Contents

About this Guide .......................................................... xxiii

Who is Acme Packet? .................................................... xxiii
Technical Assistance ..................................................... xxiii
Customer Questions, Comments, or Suggestions ......................... xxiii
Contact Us ............................................................. xxiv
Revision History .......................................................... xxiv

1 Log File Management ............................................. 25

Introduction ............................................................. 25
About Log Files ................................................................ 25
Net-Net OS Log Types .................................................... 25
Log File Message Levels .................................................. 25
Task Event Severities ..................................................... 25
Logtype Facilities .......................................................... 26
Acmelog .............................................................. 26
ACLI Configurations and Instructions ................................ 26
File Location ............................................................. 27
Syslog ................................................................. 27
ACLI Configurations and Instructions ................................ 27
Adding a Syslog Server .................................................. 27
Removing a Syslog Server .............................................. 28
Process Log Files ......................................................... 28
Task Log Output ........................................................... 28
Process Log Server ........................................................ 29
Log File Output Locations ............................................... 29
Configuring Global Task Logging Level and Process Log Server .... 29
Task Logging ............................................................. 30
Facility Logging ........................................................... 30
Real-time Logging Configuration ....................................... 32
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>set log level</td>
<td>32</td>
</tr>
<tr>
<td>set log mode</td>
<td>32</td>
</tr>
<tr>
<td>set log server</td>
<td>32</td>
</tr>
<tr>
<td>Displaying Current Logging Configuration</td>
<td>32</td>
</tr>
<tr>
<td>show log level</td>
<td>32</td>
</tr>
<tr>
<td>show log mode</td>
<td>32</td>
</tr>
<tr>
<td>show log server</td>
<td>32</td>
</tr>
<tr>
<td>Log File Maintenance</td>
<td>33</td>
</tr>
<tr>
<td>Log File Compression</td>
<td>33</td>
</tr>
<tr>
<td>set log compression</td>
<td>33</td>
</tr>
<tr>
<td>show log compression</td>
<td>33</td>
</tr>
<tr>
<td>Rotating Log Files</td>
<td>33</td>
</tr>
<tr>
<td>Manually Rotating Log Files</td>
<td>34</td>
</tr>
<tr>
<td>Manually Deleting Log Files</td>
<td>34</td>
</tr>
<tr>
<td>Inserting Text into a Log File</td>
<td>34</td>
</tr>
<tr>
<td>Trace Log</td>
<td>34</td>
</tr>
<tr>
<td>Trace Log Configuration</td>
<td>34</td>
</tr>
<tr>
<td>Trace Log Output</td>
<td>35</td>
</tr>
<tr>
<td>Task and Trace log Filenames</td>
<td>35</td>
</tr>
<tr>
<td>Debug Logging Timeout</td>
<td>36</td>
</tr>
<tr>
<td>ACLI Instructions and Examples</td>
<td>36</td>
</tr>
<tr>
<td>Panic Log Dump</td>
<td>36</td>
</tr>
<tr>
<td>Panic Log Dump Configuration</td>
<td>37</td>
</tr>
<tr>
<td>Managing Panic Log Dumps</td>
<td>37</td>
</tr>
<tr>
<td>show dumps</td>
<td>37</td>
</tr>
<tr>
<td>delete dumps</td>
<td>38</td>
</tr>
<tr>
<td>Viewing Logs</td>
<td>39</td>
</tr>
<tr>
<td>FTP</td>
<td>39</td>
</tr>
<tr>
<td>Acmealog</td>
<td>40</td>
</tr>
<tr>
<td>Facility Type List</td>
<td>41</td>
</tr>
<tr>
<td>2 Fault Management</td>
<td>43</td>
</tr>
<tr>
<td>Introduction</td>
<td>43</td>
</tr>
<tr>
<td>Alarms</td>
<td>43</td>
</tr>
<tr>
<td>Overview</td>
<td>43</td>
</tr>
<tr>
<td>Alarming Process</td>
<td>43</td>
</tr>
<tr>
<td>Alarm Categories and Responses</td>
<td>44</td>
</tr>
<tr>
<td>Alarm Severity Levels</td>
<td>44</td>
</tr>
<tr>
<td>Alarm Severity Health Deductions</td>
<td>45</td>
</tr>
</tbody>
</table>
Response to Alarms .............................................................. 45
Alarm Table ........................................................................... 46
Syslog / AcmeLog ................................................................. 46
SNMP Traps ........................................................................ 46
Dry Contacts ......................................................................... 46
Graphic Display .................................................................... 46
Card Reset ............................................................................ 47

