select the option "none - I want to specify the time zone using the Posix TZ format." in Step 2 of the timezone-set wizard.

To set the timezone using POSIX format:

1. At the root prompt, enter timezone-set and press <Enter>.

   ACMEPACKET# timezone-set

   The following displays.

   ==============================================================

   Calling tzselect. Use ^D to cancel without save
   Please identify a location so that time zone rules can be set correctly.
   Please select a continent or ocean.
   1) Africa
   2) Americas
   3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) None - I want to specify the time zone using the Posix TZ format.

2. Enter 11, and press <Enter>.

#? 11

The following displays.

Please enter the desired value of the TZ environment variable. For example, GST-10 is a zone named GST that is 10 hours ahead (east) of UTC.

3. Enter the UTC/GMT value for your location. For valid UTC/GMT values, see the <Link>Timezone Offsets Table (255).

#? UTC-10

The following displays.

The following information has been given:

TZ='UTC-10'

Therefore TZ='UTC-10' will be used.
Local time is now: Thu Apr 11 02:50:18 UTC 2013.
Is the above information OK?
1) Yes
2) No
#?
4. Enter 1 (Yes), and press <Enter>.  
   or  
   Enter 2 (No) to go back to Step 2 and enter the correct timezone information.  
   #? 1  
   The following displays. If you specified a value that does not relate to your Net-Net ESD location, a warning displays.  
   
   Timezone=UTC-10  
   WARNING: custom timezone will apply to application only.  
   ACMEPACKET#  
   
   You have completed the timezone-set wizard.  

   Manually Setting Timezone  

   Optionally, you can manually configure the timezone on the Net-Net ESD using the ACLI at the path system->timezone. Use the following procedure to configure the Net-Net ESD timezone.  

   To configure the timezone:  

   1. In Superuser mode, type configure terminal and press <Enter>.  
      ACMEPACKET# configure terminal  
      ACMEPACKET(configure)#  
   2. Type system and press <Enter>.  
      ACMEPACKET(configure)# system  
      ACMEPACKET(system)#  
   3. Type timezone and press <Enter>.  
      ACMEPACKET(system)# timezone  
      ACMEPACKET(timezone)#  
   4. name—Enter a name for this timezone configuration. Valid values are alphanumeric characters.  
   5. minutes-from-utc—Enter the number of minutes that represents the offset from the standard timezone boundary (+0). So for the Atlantic timezone (Puerto Rico and US Virgin Islands), you can enter the time zone as 240 (UTC -4h or 4 x 60 = 240 minutes). Default is zero (0). Valid values must be entered as positive integers as indicated in the following table.  

<table>
<thead>
<tr>
<th>UTC Hours</th>
<th>Minute Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (default)</td>
<td>Standard Timezone Boundary for UTC/GMT</td>
</tr>
<tr>
<td>1</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>3</td>
<td>180</td>
</tr>
<tr>
<td>4</td>
<td>140</td>
</tr>
<tr>
<td>5</td>
<td>300</td>
</tr>
<tr>
<td>6</td>
<td>360</td>
</tr>
<tr>
<td>7</td>
<td>420</td>
</tr>
</tbody>
</table>
6. `dst-start-month`—Enter the start month for daylight savings time (DST). Default is 1. Valid values must be entered as positive integers as indicated in the following table.

<table>
<thead>
<tr>
<th>Month</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>1 (default)</td>
</tr>
<tr>
<td>February</td>
<td>2</td>
</tr>
<tr>
<td>March</td>
<td>3</td>
</tr>
<tr>
<td>April</td>
<td>4</td>
</tr>
<tr>
<td>May</td>
<td>5</td>
</tr>
<tr>
<td>June</td>
<td>6</td>
</tr>
<tr>
<td>July</td>
<td>7</td>
</tr>
<tr>
<td>August</td>
<td>8</td>
</tr>
<tr>
<td>September</td>
<td>9</td>
</tr>
<tr>
<td>October</td>
<td>10</td>
</tr>
<tr>
<td>November</td>
<td>11</td>
</tr>
<tr>
<td>December</td>
<td>12</td>
</tr>
</tbody>
</table>

7. `dst-start-day`—Enter the starting day in the month for DST. Valid values are 1 to 31. Default is 1. Valid values must be entered as positive integers.

8. `dst-start-weekday`—Enter the starting weekday for DST. Default is `sunday`. Valid values are:

- `sunday` (default)
- `monday`
- `tuesday`
- `wednesday`
- `thursday`
- `friday`
- `saturday`

9. `dst-start-hour`—Enter the starting hour for DST. Valid values are 0 to 23. Default is 1.
10. **dst-start-rule**—Enter the starting rule to assign to this timezone configuration. This rule is dependant on the “dst-start-weekday” AND the “dst-start-month” parameters. If the dst-start-weekday parameter is set to **sunday**, “dst-start-month” is set to **March**, and the “dst-start-rule” is set to **third**, DST is set to begin on the third sunday of March. Default is **disabled** (no rule applied). Valid values are:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Use dst-start-month, dst-start-day, and dst-start-hour; the dst-start-weekday parameter is ignored. If set to an ordinal number, the dst-start-weekday is used and the dst-start-day parameter is ignored.</td>
</tr>
<tr>
<td>four</td>
<td>Start DST on the fourth Sunday of the month.</td>
</tr>
<tr>
<td>third</td>
<td>Start DST on the third Sunday of the month.</td>
</tr>
<tr>
<td>first</td>
<td>Start DST on the first Sunday of the month.</td>
</tr>
<tr>
<td>last</td>
<td>Start DST on the last Sunday of the month.</td>
</tr>
<tr>
<td>second</td>
<td>Start DST on the second Sunday of the month.</td>
</tr>
<tr>
<td>static</td>
<td>Use dst-start-month, dst-start-day, and dst-start-hour; the dst-start-weekday parameter is ignored. If set to an ordinal number, the dst-start-weekday is used and the dst-start-day parameter is ignored.</td>
</tr>
</tbody>
</table>

11. **dst-end-month**—Enter the ending month for daylight savings time (DST). Default is 1. Valid values must be entered as positive integers as indicated in the following table.

<table>
<thead>
<tr>
<th>Month</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>1 (default)</td>
</tr>
<tr>
<td>February</td>
<td>2</td>
</tr>
<tr>
<td>March</td>
<td>3</td>
</tr>
<tr>
<td>April</td>
<td>4</td>
</tr>
<tr>
<td>May</td>
<td>5</td>
</tr>
<tr>
<td>June</td>
<td>6</td>
</tr>
<tr>
<td>July</td>
<td>7</td>
</tr>
<tr>
<td>August</td>
<td>8</td>
</tr>
<tr>
<td>September</td>
<td>9</td>
</tr>
<tr>
<td>October</td>
<td>10</td>
</tr>
<tr>
<td>November</td>
<td>11</td>
</tr>
<tr>
<td>December</td>
<td>12</td>
</tr>
</tbody>
</table>

12. **dst-end-day**—Enter the ending day in the month for DST. Valid values are 1 to 31. Default is 1. Valid values must be entered as positive integers.

13. **dst-end-weekday**—Enter the ending weekday for DST. Default is **sunday**. Valid values are:

- Sunday (default)
- Thursday
- Monday
- Friday
14. **dst-end-hour**—Enter the ending hour for DST. Valid values are 0 to 23. Default is 1.

15. **dst-end-rule**—Enter the ending rule to assign to this timezone configuration. This rule is dependent on the “dst-end-weekday” AND the “dst-end-month” parameters. If the dst-end-weekday parameter is set to **sunday**, “dst-end-month” is set to **November**, and the “dst-end-rule” is set to **last**, DST is set to end on the last Sunday of November. Default is **disabled** (no rule applied). Valid values are:

- **disabled** (default) - Disables DST rules
- **third** - End DST on the third Sunday of the month.
- **static** - Net-Net ESD uses dst-end-month, dst-end-day, and dst-end-hour; the dst-end-weekday parameter is ignored. If set to an ordinal number, the dst-end-weekday is used and the dst-end-day parameter is ignored.
- **fourth** - End DST on the fourth Sunday of the month.
- **first** - End DST on the first Sunday of the month.
- **last** - End DST on the last Sunday of the month.
- **second** - End DST on the second Sunday of the month

16. Save and activate your configuration.

**Displaying the System Timezone**

You can display the timezone configured for your Net-Net SBC using the ACLI **show timezone** command from the root prompt.

```
ACMEPACKET# show timezone
America/New_York
ACMEPACKET#
```

To show more specific information about timezone settings, such as daylight savings time, navigate to the timezone parameter at the path `configure terminal->system>` and initiate the **show** command. The following example shows the results from the show command.

```
ACMEPACKET(timezone)# show timezone
name TimezoneA
minutes-from-utc 240
dst-start-month 1
dst-start-day 1
dst-start-weekday sunday
dst-start-hour 1
dst-start-rule disabled
dst-end-month 1
dst-end-day 1
dst-end-weekday sunday
dst-end-hour 1
dst-end-rule disabled
```
**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 server` command.

- The traps for when a server is unreachable and then again reachable are: `apSysMgmtNTPServerUnreachableTrap` and `apSysMgmtNTPServerUnreachableClearTrap`
- 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:
   ```plaintext
   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:
   ```plaintext
   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>.
   ```plaintext
   ACMEPACKET(ntp-config)# del-server 18.26.4.105
   ```

**Monitoring NTP from the ACLI**

NTP server information that you can view with the new `show ntp server` 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:

<table>
<thead>
<tr>
<th>Display Column</th>
<th>Definition</th>
</tr>
</thead>
</table>
| server         | Lists the NTP servers configured on the Net-Net SBC by IP address. Entries are accompanied by characters:  
  • 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. |
| 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:

1. At the command line, type `show ntp server` and press <Enter>.

   ACMEPACKET# show ntp server
   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:

1. 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
LOGTask     logTask     0x2134c80  8144   312   360    7784
nPwbTmr     0x0000776828 0x219e9c0 20432   168  5016   15416
tcli        cliInterface 0x21086870 65488  3136 11920   53568
tcliclTelnet 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 mbcd 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.”

<table>
<thead>
<tr>
<th>Acme Packet syslog Level (numerical code)</th>
<th>syslog Severity Level (number) From RFC 3164</th>
<th>Acme Packet Code Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency (1)</td>
<td>Emergency (0)</td>
<td>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.</td>
</tr>
<tr>
<td>Critical (2)</td>
<td>Alert (1)</td>
<td>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.</td>
</tr>
<tr>
<td>Major (3)</td>
<td>Critical (2)</td>
<td>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.</td>
</tr>
<tr>
<td>Minor (4)</td>
<td>Error (3)</td>
<td>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.</td>
</tr>
<tr>
<td>Warning (5)</td>
<td>Warning (4)</td>
<td>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.</td>
</tr>
<tr>
<td>Notice (6)</td>
<td>Notice (5)</td>
<td>These log levels are used for Acme Packet customer support purposes.</td>
</tr>
<tr>
<td>Info (7)</td>
<td>Informational (6)</td>
<td>These log levels are used for Acme Packet customer support purposes.</td>
</tr>
<tr>
<td>Trace (8)</td>
<td>Debug (7)</td>
<td>These log levels are used for Acme Packet customer support purposes.</td>
</tr>
<tr>
<td>Debug (9)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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:

   ```
   notify <task_name> <action> [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.

   ```
   notify all|<process-name> trace all|<socket-address><file-name> [outudp-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 `<filename>`.

**Notify Subcommands**

The table below lists and defines the subcommands and additional capabilities that are included in the notify command.