Operating Status Alarms ......................................................... 47
Task Status ........................................................................... 47
CPU Core Usage ................................................................... 47
CPU Core Memory Usage ...................................................... 47
SPU Status ........................................................................... 47
NPU Status ........................................................................... 47
User Configured Alarms ......................................................... 48
CPU alarms .......................................................................... 48
Memory alarms ..................................................................... 48
License threshold ................................................................. 48
ACLI Instructions ................................................................. 48

Displaying and Clearing Alarms .............................................. 49
Displaying Alarms ................................................................ 49
show alarm current ............................................................. 49
Filtering Alarms .................................................................. 49
Clearing Alarms .................................................................. 50
Automatic Alarm Clearing .................................................... 50
ACLI Instructions ................................................................. 50
Via the front-panel navigation buttons .................................... 51

Configurable Alarm Thresholds ............................................. 51
User-configured Alarms ......................................................... 51
CPU alarms .......................................................................... 51
Memory alarms ..................................................................... 51
License threshold ................................................................. 51
ACLI Instructions ................................................................. 51

SNMP Traps .......................................................................... 52
Supported Standard Traps ...................................................... 52

Alarm Descriptions ............................................................. 54
Hardware Alarms ................................................................. 54
I2C Hardware Alarms ........................................................... 54
Card Presence Alarms .......................................................... 55
I2C Alarm Types ................................................................. 55
I2C Link and Temperature Alarms ........................................ 56
Voltage Alarms ................................................................. 57
3 System Management .............................................. 69

Global System Parameters ................................... 69
  System State .................................................. 69
    show uptime ................................................. 69
    show system ................................................ 69
    show version ................................................. 69
    show clock .................................................. 70
    show bootparams ........................................... 70

Installed Features ............................................. 71

Task Overview .................................................. 72
  show cpu ...................................................... 72
  show manifest ................................................. 73