<table>
<thead>
<tr>
<th>notify Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALGD</td>
<td></td>
</tr>
<tr>
<td>notify algd nolog</td>
<td>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).</td>
</tr>
<tr>
<td>notify algd log</td>
<td>This command enables the logging of MIBOCO and MGCP messages in the alg.log.</td>
</tr>
<tr>
<td>notify Subcommand</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>notify algd mgcp-</td>
<td>This command deletes the session and the corresponding gateway entries for a specific gateway. The &quot;endpointid&quot; 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.</td>
</tr>
<tr>
<td>endpoint:&lt;endpoint id&gt;</td>
<td></td>
</tr>
<tr>
<td>BERPD</td>
<td></td>
</tr>
<tr>
<td>notify berpd force</td>
<td>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.</td>
</tr>
<tr>
<td>MBCD</td>
<td></td>
</tr>
<tr>
<td>notify mbcd nolog</td>
<td>This command disables MIBOCO logging.</td>
</tr>
<tr>
<td>notify mbcd log</td>
<td>This command enables MIBOCO logging in the miboco.log.</td>
</tr>
<tr>
<td>notify mbcd debug</td>
<td>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.</td>
</tr>
<tr>
<td>notify mbcd nodebug</td>
<td>This command disables setting the log level for MBCD. This command is used for debugging purposes.</td>
</tr>
<tr>
<td>RADD</td>
<td></td>
</tr>
<tr>
<td>notify radd reload</td>
<td>This command changes the configurations for RADIUS dynamically by reloading the configuration data in the account-config.</td>
</tr>
<tr>
<td>SIPD</td>
<td></td>
</tr>
<tr>
<td>notify sipd reload</td>
<td>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.</td>
</tr>
<tr>
<td>notify sipd nosiplog</td>
<td>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.</td>
</tr>
<tr>
<td>notify sipd siplog</td>
<td>This command enables the logging of SIP and MIBOCO messages in the sipmsg.log.</td>
</tr>
<tr>
<td>notify sipd report</td>
<td>This command writes all SIP process statistics to the log file.</td>
</tr>
<tr>
<td>notify sipd dump limit</td>
<td>This command writes CPU limit information to the log file.</td>
</tr>
<tr>
<td>notify sipd debug</td>
<td>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.</td>
</tr>
<tr>
<td>notify sipd nodebug</td>
<td>This command disables setting the log level for the SIP protocol for some SIP activity. This command is used for debugging purposes.</td>
</tr>
</tbody>
</table>
**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 (right): ON
Power Supply B (left): 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
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.
**activate** is the same as issuing the **activate-config** command and then a **reboot** force.

<table>
<thead>
<tr>
<th>reboot Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot activate</td>
<td>This subcommand reboots the Net-Net SBC and activates the newly saved configuration.</td>
</tr>
<tr>
<td>reboot force</td>
<td>This subcommand reboots the Net-Net SBC and loads the last running configuration without confirmation.</td>
</tr>
<tr>
<td>reboot force activate</td>
<td>This subcommand reboots the Net-Net SBC and activates the newly saved configuration without confirmation.</td>
</tr>
</tbody>
</table>

### 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.

```plaintext
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.

```plaintext
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.

```plaintext
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.

```plaintext
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
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA_flow_key</td>
<td>Source IPv4 address key used for matching in the look-up process.</td>
</tr>
<tr>
<td>DA_flow_key</td>
<td>Destination IPv4 address key used for matching in the look-up process.</td>
</tr>
<tr>
<td>SP_flow_key</td>
<td>UDP source port used for matching in the look-up process.</td>
</tr>
<tr>
<td>DP_flow_key</td>
<td>UDP destination port used for matching in the look-up process.</td>
</tr>
<tr>
<td>VLAN_flow_key</td>
<td>If this is a non-zero value, then there is an associated VLAN. If this value is zero, then there is no associated VLAN.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA_prefix</td>
<td>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.</td>
</tr>
<tr>
<td>DA_prefix</td>
<td></td>
</tr>
<tr>
<td>SP_prefix</td>
<td></td>
</tr>
<tr>
<td>DP_prefix</td>
<td></td>
</tr>
<tr>
<td>Protocol_flow_key</td>
<td>This value stands for the protocol used, where the following values and protocols correspond:</td>
</tr>
<tr>
<td></td>
<td>• 1 = ICMP</td>
</tr>
<tr>
<td></td>
<td>• 6 = IP</td>
</tr>
<tr>
<td></td>
<td>• 17 = UDP</td>
</tr>
<tr>
<td>Ingress_flow_key</td>
<td>This value uniquely identifies from where the packet came, and it is a combination of the Ingress Slot and Ingress Port values.</td>
</tr>
<tr>
<td>Ingress Slot</td>
<td>Together with the Ingress Port, this value makes up the Ingress_flow_key.</td>
</tr>
<tr>
<td>Ingress Port</td>
<td>Together with the Ingress Slot, this value makes up the Ingress_flow_key.</td>
</tr>
<tr>
<td>XSA_data_entry</td>
<td>This is the translated (i.e., post-lookup) source IPv4 address value.</td>
</tr>
<tr>
<td>XDA_data_entry</td>
<td>This is the translated (i.e., post-lookup) destination IPv4 address value.</td>
</tr>
<tr>
<td>XSP_data_entry</td>
<td>This is the translated (i.e., post-lookup) source port value.</td>
</tr>
<tr>
<td>XDP_data_entry</td>
<td>This is the translated (i.e., post-lookup) destination port value.</td>
</tr>
<tr>
<td>Egress_data_entry</td>
<td>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.</td>
</tr>
<tr>
<td>Egress Slot</td>
<td>Together with the Egress Port, this value makes up the Egress_data_entry.</td>
</tr>
<tr>
<td>Egress Port</td>
<td>Together with the Egress Slot, this value makes up the Egress_data_entry.</td>
</tr>
<tr>
<td>flow_action</td>
<td>This value displays the defined flow_action (i.e., flag) bits. The flow_action bit mask includes the following bit options:</td>
</tr>
<tr>
<td></td>
<td>• bit 1 - 1=MPLS strip</td>
</tr>
<tr>
<td></td>
<td>• bit 2 - 1=Diffserv clear</td>
</tr>
<tr>
<td></td>
<td>• bit 5 - 1=Latch source address</td>
</tr>
<tr>
<td></td>
<td>• bit 6 - 1=Collapse flow</td>
</tr>
<tr>
<td></td>
<td>• bit 7 - 1=Slow Path</td>
</tr>
<tr>
<td></td>
<td>• bit 8 - 1=QoS Requirement</td>
</tr>
<tr>
<td></td>
<td>• bit 9 - 1=RTCP, 0=RTP is bit 8 is set</td>
</tr>
<tr>
<td></td>
<td>• bit 10 - 1=packet capture if bit 8 is set</td>
</tr>
<tr>
<td></td>
<td>• bit 11 - 1=full packet capture, 0=header packet capture, if bit 9 is set Bits 8 through 11 only apply to QOS.</td>
</tr>
<tr>
<td>optional_data</td>
<td>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.</td>
</tr>
<tr>
<td>VLAN_data_entry</td>
<td>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.</td>
</tr>
<tr>
<td>host_table_index</td>
<td>This value refers to the virtual index for the host management of CAM processing.</td>
</tr>
<tr>
<td>init_flow_guard</td>
<td>This timer is used to age the entries in the CAM.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inact_flow_guard</td>
<td>This timer is used to age the entries in the CAM.</td>
</tr>
<tr>
<td>max_flow_guard</td>
<td>This timer is used to age the entries in the CAM.</td>
</tr>
</tbody>
</table>

This timer is used to age the entries in the CAM.
• 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-community-table
community-name : public
access-mode : READ-ONLY
ip-addresses : 10.0.200.61
               172.30.0.13
total requests in : 111
total responses out : 111

community-name : test
access-mode : READ-ONLY
ip-addresses : 172.30.0.13
               10.0.200.61
total requests in : 21
total responses out : 21

community-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-community-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 creates 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.log 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.
Inventory Management

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

<table>
<thead>
<tr>
<th>Assy, Session Director with CAM</th>
<th>Part Number:</th>
<th>Serial Number:</th>
<th>Functional Rev:</th>
<th>Board Rev:</th>
<th>PCB Family Type:</th>
<th>ID:</th>
<th>Format Rev:</th>
<th>Options:</th>
<th>Manufacturer:</th>
<th>Week/Year:</th>
<th>Sequence Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>102-1001-00</td>
<td>010323001127</td>
<td>1.18</td>
<td>2</td>
<td>Session Director</td>
<td></td>
<td>3</td>
<td>0</td>
<td>MSL, Lowell</td>
<td>23/2003</td>
<td>001127</td>
</tr>
</tbody>
</table>
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
```

Number of MAC Addresses: 16
Starting MAC Address: 00 08 25 01 07 60
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.
```
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:

```
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.

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>to-file</td>
<td>Send output from this command to a file located on the local flash system file system.</td>
</tr>
<tr>
<td>account-config</td>
<td>Account configuration</td>
</tr>
<tr>
<td>h323-config</td>
<td>H323 configuration</td>
</tr>
<tr>
<td>h323-stack</td>
<td>All h323 stacks</td>
</tr>
<tr>
<td>iwf-stack</td>
<td>SIP/H.323 IWF stack</td>
</tr>
<tr>
<td>host-route</td>
<td>All host routes</td>
</tr>
<tr>
<td>local-policy</td>
<td>All local policies</td>
</tr>
<tr>
<td>media-profile</td>
<td>All media profiles</td>
</tr>
<tr>
<td>media-manager</td>
<td>Media manager</td>
</tr>
<tr>
<td>mgcp-config</td>
<td>MGCP configuration</td>
</tr>
<tr>
<td>dns-config</td>
<td>All DNS configurations</td>
</tr>
<tr>
<td>network-interface</td>
<td>All network interfaces</td>
</tr>
<tr>
<td>Subcommand</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>ntp-config</td>
<td>NTP configuration</td>
</tr>
<tr>
<td>phys-interface</td>
<td>All physical interfaces</td>
</tr>
<tr>
<td>realm</td>
<td>All realms</td>
</tr>
<tr>
<td>MediaPolicy</td>
<td>All media policies</td>
</tr>
<tr>
<td>ClassPolicy</td>
<td>All class policies</td>
</tr>
<tr>
<td>redundancy-config</td>
<td>Redundancy configuration</td>
</tr>
<tr>
<td>ResponseMap</td>
<td>All response maps</td>
</tr>
<tr>
<td>session-agent</td>
<td>All session agents</td>
</tr>
<tr>
<td>session-group</td>
<td>All session groups</td>
</tr>
<tr>
<td>session-translation</td>
<td>All session translations</td>
</tr>
<tr>
<td>translation-rules</td>
<td>All translation rules</td>
</tr>
<tr>
<td>session-router</td>
<td>Session router</td>
</tr>
<tr>
<td>sip-config</td>
<td>All SIP configurations</td>
</tr>
<tr>
<td>sip-feature</td>
<td>All SIP features</td>
</tr>
<tr>
<td>sip-interface</td>
<td>All SIP interfaces</td>
</tr>
<tr>
<td>sip-nat</td>
<td>All SIP NATs</td>
</tr>
<tr>
<td>snmp-community</td>
<td>All SNMP communities</td>
</tr>
<tr>
<td>static-flow</td>
<td>All static flows</td>
</tr>
<tr>
<td>steering-pool</td>
<td>All steering pools</td>
</tr>
<tr>
<td>system-config</td>
<td>System configuration</td>
</tr>
<tr>
<td>TrapReceiver</td>
<td>All trap receivers</td>
</tr>
<tr>
<td>call-recording-server</td>
<td>All IP call recording servers</td>
</tr>
<tr>
<td>capture-receiver</td>
<td>All capture receivers</td>
</tr>
<tr>
<td>rph-profile</td>
<td>All RPH profiles</td>
</tr>
<tr>
<td>rph-policy</td>
<td>All RPHP policies</td>
</tr>
<tr>
<td>password-policy</td>
<td>Password policy</td>
</tr>
<tr>
<td>enforcement-profile</td>
<td>All enforcement profiles</td>
</tr>
<tr>
<td>realm-group</td>
<td>All realm groups</td>
</tr>
<tr>
<td>inventory</td>
<td>Displays an inventory of all configured elements</td>
</tr>
</tbody>
</table>

**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
  subseq-guard-timer 300
  tcp-flow-time-limit 86400
  tcp-initial-guard-timer 300
  tcp-subseq-guard-timer 300
  tcp-number-of-ports-per-flow 2
  hnt-rtcp disabled
  algd-log-level NOTICE
  mbcd-log-level NOTICE
  red-flow-port 1985
  red-mgcp-port 1986
  red-max-trans 10000
  red-sync-start-time 5000
  red-sync-comp-time 1000
  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
```

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
   mbcd-log-level              NOTICE
   red-flow-port               1985
   red-mgcp-port               1986
   red-max-trans               10000
   red-sync-start-time         5000
   red-sync-comp-time          1000
   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
```

**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
     mm-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
     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
```
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
realm-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 localhost
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

account-server
hostname 172.30.11.15
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
```
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>1813</td>
</tr>
<tr>
<td>State</td>
<td>enabled</td>
</tr>
<tr>
<td>Min-Round-Trip</td>
<td>250</td>
</tr>
<tr>
<td>Max-Inactivity</td>
<td>60</td>
</tr>
<tr>
<td>Restart-Delay</td>
<td>30</td>
</tr>
<tr>
<td>Bundle-VSA</td>
<td>enabled</td>
</tr>
<tr>
<td>Secret</td>
<td>foo</td>
</tr>
<tr>
<td>NAS-ID</td>
<td></td>
</tr>
<tr>
<td>Last-Modified-Date</td>
<td>2006-03-01 22:37:33</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Source-Port</td>
<td>1812</td>
</tr>
<tr>
<td>Type</td>
<td>local</td>
</tr>
<tr>
<td>Protocol</td>
<td>pap</td>
</tr>
<tr>
<td>Certificate-Record</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>State</td>
<td>MA</td>
</tr>
<tr>
<td>Locality</td>
<td>Burlington</td>
</tr>
<tr>
<td>Organization</td>
<td>Acme</td>
</tr>
<tr>
<td>Unit</td>
<td>Packet</td>
</tr>
<tr>
<td>Common-Name</td>
<td>Ap</td>
</tr>
<tr>
<td>Key-Size</td>
<td>1024</td>
</tr>
<tr>
<td>Alternate-Name</td>
<td>RS</td>
</tr>
<tr>
<td>Trusted</td>
<td>enabled</td>
</tr>
<tr>
<td>H323-Config</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>enabled</td>
</tr>
<tr>
<td>Log-Level</td>
<td>INFO</td>
</tr>
<tr>
<td>Response-Tmo</td>
<td>4</td>
</tr>
<tr>
<td>Connect-Tmo</td>
<td>32</td>
</tr>
<tr>
<td>RFC2833-Payload</td>
<td>101</td>
</tr>
<tr>
<td>Alternate-Routing</td>
<td>Proxy</td>
</tr>
<tr>
<td>Last-Modified-Date</td>
<td>2006-07-07 07:49:57</td>
</tr>
<tr>
<td>H323-Stack</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Tester</td>
</tr>
<tr>
<td>State</td>
<td>disabled</td>
</tr>
<tr>
<td>IsGateway</td>
<td>enabled</td>
</tr>
<tr>
<td>Realm-ID</td>
<td>Test</td>
</tr>
<tr>
<td>Assoc-Stack</td>
<td>Acme</td>
</tr>
<tr>
<td>Local-IP</td>
<td>172.30.1.150</td>
</tr>
<tr>
<td>Max-Calls</td>
<td>100</td>
</tr>
<tr>
<td>Max-Channels</td>
<td>10</td>
</tr>
<tr>
<td>Registration-TTL</td>
<td>15</td>
</tr>
<tr>
<td>Terminal-Alias</td>
<td>e164=17823484839</td>
</tr>
<tr>
<td>Prefixes</td>
<td></td>
</tr>
<tr>
<td>RAS-Port</td>
<td></td>
</tr>
<tr>
<td>Auto-GK-Discovery</td>
<td>enabled</td>
</tr>
<tr>
<td>Multicast</td>
<td>172.30.1.150:11</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>170.30.1.150:57</td>
</tr>
<tr>
<td>GK-Identifier</td>
<td>RS</td>
</tr>
<tr>
<td>Q931-Port</td>
<td>1720</td>
</tr>
<tr>
<td>Alternate-Transport</td>
<td>173.30.1.150:15</td>
</tr>
</tbody>
</table>
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
g931-start-port: 0
g931-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
test_realm: test_realm
enum-servers: 172.3.11.115
timeout: 11
activityTimer: 3600
last-modified-date: 2006-07-07 07:37:11
iwf-stack:
  state: disabled
media-profiles: disabled
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: 172.168.0.10
  action: none
  terminate-recursion: enabled
  carrier:

294 Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide  Version S-C6.2.0
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
decactivate-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-rtpc                       disabled
alg-log-level                 NOTICE
mbcd-log-level                 NOTICE
red-flow-port                  1985
red-mgcp-port                  1986
red-max-trans                  10000
red-sync-start-time            5000
red-sync-comp-time             1000
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

mgcp-config
private-realm                  RS
private-address                172.30.1.150
private-port                   11
public-realm                   acme
public-ca-host                 packet
public-ca-address              170.2.30.150
public-ca-port                 15
public-gw-host                 rs
public-gw-address              150.20.1.158
public-gw-port                 20
second-public-gw-port          22
alg-port                       2427
mode                           LineUnit
divisor                         256
unit-prefix
audit-interval                 0
nat-traversal                  disabled
dns-authentication             disabled
dns-translation
ca-redundancy                  disabled
caping-method
ca-ping-interval               0
cap-failover-ip-addresses      175.30.1.150
last-modified-date             2006-07-07 12:42:25

dns-config
client-realm                   dns_realm
description                   test description
client-address-list
10.0.0.1
192.168.10.1
17.16.0.1
server-dns-attributes
  server-realm
  domain-suffix
  server-address-list
  source-address
  source-port 3973
  transaction-timeout 19136512

network-interface
  name f00
  sub-port-id 0
  hostname
  ip-address 10.10.0.10
  pri-utility-addr
  sec-utility-addr
  netmask 255.255.0.0
  gateway 10.10.0.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  hip-ip-list
  ftp-address
  icmp-address
  snmp-address
  telnet-address
  last-modified-date 2006-06-13 16:41:09

network-interface
  name f01
  sub-port-id 0
  hostname
  ip-address 10.10.0.11
  pri-utility-addr
  sec-utility-addr
  netmask 255.255.0.0
  gateway 10.10.0.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
INVENTORY MANAGEMENT

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

gos-enable disabled

max-bandwidth 0
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext-policy-svr</td>
<td>boffo.com</td>
</tr>
<tr>
<td>max-latency</td>
<td>0</td>
</tr>
<tr>
<td>max-jitter</td>
<td>0</td>
</tr>
<tr>
<td>max-packet-loss</td>
<td>0</td>
</tr>
<tr>
<td>observe-window-size</td>
<td>0</td>
</tr>
<tr>
<td>parent-realm</td>
<td></td>
</tr>
<tr>
<td>dns-realm</td>
<td></td>
</tr>
<tr>
<td>media-policy</td>
<td></td>
</tr>
<tr>
<td>in-translationid</td>
<td></td>
</tr>
<tr>
<td>out-translationid</td>
<td></td>
</tr>
<tr>
<td>in-manipulationid</td>
<td></td>
</tr>
<tr>
<td>out-manipulationid</td>
<td></td>
</tr>
<tr>
<td>class-profile</td>
<td></td>
</tr>
<tr>
<td>average-rate-limit</td>
<td>0</td>
</tr>
<tr>
<td>access-control-trust-level</td>
<td>low</td>
</tr>
<tr>
<td>invalid-signal-threshold</td>
<td>0</td>
</tr>
<tr>
<td>maximum-signal-threshold</td>
<td>0</td>
</tr>
<tr>
<td>untrusted-signal-threshold</td>
<td>758</td>
</tr>
<tr>
<td>deny-period</td>
<td>30</td>
</tr>
<tr>
<td>symmetric-latching</td>
<td>disabled</td>
</tr>
<tr>
<td>pai-strip</td>
<td>disabled</td>
</tr>
<tr>
<td>trunk-context</td>
<td></td>
</tr>
<tr>
<td>early-media-allow</td>
<td>reverse</td>
</tr>
<tr>
<td>additional-prefixes</td>
<td>10.0.0.0/24, 172.16.0.0</td>
</tr>
<tr>
<td>restricted-latching</td>
<td>peer-ip</td>
</tr>
<tr>
<td>restriction-mask</td>
<td>17</td>
</tr>
<tr>
<td>accounting-enable</td>
<td>enabled</td>
</tr>
<tr>
<td>last-modified-date</td>
<td>2006-07-06 12:43:39</td>
</tr>
<tr>
<td>realm-config</td>
<td></td>
</tr>
<tr>
<td>identifier</td>
<td>testrealm</td>
</tr>
<tr>
<td>addr-prefix</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>network-interfaces</td>
<td></td>
</tr>
<tr>
<td>mm-in-realm</td>
<td>disabled</td>
</tr>
<tr>
<td>mm-in-network</td>
<td>enabled</td>
</tr>
<tr>
<td>mm-same-ip</td>
<td>enabled</td>
</tr>
<tr>
<td>mm-in-system</td>
<td>disabled</td>
</tr>
<tr>
<td>mm-release</td>
<td>disabled</td>
</tr>
<tr>
<td>qos-enable</td>
<td>disabled</td>
</tr>
<tr>
<td>max-bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>ext-policy-svr</td>
<td>boffo.com</td>
</tr>
<tr>
<td>max-latency</td>
<td>0</td>
</tr>
<tr>
<td>max-jitter</td>
<td>0</td>
</tr>
<tr>
<td>max-packet-loss</td>
<td>0</td>
</tr>
<tr>
<td>observe-window-size</td>
<td>0</td>
</tr>
<tr>
<td>parent-realm</td>
<td></td>
</tr>
<tr>
<td>dns-realm</td>
<td></td>
</tr>
<tr>
<td>media-policy</td>
<td></td>
</tr>
<tr>
<td>in-translationid</td>
<td></td>
</tr>
<tr>
<td>out-translationid</td>
<td></td>
</tr>
<tr>
<td>in-manipulationid</td>
<td></td>
</tr>
<tr>
<td>out-manipulationid</td>
<td></td>
</tr>
<tr>
<td>class-profile</td>
<td></td>
</tr>
<tr>
<td>average-rate-limit</td>
<td>0</td>
</tr>
</tbody>
</table>
access-control-trust-level     low
invalid-signal-threshold       0
maxum-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
realm-config
identifier                     testrealm
addrs-prefix                  0.0.0.0
network-interfaces
mm-in-realm                   disabled
mm-in-network                 enabled
mm-same-ip                    enabled
mm-in-system                  disabled
mm-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
maxum-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
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

observing-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: 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

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
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
divide-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-real-m-id
egress-real-m-id
nat-mode None
INVENTORY MANAGEMENT

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-callid-lifetime 600
pac-user-lifetime 3600
red-sip-port 1988
red-max-trans 10000
red-sync-start-time 5000
red-sync-comp-time 1000
add-reason-header disabled
sip-message-len 4096
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
disable-privacy
trust-mode
call
max-nat-interval
3600
nat-int-increment
10
nat-test-increment
30
sip-dynamic-hnt
disabled
stop-recuse
401, 407
port-map-start
0
port-map-end
0
in-manipulationid
out-manipulationid
disable-privacy
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
pass
charging-vector-mode
charge function-address-mode
pass
ccf-address
ecf-address
term-tgrp-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
flmrtv
last-modified-date
2005-02-15 10:33:24
snmp-community
community-name
public
access-mode
READ-ONLY
ip-addresses
<table>
<thead>
<tr>
<th>Static Flow</th>
<th>10.0.1.42</th>
</tr>
</thead>
<tbody>
<tr>
<td>in-realm-id</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>in-source</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>in-destination</td>
<td>test100</td>
</tr>
<tr>
<td>out-realm-id</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>out-source</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>out-destination</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>protocol</td>
<td>UDP</td>
</tr>
<tr>
<td>alg-type</td>
<td>none</td>
</tr>
<tr>
<td>average-rate-limit</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Steering-Pool</th>
<th>2006-07-07 12:08:20</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>192.168.200.100</td>
</tr>
<tr>
<td>start-port</td>
<td>10000</td>
</tr>
<tr>
<td>end-port</td>
<td>60000</td>
</tr>
<tr>
<td>realm-id</td>
<td>h323192</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Surrogate-Agent</th>
<th>2005-05-25 01:28:52</th>
</tr>
</thead>
<tbody>
<tr>
<td>register-host</td>
<td>acme</td>
</tr>
<tr>
<td>register-user</td>
<td>enabled</td>
</tr>
<tr>
<td>description</td>
<td></td>
</tr>
<tr>
<td>customer-host</td>
<td></td>
</tr>
<tr>
<td>customer-next-hop</td>
<td>175.3.11.157</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TLS Profile</th>
<th>2006-07-07 12:56:06</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>test</td>
</tr>
<tr>
<td>end-entity-certificate</td>
<td>enabled</td>
</tr>
<tr>
<td>trusted-ca-certificates</td>
<td>enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Config</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>acme</td>
</tr>
<tr>
<td>location</td>
<td>burlington</td>
</tr>
<tr>
<td>mib-system-contact</td>
<td></td>
</tr>
<tr>
<td>mib-system-name</td>
<td></td>
</tr>
<tr>
<td>mib-system-location</td>
<td></td>
</tr>
<tr>
<td>snmp-enabled</td>
<td>enabled</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session capacity</td>
<td>Determines the maximum number of sessions allowed by a Net-Net system for all protocols combined: SIP, MGCP, H.323, and SIP&lt;–&gt;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.</td>
</tr>
<tr>
<td>SIP</td>
<td>Enables SIP signaling.</td>
</tr>
<tr>
<td>H.323</td>
<td>Enables H.323 signaling.</td>
</tr>
<tr>
<td>SIP&lt;–&gt;H.323</td>
<td>Enables SIP&lt;–&gt;H.323 IWF signaling. In order to run IWF between these two protocols, you must also have valid SIP and H.323 licenses.</td>
</tr>
<tr>
<td>MGCP</td>
<td>Enables MGCP signaling.</td>
</tr>
<tr>
<td>QoS</td>
<td>Enables measurement for QoS (jitter, packet latency, and packet loss) on the Net-Net SBC.</td>
</tr>
<tr>
<td>ACP</td>
<td>Enables the Net-Net SBC to respond to ACP requests. Required for Net-Net EMS use.</td>
</tr>
<tr>
<td>Routing policies</td>
<td>Establishes routing policies on the Net-Net SBC.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Establishes distribution of traffic across gateways, application servers, softswitches, and so on.</td>
</tr>
<tr>
<td>Accounting</td>
<td>Establishes RADIUS servers to which the Net-Net SBC can make connections and send CDRs.</td>
</tr>
<tr>
<td>HA</td>
<td>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.</td>
</tr>
<tr>
<td>PAC</td>
<td>Enables the Net-Net system to operate in a PAC configuration with other Net-Net systems.</td>
</tr>
</tbody>
</table>

**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 ACLI 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
   ```

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,
```
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 -- Period -- -------- Lifetime --------
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 -- Period -- -------- Lifetime --------
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#
```
6 Net-Net 4250 Upgrading

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 51.64 Seconds 185.65 Kbytes/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 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 required 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

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-C6.1.0, 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 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
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.


4. Verify the configuration.

5. Confirm synchronization settings. (You can back out of the upgrade after this step—see HA Backout Procedure 2 (354).)

6. Force Net-Net SBC1 to become the active peer, and verify that is has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release S-C6.2.0 software image.


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# 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 `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-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 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/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 : booothost
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.


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
```

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 (353) in this chapter’s HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 (353) 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 (354) in this chapter’s HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 (353) 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.
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# 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

   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.


4. Verify the configuration.

5. Confirm synchronization settings. (You can back out of the upgrade after this step—see HA Backout Procedure 2 (357).)

6. Force Net-Net SBC1 to become the active peer, and verify that is has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release S-C6.1.0 software image.
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# 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 `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-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
   
   NETNETSBC1# configure terminal
   NETNETSBC1(configure)# bootparam
   ```

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.


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 (356) in this chapter's HA Backout Procedures: Release S-C6.2.0 to Release S-C6.1.0 (353) 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 (359) in this chapter’s HA Backout Procedures: Release C5.1 to Release C5.0 (358) 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
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**

   
   boot device : wancom0
   processor number : 0
   host name : boothost
   file name : /tffs0/nnC500xxx.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 boot params on Net-Net SBC1 to boot from the new Release C6.0 software image.


4. Verify the configuration.

5. Confirm synchronization settings. (You can back out of the upgrade after this step—see **HA Backout Procedure 2 (359)**.)

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.
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 `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 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

<table>
<thead>
<tr>
<th>boot device</th>
<th>wancom0</th>
</tr>
</thead>
<tbody>
<tr>
<td>processor number</td>
<td>0</td>
</tr>
<tr>
<td>host name</td>
<td>boothost</td>
</tr>
<tr>
<td>file name</td>
<td>/tffs0/nnC510xxx.gz /tffs0/nnC600xxx.gz</td>
</tr>
</tbody>
</table>
```

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.


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
```

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 (358) in this chapter's HA Backout Procedures: Release C5.1 to Release C5.0 (358) 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 (359) in this chapter’s HA Backout Procedures: Release C5.1 to Release C5.0 (358) 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
   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.


4. Verify the configuration.

5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA 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 Release C5.1 software image.


9. Confirm that Net-Net SBC2 is running the Release C5.1 software image.
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# 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 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.


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
```

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 (358)` in this chapter’s `HA Backout Procedures: Release C5.1 to Release C5.0 (358)` 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 (359)` in this chapter’s `HA Backout Procedures: Release C5.1 to Release C5.0 (358)` 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.

```bash
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 `/ttfs0/` 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.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see **HA Backout Procedure 2** (367).)
6. Force Net-Net SBC1 to become the active peer, and verify that is has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release C5.0 software image.
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.

```plaintext
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.

```plaintext
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.

```plaintext
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 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 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.


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
```

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** (366) in this chapter’s **HA Backout Procedures: Release C5.0 to Release 4.1 (361)** 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 (367)** in this chapter’s **HA Backout Procedures: Release C5.0 to Release 4.1 (361)** 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.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see HA 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 Release 4.1 software image.
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 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 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.


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 (363) in this chapter’s HA Backout Procedures: Release C5.0 to Release 4.1 (361) 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 (364) in this chapter’s HA Backout Procedures: Release C5.0 to Release 4.1 (361) 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:**

1. 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.

2. Verify the integrity of your Release 2.x configuration using the ACLI verify-config command.

3. 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.

1. 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-remaining boot
   boot: 29759488/29760512 bytes (99%) remaining
   ACMEPACKET#
   ```

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 4.0 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 `/ttfs0/SBC210xxx.gz` and `/ttfs0/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 : /ttfs0/SBC210xxx.gz /ttfs0/SBC400xxx.gz
```

Note that `/ttfs0/` 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.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see [HA 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 Release 4.0 software image.
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 CLI `show health` command to make sure that all processes are synchronized.

1b. On Net-Net SBC1, show the current configuration version by using the CLI `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 CLI `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 CLI `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 `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 4.0 software image.

4a. Access the boot parameters on Net-Net SBC1:

- In the CLI 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.
NET-NET SBC1# configure terminal
NET-NET SBC1(configure)# bootparam

'.' = clear field; ' ' = go to previous field; ^D = quit

boot device : wancom0
processor number : 0
host name : booothost
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.


5. After Net-Net SBC1 has completed the boot process, use the verify-config command to confirm that the configuration has been upgraded properly.

NET-NET SBC1# verify-config

6. Confirm the Net-Net SBC1 is running the new boot image using the show version command.

NET-NET SBC1# show version
ACME Firmware 4.0.0
01/31/06
NET-NET SBC1#

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 (366) in this chapter’s HA Backout Procedures: Release 4.0 to Release 2.0/2.1 (366) section.

8. Initiate a switchover on Net-Net SBC1.

NET-NET SBC1# 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.

NET-NET SBC2# 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 (367) in this chapter’s HA Backout Procedures: Release 4.0 to Release 2.0/2.1 (366) 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:

1. 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.

2. Verify the integrity of your Release 2.0/2.1 configuration using the ACLI verify-config command.

3. 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.

Upgraded 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.

1. 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#
   ```

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 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

<table>
<thead>
<tr>
<th>boot device</th>
<th>wancom0</th>
</tr>
</thead>
<tbody>
<tr>
<td>processor number</td>
<td>0</td>
</tr>
<tr>
<td>host name</td>
<td>boothost</td>
</tr>
<tr>
<td>file name</td>
<td>/tffs0/SBC210xxx.gz /tffs0/SBC220xxx.gz</td>
</tr>
</tbody>
</table>

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.
4. Verify the configuration.
5. Confirm synchronization settings. (You can back out of the upgrade after this step—see HA Backout Procedure 2 (367).)
6. Force Net-Net SBC1 to become the active peer, and verify that is has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Release 2.2 software image.
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.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 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
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.


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 (366) in this chapter’s HA Backout Procedures: Release 4.0 to Release 2.0/2.1 (366) 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 (367) in this chapter’s HA Backout Procedures: Release C5.0 to Release 4.1 (361) 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
   ```
boot device          : wancom0
processor number     : 0
host name            : boothost
file name            : /ttfs0/SBC200xxx.gz /ttfs0/SBC210xxx.gz

Note that /ttfs0/ 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.
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 is has done so.
7. Change the bootparams on Net-Net SBC2 to boot from the new Net-Net SBC Release 2.1 software image.
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 diags.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.


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 (371) in this chapter’s HA Backout Procedures: Release 2.1 to Release 2.0 (371) section.


   NETNETSBC1# notify 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 health

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-config

13. After you have saved the configuration on Net-Net SBC1, use the ACLI activate-config command to activate the configuration.

   NETNETSBC1# activate-config

   Note: At this point, if you need to revert to Release 2.0 for any reason, use HA Backout Procedure 2 (373) in this chapter’s HA Backout Procedures: Release 2.1 to Release 2.0 (371) 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 health

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.


```
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 bring up 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/nnSC620xxx.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/nnSC620xxx.xz
```

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# exit
NETNETSBC2#
```


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.

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 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/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.


   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 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 `/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
   NETNETSBC2(configure)# exit
   NETNETSBC2#


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.


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 the 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.


   ```
   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 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 `/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
```

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
```
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.

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.

   ```plaintext
   NETNETSBC1# show health
   ```

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:

   ```plaintext
   NETNETSBC1# configure terminal
   NETNETSBC1(configure)# bootparam
   '.' = clear field; '-' = go to previous field; '^D' = quit
   ```

   ```plaintext
   boot device          : wancom0
   processor number     : 0
   host name            : boothost
   file name            : /tffs0/nnC500xxx.gz /tffs0/sd410xxx.gz
   ```

   2b. Scroll through the boot parameters by pressing <Enter>. Stop when you reach the file name boot parameter.

   ```plaintext
   NETNETSBC1# configure terminal
   NETNETSBC1(configure)# bootparam
   ```

   ```plaintext
   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.

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# reboot
```

```
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 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 `/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 : bohost
```

```
1a. Using one of these methods, access the boot parameters on Net-Net SBC2:
```

```
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.

```
```
```
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#


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.


**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.


   ```
   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 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 /tffs0/SBC400xxx.gz and /tffs0/SBC410xxx.gz, where xxx represents the individual software numbers for these releases.

   NETNETSBC2# configure terminal
   NETNETSBC2(configure)# bootparam
   boot device            : wancom0
   processor number       : 0
   host name              : boothost
   file name              : /tffs0/SBC400xxx.gz /tffs0/SBC410xxx.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#


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.

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 health
   ```

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 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/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.

4. Confirm that Net-Net SBC1 and Net-Net SBC2 are synchronized.
   a. On both Net-Net SBCs, use the ACLI `show health` command to make sure that all processes are synchronized.
   b. 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.
   a. 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.
   b. 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(configure)# exit
NETNETSBC2#


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

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 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.


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 health
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 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/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.

   ```
   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.
   ```
   NETNETSBC1# show health
   NETNETSBC2# show health
   ```

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
   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 be 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
   
   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#


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.

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 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/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 : booothost
   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# 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
   NETNETSBC1#
   ```


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 config
   task done
   ```

6. Use the ACLI `show version` command to confirm that you are using the appropriate release.

   ```
   NETNETSBC1# show version
   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# acquire-config 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# display-current-cfg-version
   Current configuration version is 5
   NETNETSBC1#
   ```

   ```
   NETNETSBC2# display-current-cfg-version
   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 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 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 `/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
```

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
```


```
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.

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 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 (313) section of this guide’s Net-Net 4500 Upgrading (375) 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 (244) 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.

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.


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. 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
   ```
Reboot this SD [y/n]?: y
Rebooting Net-Net SBC2 causes Net-Net SBC1 to become the active system in the HA node.

9. 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 in this chapter.

10. If upgrading from a release prior to a C6 release, run the save-config command after you have confirmed that both systems are running Release C6.2.0. Saving the configuration creates a persistent configuration file in the file format data.tar.gz.

11. If you performed step 12, activate your configuration using the activate-config command.

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-C6.2.0 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 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 : bohost
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#


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.


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.

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.

   \[ \text{NETNETSBC# check-space-remaining boot} \]
   
   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.

   \[ \text{NETNETSBC1# configure terminal} \]
   \[ \text{NETNETSBC1(configure)# bootparam} \]
   
   ‘.’ = 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.


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
   ```

7. Use the ACLI `show health` command to confirm that Net-Net SBC1 is the standby system.


   ```
   NETNETSBC1# reboot
   ```

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 (389) 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 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/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#


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.


## 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.

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 `ACL1 show health` command to make sure that all processes are synchronized.

   1b. On Net-Net SBC1, show the current configuration version by using the `ACL1 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 `<Enter>`. 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/nnC600xxx.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 <Enter> to continue scrolling through the boot
parameters.


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 CX6.0.0 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.


```
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 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](#) (389) 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/nnCX600.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.

   ```

3. Using the CLI 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
   ```

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.


### 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
```

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
  BACK_UP_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
```

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. Correct the Virtual MAC address configuration established on the former device to be suitable for the new device.

   2a. Establish the base MAC needed for HA operation by, first, determining the base MAC via the ethernet address value of the `show media physical` command.

   ```
   ACMEPACKET4500# show media physical
   s0p0 (media slot 0, port 0)
   Flags: UP BROADCAST MULTICAST ARP RUNNING
   Type: ETHERNET_CSMACD
   Admin State: enabled
   Auto Negotiation: enabled
   ... Ethernet address is 00:08:25:01:08:44
   ```

   2b. Next, apply the formula for calculating virtual MAC addressing to the MAC addressing used for the Net-Net 4500 system. This formula is described in the Net-Net 4000 ACLI Configuration Guide.

   2c. Finally, configure your physical interfaces with the computed virtual MAC addressing. Refer to the command line sequence shown below as an example of this procedure.

   ```
   ACMEPACKET4500# configure terminal
   ACMEPACKET4500(configure)# system
   ACMEPACKET4500(system)# phy-interface
   ACMEPACKET4500(phy-interface)# select <name>:
   1: s0p0
   2: s1p0
   selection: 1
   ACMEPACKET4500(phy-interface)# virtual-mac 00:08:25:01:08:48
   ACMEPACKET4500(phy-interface)# done
   ````
3. Save your configuration.
   ACMEPACKET4500# save-config

4. Activate your configuration.
   ACMEPACKET4500# activate-config
8 Working with Configurations

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.

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>ACLI Command to create</th>
<th>Location of Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Configuration</td>
<td><code>done</code></td>
<td>/ramdrv/data</td>
</tr>
<tr>
<td>Last-saved Configuration</td>
<td><code>save-config</code></td>
<td>/code/config</td>
</tr>
<tr>
<td>Running Configuration</td>
<td><code>activate-config</code></td>
<td>/ramdrv/running</td>
</tr>
</tbody>
</table>

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)# exit
ACMEPACKET(system)# exit
ACMEPACKET(configure)# exit
```
2. Save all configurations to the last-saved configuration by using the `save-config` command. This step is mandatory.

```shell
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.

```shell
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:

```shell
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:

```shell
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:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>pri-utility-addr</td>
<td>Primary</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>sec-utility-addr</td>
<td>Secondary</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ip-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ftp-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>snmp-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>telnet-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dns-ip-primary</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dns-ip-backup1</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dns-ip-backup2</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hip-ip-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>icmp-address</td>
<td>Unknown</td>
<td>itself</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Steering-Pool

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>UDP</td>
<td>network-interface or realm-id</td>
<td>start-port</td>
<td>end-port</td>
</tr>
</tbody>
</table>

### SIP-Interface

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip-port address</td>
<td>transport-protocol (UDP or TCP)</td>
<td>realm-id</td>
<td>sip-port</td>
<td>0</td>
</tr>
<tr>
<td>sip-port address</td>
<td>UDP if transport-protocol is UDP</td>
<td>realm-id</td>
<td>port-map-start</td>
<td>port-map-end</td>
</tr>
</tbody>
</table>

### SIP-NAT

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext-proxy-address</td>
<td>Unknown</td>
<td>realm-id</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>home-proxy-address</td>
<td>Unknown</td>
<td>realm-id</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>home-address</td>
<td>Unknown</td>
<td>realm-id</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ext-address</td>
<td>Unknown</td>
<td>realm-id</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

* The **home-address value** must be unique across all network interfaces configured on the Net-Net SBC.

### MGCP-Config

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-address</td>
<td>UDP</td>
<td>private-realm</td>
<td>private-port</td>
<td>0</td>
</tr>
<tr>
<td>public-ca-address</td>
<td>UDP</td>
<td>public-realm</td>
<td>pub-ca-port</td>
<td>0</td>
</tr>
<tr>
<td>public-gw-address/32</td>
<td>UDP</td>
<td>public-realm</td>
<td>pub-gw-port</td>
<td>0</td>
</tr>
<tr>
<td>public-gw-address/32</td>
<td>UDP</td>
<td>public-realm</td>
<td>second-pub-gw-port</td>
<td>0</td>
</tr>
<tr>
<td>public-gw-address/32</td>
<td>UDP</td>
<td>public-realm</td>
<td>port-map-start</td>
<td>port-map-end</td>
</tr>
</tbody>
</table>
## H323-Stack

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-ip</td>
<td>TCP</td>
<td>realm-id</td>
<td>q031-port</td>
<td>0</td>
</tr>
<tr>
<td>local-ip</td>
<td>TCP</td>
<td>realm-id</td>
<td>q931-start-port</td>
<td>q931-start-port + q931-number-ports - 1</td>
</tr>
<tr>
<td>local-ip</td>
<td>TCP</td>
<td>realm-id</td>
<td>dynamic-start-port</td>
<td>dynamic-start-port + dynamic-number-port - 1</td>
</tr>
<tr>
<td>local-ip</td>
<td>UDP</td>
<td>realm-id</td>
<td>ras-port</td>
<td>0</td>
</tr>
<tr>
<td>gatekeeper</td>
<td>Unknown</td>
<td>realm-id</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>alternate-protocol</td>
<td>UDP</td>
<td>realm-id</td>
<td>it's port</td>
<td>0</td>
</tr>
</tbody>
</table>

* 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

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop</td>
<td>Unknown</td>
<td>realm</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Session-Agent

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>UDP or TCP</td>
<td>realm-id</td>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>host-name</td>
<td>UDP or TCP</td>
<td>realm-id</td>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>ip-address</td>
<td>UDP or TCP</td>
<td>egress-realm-id if no realm-id or different from it</td>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>host-name</td>
<td>UDP or TCP</td>
<td>egress-realm-id if no realm-id or different from it</td>
<td>port</td>
<td>0</td>
</tr>
</tbody>
</table>
## Static-Flow

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>in-source/32</td>
<td>Unknown</td>
<td>in-realm-id</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>in-destination/32</td>
<td>TCP or UDP</td>
<td>in-realm-id</td>
<td>start-port</td>
<td>end-port</td>
</tr>
<tr>
<td>out-source/32</td>
<td>UDP or TCP</td>
<td>out-realm-id</td>
<td>start-port</td>
<td>end-port</td>
</tr>
<tr>
<td>out-destination/32</td>
<td>Unknown</td>
<td>out-realm-id</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Capture-Receiver

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Unknown</td>
<td>network-interface</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Realm-Config

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Address Type</th>
<th>Network Interface or Realm</th>
<th>Port Start</th>
<th>Port End</th>
</tr>
</thead>
<tbody>
<tr>
<td>stun-server-ip</td>
<td>UDP</td>
<td>network-interfaces</td>
<td>stun-server-port</td>
<td>0</td>
</tr>
<tr>
<td>stun-changed-ip</td>
<td>UDP</td>
<td>network-interfaces</td>
<td>stun-changed-port</td>
<td>0</td>
</tr>
</tbody>
</table>

## Verify-Config

### Errors and Warnings

The following tables list every error and warning the verify-config command produces for each configuration element:

## Access-Control

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: access-control [id] has unsupported application-protocol [x]</td>
<td>Unsupported protocols [x]</td>
</tr>
<tr>
<td>ERROR: access-control [id] has reference to realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
</tbody>
</table>
## Account-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: account-config is enabled, but there are no account servers configured</td>
<td>State is enabled, file-output is disabled and there are not servers</td>
</tr>
<tr>
<td>WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled</td>
<td>State and file-output are enabled, there are not account servers and ftp-push is disabled</td>
</tr>
<tr>
<td>WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled</td>
<td>State and ftp-push are enabled, account servers are configured, file-output is disabled</td>
</tr>
<tr>
<td>ERROR: account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured</td>
<td>State and ftp-push are enabled, but there is no ftp-address or push-receiver configured</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which can not get password</td>
<td>Password failed decryption</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set</td>
<td>Push-receiver has no remote-path set</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have username set</td>
<td>Push-receiver has no username set</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP</td>
<td>Push-receiver has no password set for FTP</td>
</tr>
<tr>
<td>WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP</td>
<td>Push-receiver has set public key, but protocol is FTP</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have password or public key set for protocol SFTP</td>
<td>Push-receiver has no password or public key set for SFTP</td>
</tr>
<tr>
<td>ERROR: account-config has push-receiver [xyz] with reference to public-key [zyx] which does not exist</td>
<td>Public key was not found in public key table</td>
</tr>
<tr>
<td>ERROR: account-config has account-server [IP:Port] with empty secret</td>
<td>Account-server [IP:Port] has empty secret field</td>
</tr>
</tbody>
</table>

## Authentication

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: authentication has specified unsupported protocol [x] for type [y]</td>
<td>Unsupported protocols for given type</td>
</tr>
<tr>
<td>ERROR: authentication has no configured active radius servers for authentication type [x]</td>
<td>No configured active radius for given type</td>
</tr>
</tbody>
</table>

## Call-Recording-Server

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: call-recording-server must have a name</td>
<td>Name is missing</td>
</tr>
<tr>
<td>ERROR: call-recording-server [id] must have a primary-signaling-addr or primary-media-addr</td>
<td>There has to be either primary signaling or media address</td>
</tr>
</tbody>
</table>
### Capture-Receiver

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface was not found in network-interface table</td>
</tr>
</tbody>
</table>

### Certificate-Record

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: certificate-record [id] is not trusted and will not be loaded</td>
<td>Certificate record is not trusted</td>
</tr>
<tr>
<td>ERROR: certificate-record [id] cannot extract private key</td>
<td>Certificate record failed to extract the private key</td>
</tr>
<tr>
<td>ERROR: certificate-record [id] cannot convert PKCS7 string to structure</td>
<td>Failure to convert PKCS7 record to the structure</td>
</tr>
</tbody>
</table>

### Class-Policy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: class-policy [id] has reference to the media-policy [xyz] which does not exist</td>
<td>Media-policy [xyz] was not found in the media-policy table</td>
</tr>
</tbody>
</table>

### DNS-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: dns-config [id] is missing client-realm entry</td>
<td>Missing client realm</td>
</tr>
<tr>
<td>ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: dns-config [id] does not have any server-dns-attributes</td>
<td>Server-dns-attributes are missing</td>
</tr>
<tr>
<td>ERROR: dns-config [id] is missing server-realm entry</td>
<td>Realm entry is missing (source address is empty)</td>
</tr>
<tr>
<td>ERROR: dns-config [id] is missing server-realm entry for source-address [x]</td>
<td>Realm entry is missing (source address is not empty)</td>
</tr>
<tr>
<td>ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
</tbody>
</table>
## ENUM-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: enum-config [id] is missing realm-id entry</td>
<td>Missing realm</td>
</tr>
<tr>
<td>ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: enum-config [id] has no enum-servers</td>
<td>List of ENUM servers is empty</td>
</tr>
</tbody>
</table>

## Ext-Policy-Server

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: ext-policy-server [id] is missing realm entry</td>
<td>Missing realm</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] address is not valid</td>
<td>Invalid address entry</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid</td>
<td>Invalid protocol entry</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
</tbody>
</table>

## H323-Stack

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: h323-stack [id] has no realm-id</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>WARNING: h323-stack [id] is missing local-ip address entry</td>
<td>Missing address entry</td>
</tr>
<tr>
<td>WARNING: h323-stack [id] has reference to media-profile [xyz] which does not exist</td>
<td>Media profile was not found in media profile table</td>
</tr>
<tr>
<td>ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist</td>
<td>Stack name was not found in the h323-stack table</td>
</tr>
</tbody>
</table>

## Host-Route

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: host-route [id] has reference to gateway [xyz] which does not exist</td>
<td>gateway entry was not found in any network-interface object</td>
</tr>
</tbody>
</table>

## IWF-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: iwf-config has reference to media-profile [xyz] which does not exist</td>
<td>media profile was not found in media profile table</td>
</tr>
</tbody>
</table>
## Local-Policy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist</td>
<td>Source-realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>WARNING: local-policy [id] has no policy-attributes set</td>
<td>No policy-attributes set</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry</td>
<td>Next-hop is missing for given attribute</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid</td>
<td>Invalid value for the next-hop</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist</td>
<td>Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group)</td>
</tr>
<tr>
<td>WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist</td>
<td>Media-policy [xyz] was not found in media-policy table</td>
</tr>
</tbody>
</table>

## Local-Routing-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist</td>
<td>Specified file is missing from /boot/code/lrt folder</td>
</tr>
</tbody>
</table>

## MGCP-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: mgcp-config [id] is missing private-realm entry</td>
<td>Private-realm empty</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has reference to private-realm [xyz] which does not exist</td>
<td>Realm was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] is missing public-realm entry</td>
<td>Public-realm empty</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has reference to public-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has identical private-address and public-gw-address [x] for the same network interface</td>
<td>Private-address and public-gw-address are identical on same NI</td>
</tr>
</tbody>
</table>

## Network-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist</td>
<td>Phy-interface [xyz] was not found in phy-interface table</td>
</tr>
<tr>
<td>ERROR: network-interface [id] is missing pri-utility-addr entry</td>
<td>If redundancy is enabled pri-utility-addr entry has to be entered</td>
</tr>
</tbody>
</table>
### Phy-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: phy-interface [id] has invalid operation-type value [x]</td>
<td>Operation-type value is invalid</td>
</tr>
<tr>
<td>ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name</td>
<td>If type is MAINTENANCE or CONTROL name has to start with either “eth” or “wancom”</td>
</tr>
<tr>
<td>ERROR: phy-interface [id] has duplicated port [y] and slot [z] values with phy-interface [di]</td>
<td>Port and slot values are duplicated with another phy-interface</td>
</tr>
</tbody>
</table>

### Public-Key

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: public-key [id] has no public/private key pair generated for public-key [x]</td>
<td>No public/private key generated</td>
</tr>
<tr>
<td>ERROR: public-key [id] cannot extract private key</td>
<td>Cannot extract private key</td>
</tr>
</tbody>
</table>

### Realm-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which does not exist</td>
<td>Missing external BW manager</td>
</tr>
<tr>
<td>ERROR: realm-config [id] is missing entry for network-interface</td>
<td>Missing Network Interface</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network interface was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist</td>
<td>Media-policy was not found in media-policy table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist</td>
<td>Class-profile was not found in class-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist</td>
<td>In-translationid was not found in session translation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist</td>
<td>Out-translationid was not found in session translation table</td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>In-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>Out-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement-profile was not found in enforcement-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to call-recording-server-id [xyz] which does not exist</td>
<td>Call-recording-server-id was not found in call-recording-server-table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to codec-policy [xyz] which does not exist</td>
<td>Codec-policy was not found in codec-policy table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to constraint-name [xyz] which does not exist</td>
<td>Constraint-name was not found in session constraint table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to qos-constraint [xyz] which does not exist</td>
<td>Qos-constraint was not found in qos constraint table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms</td>
<td>Realm and its parent realm are part of the closed loop where they referring back to themselves</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist</td>
<td>Dns-realm doesn’t exist in the realm table</td>
</tr>
<tr>
<td>WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)</td>
<td>Realm name and parent name are the same</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to parent-realm [xyz] which does not exist</td>
<td>Parent realm doesn’t exist in the realm table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has identical stun-server-port and stun-changed port [x]</td>
<td>Stun-server-ip is identical to stun-changed-ip, when stun is enabled</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has identical stun-server-ip and stun-changed-ip [x]</td>
<td>Stun-server-port is identical to stun-changed-port, when stun is enabled</td>
</tr>
</tbody>
</table>

### Realm-Group

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist</td>
<td>Realm was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist</td>
<td>Realm was not found in realm-config table</td>
</tr>
</tbody>
</table>
## Redundancy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface (pri-utility-addr is missing here)</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr [z] from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match sec-utility-addr from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface (sec-utility-addr is missing here)</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has IP Address [x] which does not match sec-utility-addr [z] from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface [xyz] was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] is missing destination object</td>
<td>Destination object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing Primary peer object</td>
<td>Primary peer object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing Secondary peer object</td>
<td>Secondary peer object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing both Primary and Secondary peer objects</td>
<td>Primary and Secondary peer objects are missing</td>
</tr>
</tbody>
</table>

## Security-Association

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: security-association [id] is missing network-interface entry</td>
<td>Missing network-interface entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid local-ip-addr</td>
<td>Invalid local-ip-addr entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid remote-ip-addr</td>
<td>Invalid remote-ip-addr entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface</td>
<td>Network-interface is not valid IPSEC enabled media interface</td>
</tr>
<tr>
<td>ERROR: security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password</td>
<td>Failed to decrypt auth-key</td>
</tr>
<tr>
<td>ERROR: security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long</td>
<td>Invalid length of the auth-key for auth-algo [hmac-md5]</td>
</tr>
<tr>
<td>ERROR: security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long</td>
<td>Invalid length of the auth-key for auth-algo [hmac-sha1]</td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password</td>
<td>Failed to decrypt encr-key</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 64 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 192 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 128 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 256 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]</td>
<td>Has invalid aes-ctr-nonce for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)</td>
<td>Invalid tunnel-mode local-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)</td>
<td>Invalid tunnel-mode remote-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp local-ip-addr (must be non-zero)</td>
<td>Invalid espudp local-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp remote-ip-addr (must be non-zero)</td>
<td>Invalid espudp remote-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp local-port (must be non-zero)</td>
<td>Invalid espudp local-port</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp remote-port (must be non-zero)</td>
<td>Invalid espudp remote-port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security-Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Text</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid local-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid local-ip-addr-match [x]</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid remote-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid remote-ip-addr-match [x]</td>
</tr>
<tr>
<td>ERROR: security-policy [id] is missing network-interface entry</td>
</tr>
<tr>
<td>ERROR: security-policy [id] priority [x] is identical to security-policy [id2]</td>
</tr>
</tbody>
</table>
### Session-Agent

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to egress-realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist</td>
<td>Translation id was not found in translation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist</td>
<td>Translation id was not found in translation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>Manipulation id was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>Manipulation id was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement-profile was not found in enforcement-profile table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to code-policy [xyz] which does not exist</td>
<td>Codec-policy was not found in codec-policy table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to response-map [xyz] which does not exist</td>
<td>Response-map was not found in response map table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist</td>
<td>Response-map was not found in response map table</td>
</tr>
</tbody>
</table>

### Session-Group

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: session-group [id] has reference to session-agent [xyz] which does not exist</td>
<td>Session agent was not found in the session agent table</td>
</tr>
</tbody>
</table>

### Session-Translation

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: session-translation [id] has reference to rules-called [xyz] which does not exist</td>
<td>Translation rule was not found in the translation rule table</td>
</tr>
<tr>
<td>ERROR: session-translations [id] has reference to rules-calling [xyz] which does not exist</td>
<td>Translation rule was not found in the translation rule table</td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: sip-config has reference to home-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement profile was not found in enforcement profile table</td>
</tr>
<tr>
<td>WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [sip-internal-realm]</td>
<td>Missing home-realm-id, defaulted to sip-internal-realm</td>
</tr>
<tr>
<td>WARNING: sip-config home-realm-id [xyz] does not have a sip-interface</td>
<td>Sip-interface missing for the home realm</td>
</tr>
<tr>
<td>WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects</td>
<td>Nat-mode needs to be set to either Public or Private if there are sip-nat objects in the configuration</td>
</tr>
<tr>
<td>ERROR: sip-config object is disabled</td>
<td>Sip-config is disabled, but there are configured sip-interface objects</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-interface [id] is missing realm-id entry</td>
<td>missing realm</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist</td>
<td>realm was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>in-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>out-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>enforcement profile was not found in enforcement profile table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist</td>
<td>response-map was not found in response-map table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist</td>
<td>local-response-map was not found in response-map table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist</td>
<td>constraint-name was not found in session constraint table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has no sip-ports</td>
<td>sip-ports are missing</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist</td>
<td>tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist</td>
<td>ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS)</td>
</tr>
</tbody>
</table>
### SIP-Manipulation

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-manipulation [id] has no header-rules defined</td>
<td>Missing header rules</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] is missing new-value entry</td>
<td>Missing new-value entry (checked only for action type &quot;sip-manip&quot;)</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] has reference to new-value [zxy] which does not exist</td>
<td>New-value entry missing from the sip-manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] has new-value that refers to itself from sip-manipulation [di]</td>
<td>Looping reference between two objects</td>
</tr>
</tbody>
</table>

### SIP-NAT

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-nat [id] is missing home-address entry</td>
<td>Missing home-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid home-address [x] entry</td>
<td>Invalid home-address entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing ext-address entry</td>
<td>Missing ext-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid ext-address [x] entry</td>
<td>Invalid ext-address entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing ext-proxy-address entry</td>
<td>Missing ext-proxy-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry</td>
<td>Invalid ext-proxy-address entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing user-nat-tag entry</td>
<td>Missing user-nat-tag</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing host-nat-tag entry</td>
<td>Missing host-nat-tag</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing domain-suffix entry</td>
<td>Missing domain-suffix</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing realm-id entry</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] does not match sip-interface realm [xyz]</td>
<td>Sip-interface name was not found in realm table</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] does not have a sip-interface</td>
<td>Sip-interface is missing</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]</td>
<td>Duplicated user-nat-tag</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]</td>
<td>Duplicated host-nat-tag</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y]</td>
<td>Sip-nat ext-address needs to be the same as sip-port address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]</td>
<td>Duplicated home-address</td>
</tr>
</tbody>
</table>
## Static-Flow

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: static-flow [id] is missing in-realm-id entry</td>
<td>Missing in-realm-id</td>
</tr>
<tr>
<td>ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: static-flow [id] is missing out-realm-id entry</td>
<td>Missing out-realm-id</td>
</tr>
<tr>
<td>ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has illegal protocol value [xyz]</td>
<td>Invalid protocol entry</td>
</tr>
</tbody>
</table>

## Steering-Pool

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: steering-pool [id] has invalid start-port [x]</td>
<td>Invalid start-port value (smaller than 1025)</td>
</tr>
<tr>
<td>ERROR: steering-pool [id] has start-port [x] greater than end-port [y]</td>
<td>Start-port value is greater than end-port value</td>
</tr>
<tr>
<td>ERROR: steering-pool [id] is missing realm entry</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: steering-pool [id] has reference to realm [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: steering-pool [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface [xyz] was not found in network-interface table</td>
</tr>
</tbody>
</table>

## Surrogate-Agent

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: surrogate-agent [id] is missing realm entry</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing customer-next-hop entry</td>
<td>Missing customer-next-hop entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing register-contact-user entry</td>
<td>Missing register-contact-user entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing register-contact-host entry</td>
<td>Missing register-contact-host entry</td>
</tr>
</tbody>
</table>

## System-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: system-config has reference to default-gateway [xyz] which does not exist</td>
<td>Gateway was not found in the network-interface table or boot parameters</td>
</tr>
<tr>
<td>ERROR: system-config collect has sample-interval [x] greater than push-interval</td>
<td>Sample-interval greater than push-interval</td>
</tr>
</tbody>
</table>
### TLS-Profile

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates</td>
<td>End-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.</td>
<td>Bad private key for the cert-record</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist</td>
<td>Certificate record was not found in cert-record table</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has an end-entity-certificate records without any end entity certificate</td>
<td>End certificate missing from all end-entity-certificate records or none of them where imported to the SD</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length</td>
<td>Found an empty trusted-ca-record in the list</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates</td>
<td>Trusted-ca-records entry missing certificate</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] with PKCS7 structure which does not have any certificates</td>
<td>Trusted-ca-records entry with PKCS7 structure missing certificate</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not exist</td>
<td>Certificate record was not found in cert-record table</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has no trusted-ca-certificates, but mutual-authentication is enabled</td>
<td>No trusted certificates, but enabled mutual-authentication</td>
</tr>
</tbody>
</table>
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 cannot 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# 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
   ```

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# acquire-config 10.0.1.8
   ```

2. Following the procedure defined directly above, confirm that the HA node now has synchronized configurations.

   ```
   ACMEPACKET-1# display-current-cfg-version
   Current configuration version is 30
   ACMEPACKET-1# display-running-cfg-version
   Running configuration version is 30
   ACMEPACKET-2# display-current-cfg-version
   Current configuration version is 30
   ACMEPACKET-2# display-running-cfg-version
   Running configuration version is 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.

<table>
<thead>
<tr>
<th>ACLI Configuration Name</th>
<th>ACLI Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-control</td>
<td>realm-id</td>
</tr>
<tr>
<td>call-recording-server</td>
<td>primary-realm</td>
</tr>
<tr>
<td></td>
<td>secondary-realm</td>
</tr>
<tr>
<td>dns-config</td>
<td>client-realm</td>
</tr>
<tr>
<td>enum-config</td>
<td>realm-id</td>
</tr>
<tr>
<td>ext-policy-server</td>
<td>realm</td>
</tr>
<tr>
<td>h323&gt;h323-stack</td>
<td>realm-id</td>
</tr>
<tr>
<td>lawful-intercept</td>
<td>(associated parameters; specified in Net-Net LI support documentation)</td>
</tr>
<tr>
<td>local-policy</td>
<td>source-realm</td>
</tr>
<tr>
<td>mgcp-config</td>
<td>private-realm</td>
</tr>
<tr>
<td></td>
<td>public-realm</td>
</tr>
<tr>
<td>realm-config</td>
<td>identifier</td>
</tr>
<tr>
<td>session-agent</td>
<td>realm-id</td>
</tr>
<tr>
<td>sip-features</td>
<td>realm</td>
</tr>
<tr>
<td>sip-interface</td>
<td>realm-id</td>
</tr>
<tr>
<td>sip-nat</td>
<td>realm-id</td>
</tr>
<tr>
<td>static-flow</td>
<td>in-realm-id</td>
</tr>
<tr>
<td></td>
<td>out-realm-id</td>
</tr>
<tr>
<td>steering-pool</td>
<td>realm-id</td>
</tr>
<tr>
<td>surrogate-agent</td>
<td>realm-id</td>
</tr>
</tbody>
</table>

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
WORKING WITH CONFIGURATIONS

- 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 confirming 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.

<table>
<thead>
<tr>
<th>ACLI Configuration Name</th>
<th>ACLI Parameter Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-config</td>
<td>server-realm</td>
</tr>
<tr>
<td>local-policy</td>
<td>source-realm</td>
</tr>
<tr>
<td></td>
<td>next-hop</td>
</tr>
<tr>
<td></td>
<td>realm</td>
</tr>
<tr>
<td>media-manager</td>
<td>home-realm-id</td>
</tr>
<tr>
<td>realm-config</td>
<td>parent-realm</td>
</tr>
<tr>
<td></td>
<td>dns-realm</td>
</tr>
<tr>
<td></td>
<td>ext-policy-svr</td>
</tr>
<tr>
<td>realm-group</td>
<td>source-realm</td>
</tr>
<tr>
<td></td>
<td>destination-realm</td>
</tr>
<tr>
<td>session-agent</td>
<td>egress-realm</td>
</tr>
<tr>
<td>session-group</td>
<td>dest</td>
</tr>
<tr>
<td>sip-config</td>
<td>egress-realm-id</td>
</tr>
<tr>
<td></td>
<td>home-realm-id</td>
</tr>
</tbody>
</table>

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(configure)#
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.
Managing Backups and Archives

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-config 01_Feb_2005_Test running
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_config.gz
   test-config.gz
   runningcfgtest.gz
   runningtest_one.gz
   BACK_UP_CONFIG.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-config backup_file.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-config 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_HMRSI_PNAT_Overlay.gz
0606_HMRSI_Peering.gz
0605_SingleSI_PNAT_in_access.gz
0605_SingleSI_PNAT_HTN_ABBN.gz
0605_SN8_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.

<table>
<thead>
<tr>
<th>Configuration Type</th>
<th>Source Directory</th>
<th>Destination Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log</td>
<td>/ramdrv/logs</td>
<td>/code/logs</td>
</tr>
</tbody>
</table>

#### 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 All_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.lemd.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

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: access-control [id] has unsupported application-protocol [x]</td>
<td>Unsupported protocols [x]</td>
</tr>
<tr>
<td>ERROR: access-control [id] has reference to realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
</tbody>
</table>

### Account-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: account-config is enabled, but there are no account servers configured</td>
<td>State is enabled, file-output is disabled and there are not servers</td>
</tr>
<tr>
<td>WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled</td>
<td>State and file-output are enabled, there are not account servers and ftp-push is disabled</td>
</tr>
<tr>
<td>WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled</td>
<td>State and ftp-push are enabled, account servers are configured, file-output is disabled</td>
</tr>
<tr>
<td>ERROR: account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured</td>
<td>State and ftp-push are enabled, but there is no ftp-address or push-receiver configured</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which can not get password</td>
<td>Password failed decryption</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set</td>
<td>Push-receiver has no remote-path set</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have username set</td>
<td>Push-receiver has no username set</td>
</tr>
<tr>
<td>ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP</td>
<td>Push-receiver has no password set for FTP</td>
</tr>
<tr>
<td>WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP</td>
<td>Push-receiver has set public key, but protocol is FTP</td>
</tr>
<tr>
<td>Error Text</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Call-Recording-Server</td>
<td></td>
</tr>
<tr>
<td>Capture-Receiver</td>
<td></td>
</tr>
<tr>
<td>Certificate-Record</td>
<td></td>
</tr>
</tbody>
</table>

### Authentication

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: authentication has specified unsupported protocol [x] for type [y]</td>
<td>Unsupported protocols for given type</td>
</tr>
<tr>
<td>ERROR: authentication has no configured active radius servers for authentication type [x]</td>
<td>No configured active radius servers for given type</td>
</tr>
</tbody>
</table>

### Call-Recording-Server

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: call-recording-server [id] must have a name</td>
<td>Name is missing</td>
</tr>
<tr>
<td>ERROR: call-recording-server [id] must have a primary-signaling-addr or primary-media-addr</td>
<td>There has to be either primary signaling or media address</td>
</tr>
<tr>
<td>ERROR: call-recording-server [id] is missing primary-realm</td>
<td>Realm name is missing</td>
</tr>
<tr>
<td>ERROR: call-recording-server [id] has reference to the primary-realm [xyz] which does not exist</td>
<td>Primary-realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: call-recording-server [id] has reference to the secondary-realm [xyz] which does not exist</td>
<td>Secondary-realm [xyz] was not found in realm-config table</td>
</tr>
</tbody>
</table>

### Capture-Receiver

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface was not found in network-interface table</td>
</tr>
</tbody>
</table>

### Certificate-Record

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: certificate-record [id] is not trusted and will not be loaded</td>
<td>Certificate record is not trusted</td>
</tr>
<tr>
<td>ERROR: certificate-record [id] cannot extract private key</td>
<td>Certificate record failed to extract the private key</td>
</tr>
<tr>
<td>ERROR: certificate-record [id] cannot convert PKCS7 string to structure</td>
<td>Failure to convert PKCS7 record to the structure</td>
</tr>
</tbody>
</table>
### Class-Policy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: class-policy [id] has reference to the media-policy [xyz] which does not exist</td>
<td>Media-policy [xyz] was not found in the media-policy table</td>
</tr>
</tbody>
</table>

### DNS-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: dns-config [id] is missing client-realm entry</td>
<td>Missing client realm</td>
</tr>
<tr>
<td>ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: dns-config [id] does not have any server-dns-attributes</td>
<td>Server-dns-attributes are missing</td>
</tr>
<tr>
<td>ERROR: dns-config [id] is missing server-realm entry</td>
<td>Realm entry is missing (source address is empty)</td>
</tr>
<tr>
<td>ERROR: dns-config [id] is missing server-realm entry for source-address [x]</td>
<td>Realm entry is missing (source address is not empty)</td>
</tr>
<tr>
<td>ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
</tbody>
</table>

### ENUM-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: enum-config [id] is missing realm-id entry</td>
<td>Missing realm</td>
</tr>
<tr>
<td>ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: enum-config [id] has no enum-servers</td>
<td>List of ENUM servers is empty</td>
</tr>
</tbody>
</table>

### Ext-Policy-Server

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: ext-policy-server [id] is missing realm entry</td>
<td>Missing realm</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] address is not valid</td>
<td>Invalid address entry</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid</td>
<td>Invalid protocol entry</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
</tbody>
</table>
## H323-Stack

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: h323-stack [id] has no realm-id</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>WARNING: h323-stack [id] is missing local-ip address entry</td>
<td>Missing address entry</td>
</tr>
<tr>
<td>WARNING : h323-stack [id] has reference to media-profile [xyz] which does not exist</td>
<td>Media profile was not found in media profile table</td>
</tr>
<tr>
<td>ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist</td>
<td>Stack name was not found in the h323-stack table</td>
</tr>
</tbody>
</table>

## Host-Route

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: host-route [id] has reference to gateway [xyz] which does not exist in any network-interface</td>
<td>gateway entry was not found in any network-interface object</td>
</tr>
</tbody>
</table>

## IWF-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: iwf-config has reference to media-profile [xyz] which does not exist</td>
<td>media profile was not found in media profile table</td>
</tr>
</tbody>
</table>

## Local-Policy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist</td>
<td>Source-realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>WARNING: local-policy [id] has no policy-attributes set</td>
<td>No policy-attributes set</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry</td>
<td>Next-hop is missing for given attribute</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid</td>
<td>Invalid value for the next-hop</td>
</tr>
<tr>
<td>ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist</td>
<td>Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group)</td>
</tr>
<tr>
<td>WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist</td>
<td>Media-policy [xyz] was not found in media-policy table</td>
</tr>
</tbody>
</table>
### Local-Routing-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist</td>
<td>specified file is missing from /boot/code/irt folder</td>
</tr>
</tbody>
</table>

### MGCP-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: mgcp-config [id] is missing private-realm entry</td>
<td>Private-realm empty</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has reference to private-realm [xyz] which does not exist</td>
<td>Realm was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] is missing public-realm entry</td>
<td>Public-realm empty</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has reference to public-realm [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: mgcp-config [id] has identical private-address and public-gw-address [x] for the same network interface</td>
<td>Private-address and public-gw-address are identical on same NI</td>
</tr>
</tbody>
</table>

### Network-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist</td>
<td>Phy-interface [xyz] was not found in phy-interface table</td>
</tr>
<tr>
<td>ERROR: network-interface [id] is missing pri-utility-addr entry</td>
<td>If redundancy is enabled pri-utility-addr entry has to be entered</td>
</tr>
<tr>
<td>ERROR: network-interface [id] is missing sec-utility-addr entry</td>
<td>If redundancy is enabled sec-utility-addr entry has to be entered</td>
</tr>
<tr>
<td>ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty</td>
<td>Dns-domain is empty. Word “address” will be plural “addresses” if there are more DNS addresses entered</td>
</tr>
<tr>
<td>ERROR: network-interface [id] has reference to DNS address, but ip-address is empty</td>
<td>Ip-address is empty. Word “address” will be plural “addresses” if there are more DNS addresses entered</td>
</tr>
</tbody>
</table>

### Phy-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: phy-interface [id] has invalid operation-type value [x]</td>
<td>Operation-type value is invalid</td>
</tr>
<tr>
<td>ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name</td>
<td>If type is MAINTENANCE or CONTROL name has to start with either “eth” or “wancom”</td>
</tr>
<tr>
<td>ERROR: phy-interface [id] of type [x] has duplicated port [y] and slot [z] values with phy-interface [di]</td>
<td>Port and slot values are duplicated with another phy-interface</td>
</tr>
</tbody>
</table>
# Public-Key

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: public-key [id] has no public/private key pair generated for public-key [x]</td>
<td>No public/private key generated</td>
</tr>
<tr>
<td>ERROR: public-key [id] cannot extract private key</td>
<td>Cannot extract private key</td>
</tr>
</tbody>
</table>

# Realm-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which does not exist</td>
<td>Missing external BW manager</td>
</tr>
<tr>
<td>ERROR: realm-config [id] is missing entry for network-interface</td>
<td>Missing Network Interface</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network interface was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist</td>
<td>Media-policy was not found in media-policy table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist</td>
<td>Class-profile was not found in class-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist</td>
<td>In-translationid was not found in session translation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist</td>
<td>Out-translationid was not found in session translation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>In-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>Out-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement-profile was not found in enforcement-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to call-recording-server-id [xyz] which does not exist</td>
<td>Call-recording-server-id was not found in call-recording-server-table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to codec-policy [xyz] which does not exist</td>
<td>Codec-policy was not found in codec-policy table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to constraint-name [xyz] which does not exist</td>
<td>Constraint-name was not found in session constraint table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to qos-constraint [xyz] which does not exist</td>
<td>Qos-constraint was not found in qos constraint table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms</td>
<td>Realm and its parent realm are part of the closed loop where they referring back to themselves</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist</td>
<td>Dns-realm doesn’t exist in the realm table</td>
</tr>
<tr>
<td>WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)</td>
<td>Realm name and parent name are the same</td>
</tr>
</tbody>
</table>
### Realm-Group

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist</td>
<td></td>
</tr>
<tr>
<td>Realm was not found in realm-config table</td>
<td></td>
</tr>
<tr>
<td>ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist</td>
<td></td>
</tr>
<tr>
<td>Realm was not found in realm-config table</td>
<td></td>
</tr>
</tbody>
</table>

### Redundancy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface (pri-utility-addr is missing here)</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr [z] from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has Address [x] which does not match sec-utility-addr from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface (sec-utility-addr is missing here)</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has IP Address [x] which does not match sec-utility-addr [z] from network-interface [y]</td>
<td>If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface [xyz] was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: redundancy-config peer [id] is missing destination object</td>
<td>Destination object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing Primary peer object</td>
<td>Primary peer object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing Secondary peer object</td>
<td>Secondary peer object is missing</td>
</tr>
<tr>
<td>ERROR: redundancy-config is missing both Primary and Secondary peer objects</td>
<td>Primary and Secondary peer objects are missing</td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: security-association [id] is missing network-interface entry</td>
<td>Missing network-interface entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid local-ip-addr</td>
<td>Invalid local-ip-addr entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid remote-ip-addr</td>
<td>Invalid remote-ip-addr entry</td>
</tr>
<tr>
<td>ERROR: security-association [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface</td>
<td>Network-interface is not valid IPSEC media interface</td>
</tr>
<tr>
<td>ERROR: security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password</td>
<td>Failed to decrypt auth-key</td>
</tr>
<tr>
<td>ERROR: security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long</td>
<td>Invalid length of the auth-key for auth-algo [hmac-md5]</td>
</tr>
<tr>
<td>ERROR: security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long</td>
<td>Invalid length of the auth-key for auth-algo [hmac-sha1]</td>
</tr>
<tr>
<td>ERROR: security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password</td>
<td>Failed to decrypt encr-key</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 64 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 192 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 128 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 256 bits (odd parity in hex)</td>
<td>Invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]</td>
<td>Has invalid aes-ctr-nonce for given algorithm</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)</td>
<td>Invalid tunnel-mode local-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)</td>
<td>Invalid tunnel-mode remote-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp local-ip-addr (must be non-zero)</td>
<td>Invalid espudp local-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-association [id] has invalid espudp remote-ip-addr (must be non-zero)</td>
<td>Invalid espudp remote-ip-addr</td>
</tr>
</tbody>
</table>
## Security-Policy

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: security-policy [id] has invalid local-ip-addr-match</td>
<td>Empty local-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid remote-ip-addr-match</td>
<td>Empty remote-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid remote-ip-addr-match [x]</td>
<td>Invalid remote-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] priority [x] is identical to security-policy [id2]</td>
<td>Duplication of the priorities</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has reference to network-interface [xyz] which does not exist</td>
<td>Network-interface was not found in network-interface table</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has reference to network-interface [xyz] which is not valid IPSEC media interface</td>
<td>Network-interface is not valid IPSEC media interface</td>
</tr>
</tbody>
</table>

## Session-Agent

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to egress-realm-id [xyz] which does not exist</td>
<td>Realm was not found in realm table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist</td>
<td>Translation id was not found in translation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist</td>
<td>Translation id was not found in translation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>Translation id was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>Translation id was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement-profile was not found in enforcement-profile table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to code-policy [xyz] which does not exist</td>
<td>Codec-policy was not found in codec-policy table</td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to response-map [xyz] which does not exist</td>
<td>Response-map was not found in response map table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist</td>
<td>Response-map was not found in response map table</td>
</tr>
<tr>
<td>Session-Group</td>
<td></td>
</tr>
<tr>
<td>ERROR: session-group [id] has reference to session-agent [xyz] which does not exist</td>
<td>Session agent was not found in the session agent table</td>
</tr>
<tr>
<td>Session-Translation</td>
<td></td>
</tr>
<tr>
<td>ERROR: session-translation [id] has reference to rules-called [xyz] which does not exist</td>
<td>Translation rule was not found in the translation rule table</td>
</tr>
<tr>
<td>ERROR: session-translations [id] has reference to rules-calling [xyz] which does not exist</td>
<td>Translation rule was not found in the translation rule table</td>
</tr>
<tr>
<td>SIP-Config</td>
<td></td>
</tr>
<tr>
<td>ERROR: sip-config has reference to home-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist</td>
<td>Enforcement profile was not found in enforcement profile table</td>
</tr>
<tr>
<td>WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [sip-internal-realm]</td>
<td>Missing home-realm-id, defaulted to sip-internal-realm</td>
</tr>
<tr>
<td>WARNING: sip-config home-realm-id [xyz] does not have a sip-interface</td>
<td>Sip-interface missing for the home realm</td>
</tr>
<tr>
<td>WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects</td>
<td>Nat-mode needs to be set to either Public or Private if there are sip-nat objects in the configuration</td>
</tr>
<tr>
<td>ERROR: sip-config object is disabled</td>
<td>Sip-config is disabled, but there are configured sip-interface objects</td>
</tr>
</tbody>
</table>
## SIP-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-interface [id] is missing realm-id entry</td>
<td>missing realm</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist</td>
<td>realm was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist</td>
<td>in-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist</td>
<td>out-manipulationid was not found in manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist</td>
<td>enforcement profile was not found in enforcement profile table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist</td>
<td>response-map was not found in response-map table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist</td>
<td>local-response-map was not found in response-map table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist</td>
<td>constraint-name was not found in session constraint table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has no sip-ports</td>
<td>sip-ports are missing</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist</td>
<td>tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist</td>
<td>ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS)</td>
</tr>
<tr>
<td>WARNING: sip-interface [id] has no sip-ports, using SIP-NAT external-address</td>
<td>no sip-ports so SIP-NAT external-address is used</td>
</tr>
<tr>
<td>WARNING: sip-interface [id] has no valid sip-ports, using SIP-NAT external-address</td>
<td>no valid sip-ports so SIP-NAT external-address is used</td>
</tr>
</tbody>
</table>

## SIP-Manipulation

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-manipulation [id] has no header-rules defined</td>
<td>Missing header rules</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] is missing new-value entry</td>
<td>Missing new-value entry (checked only for action type “sip-manip”)</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] has reference to new-value [zxy] which does not exist</td>
<td>New-value entry missing from the sip-manipulation table</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [id] with header-rule [xyz] has new-value that refers to itself from sip-manipulation [di]</td>
<td>Looping reference between two objects</td>
</tr>
</tbody>
</table>
### SIP-NAT

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: sip-nat [id] is missing home-address entry</td>
<td>Missing home-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid home-address [x] entry</td>
<td>Invalid home-address entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing ext-address entry</td>
<td>Missing ext-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid ext-address [x] entry</td>
<td>Invalid ext-address entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing ext-proxy-address entry</td>
<td>Missing ext-proxy-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry</td>
<td>Invalid ext-proxy-address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing user-nat-tag entry</td>
<td>Missing user-nat-tag</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing host-nat-tag entry</td>
<td>Missing host-nat-tag</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing domain-suffix entry</td>
<td>Missing domain-suffix</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] is missing realm-id entry</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] does not match sip-interface realm [xyz]</td>
<td>Sip-interface name was not found in realm table</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] does not have a sip-interface</td>
<td>Sip-interface is missing</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]</td>
<td>Duplicated user-nat-tag</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]</td>
<td>Duplicated host-nat-tag</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y]</td>
<td>Sip-nat ext-address needs to be the same as sip-port address</td>
</tr>
<tr>
<td>ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]</td>
<td>Duplicated home-address</td>
</tr>
</tbody>
</table>

### Static-Flow

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: static-flow [id] is missing in-realm-id entry</td>
<td>Missing in-realm-id</td>
</tr>
<tr>
<td>ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: static-flow [id] is missing out-realm-id entry</td>
<td>Missing out-realm-id</td>
</tr>
<tr>
<td>ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist</td>
<td>Realm was not found in the realm-config table</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has illegal protocol value [xyz]</td>
<td>Invalid protocol entry</td>
</tr>
</tbody>
</table>

### Steering-Pool

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: steering-pool [id] conflict with well-known ports, start-port [x] below 1025</td>
<td>Invalid start-port value (smaller than 1025)</td>
</tr>
<tr>
<td>ERROR: steering-pool [id] has start-port [x] greater than end-port [y]</td>
<td>Start-port value is greater than end-port value</td>
</tr>
</tbody>
</table>
### Surrogate-Agent

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: surrogate-agent [id] is missing realm entry</td>
<td>Missing realm entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist</td>
<td>Realm [xyz] was not found in realm-config table</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing customer-next-hop entry</td>
<td>Missing customer-next-hop entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing register-contact-user entry</td>
<td>Missing register-contact-user entry</td>
</tr>
<tr>
<td>ERROR: surrogate-agent [id] is missing register-contact-host entry</td>
<td>Missing register-contact-host entry</td>
</tr>
</tbody>
</table>

### System-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: system-config has reference to default-gateway [xyz] which does not exist</td>
<td>gateway was not found in the network-interface table or boot parameters</td>
</tr>
<tr>
<td>ERROR: system-config collect has sample-interval [x] greater than push-interval</td>
<td>sample-interval greater than push-interval</td>
</tr>
<tr>
<td>ERROR: system-config collect has start-time [x] greater than end-time [y]</td>
<td>Start-time greater than end-time</td>
</tr>
<tr>
<td>ERROR: system-config collect has group [xyz] with sample-interval [x] greater than collection push-interval [y]</td>
<td>Group [xyz] has incorrect sample interval</td>
</tr>
<tr>
<td>ERROR: system-config collect has group [xyz] with start-time [x] greater than end-time [y]</td>
<td>Group [xyz] has incorrect sample interval</td>
</tr>
<tr>
<td>ERROR: system-config collect has no push-receivers defined</td>
<td>No push-receivers defined</td>
</tr>
<tr>
<td>ERROR: system-config collect has reference to push-receiver [xyz] which does not have user-name set</td>
<td>No user-name set</td>
</tr>
<tr>
<td>ERROR: system-config collect has reference to push-receiver [xyz] which does not have password set</td>
<td>No password set</td>
</tr>
<tr>
<td>ERROR: system-config collect has reference to push-receiver [xyz] which does not have address set</td>
<td>No address set</td>
</tr>
<tr>
<td>ERROR: system-config collect has reference to push-receiver [xyz] which does not have data-store set</td>
<td>No data-store set</td>
</tr>
</tbody>
</table>
## TLS-Profile

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates</td>
<td>End-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.</td>
<td>Bad private key for the cert-record</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist</td>
<td>Certificate record was not found in cert-record table</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has an end-entity-certificate records without any end entity certificate</td>
<td>End certificate missing from all end-entity-certificate records or none of them where imported to the SD</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length</td>
<td>Found an empty trusted-ca-record in the list</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates</td>
<td>Trusted-ca-records entry missing certificate</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] with PKCS7 structure which does not have any certificates</td>
<td>Trusted-ca-records entry with PKCS7 structure missing certificate</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not exist</td>
<td>Certificate record was not found in cert-record table</td>
</tr>
<tr>
<td>ERROR: tls-profile [id] has no trusted-ca-certificates, but mutual-authentication is enabled</td>
<td>No trusted certificates, but enabled mutual-authentication</td>
</tr>
</tbody>
</table>