User Sessions ................................................... 74
  show users ..................................................... 74
  Identifying Config Sessions ................................ 74
  Terminating Sessions ........................................ 74
Management Applications .............................................74
  show telnet ..........................................................75
  show ftp ............................................................75
  show ssh ............................................................75
Statistic Counts Explained .............................................75
Task Statistics ...........................................................76
  Task Statistic Overviews ..........................................76
    show task active ................................................76
    show task standby ..............................................77
Individual Task Statistics .............................................77
  show task acl ........................................................78
  show task arpm ....................................................79
  show task auth .....................................................79
  show task broker ..................................................79
  show task cm .......................................................80
  show task collect ................................................80
  show task dnsres ..................................................81
  show task ftpalg ..................................................81
  show task h323GkGw ..............................................82
  show task h323RasGk ..............................................82
  show task lcm .....................................................83
  show task lem .....................................................83
  show task logman ..................................................84
  show task mbcd ....................................................84
  show task msfe ....................................................85
  show task natm ....................................................85
  show task npm .....................................................86
  show task ntpd .....................................................86
  show task rasm ....................................................87
  show task secured ................................................87
  show task sem .....................................................88
  show task sfe .....................................................88
  show task sipc .....................................................89
  show task sipl .....................................................89
  show task sipt .....................................................90
  show task sm ......................................................90
  show task snmpd ...................................................91
  show task soapd ...................................................91
  show task sshd ....................................................92
  show task xserv ...................................................92
Chassis Management Application Statistics .......................93
  Socket Front End (SFE) .............................................93
show sfe summary ................................................................. 93
show sfe pending ............................................................... 94
show sfe clients ................................................................. 94
show sfe load ................................................................. 94
show sfe sockets ............................................................. 94
Management Socket Front End (MSFE) ...................................... 95
  show msfe summary .......................................................... 95
  show msfe pending .......................................................... 95
  show msfe clients .......................................................... 95
  show msfe load ............................................................. 96
  show msfe sockets ........................................................ 96
Acme Messaging Protocol (AMP) ............................................. 96
  show amp aclii .............................................................. 97
  show amp arpm ............................................................. 97
  show amp auth ............................................................. 97
  show amp broker ........................................................... 98
  show amp cm ............................................................... 98
  show amp collect .......................................................... 99
  show amp dnsres .......................................................... 99
  show amp ftpdalg .......................................................... 99
  show amp h323GkGw ...................................................... 100
  show amp h323RasGk ...................................................... 100
  show amp ipci .............................................................. 100
  show amp lcm ............................................................. 101
  show amp lems ............................................................ 101
  show amp logman .......................................................... 102
  show amp mbcd ............................................................. 102
  show amp msfe ........................................................... 102
  show amp natm ............................................................. 103
  show amp npm ............................................................. 103
  show amp ntpd ............................................................. 104
  show amp rasm ............................................................ 104
  show amp secured ........................................................ 104
  show amp sem ............................................................. 105
  show amp sfe ............................................................... 105
  show amp sipc ............................................................ 106
  show amp sipls ............................................................ 106
  show amp sipt ............................................................. 106
  show amp sm ............................................................... 107
  show amp snmpd .......................................................... 107
  show amp soapd .......................................................... 108
  show amp sshd ............................................................. 108
  show amp xserv ........................................................... 108
Reliable Datagram Protocol (RDP) .......................................................... 109
  show rdp ................................................................. 109
  show rdp all ....................................................... 109
  show rdp links .................................................... 110
  show rdp linkstats ................................................ 110
  show rdp serv .................................................... 111
  show rdp servstats ............................................. 111
  show rdp conn ................................................... 112
  show rdp connstats ............................................. 113
System Name Registry (SNR) ......................................................... 113
  show snr core ................................................... 113
  show snr relay .................................................. 114
Redundancy Statistics ............................................................... 114
  show redundancy standby ...................................... 115
Chassis Hardware Statistics ......................................................... 115
  Card and Hardware Status ...................................... 115
    show status ..................................................... 116
    show health ..................................................... 116
  Temperature and I2C Status and Alarms ....................... 117
    SPU Sensors .................................................... 118
    NPU Sensors .................................................... 118
    TCU Sensors .................................................... 119
  Interface Card and Fan Sensors ................................ 119
  MIB Information .................................................. 120
    show i2c .......................................................... 120
Network Processor Card Statistics ............................................. 123
  show npu phy-port ............................................. 124
  show npu phy-stats ............................................. 124
  show npu phy-registers ....................................... 124
  show npu gmac-port ........................................... 125
  show npu gmac-stats ......................................... 125
  show npu cpu-stats ........................................... 125
  show npu registers ............................................ 126
  dump npu-stats ................................................ 127
Internal Switch Statistics ....................................................... 127
  show switch portstate ....................................... 127
  show switch linkstate ....................................... 127
  show switch portstats ....................................... 128
  show switch l2table ......................................... 129
TCU Statistics ............................................................ 129
  show tcu flair .................................................. 129
  show tcu gbe ................................................... 130
show tcu hm ....................................................... 131
show tcu ibx .................................................... 131
show tcu tcm .................................................... 131

Internal Switch Port Mirroring ........................................ 132
BCM 56000 Ports .................................................. 132

Switching Cores from the ACLI ......................................... 132

System Card Communication Integrity .................................... 133
SPU to MIU Communication ........................................... 133
NPU to TCU Communication ........................................... 133

Password Strength ..................................................... 133
Password Policy ....................................................... 133
Setting the Password Policy ........................................... 134
Setting a New Password ............................................... 134
Resetting Passwords ................................................... 135

Tech Support Show Command ........................................... 135
General System Commands ............................................. 136
Physical Interface Commands ........................................... 136
SIP Commands ......................................................... 136
Call Media Commands .................................................. 136
xserver Commands .................................................... 137
Security Commands ..................................................... 137
Display Information to the Screen ....................................... 137
System Configuration Listing ........................................... 137

ACLI Management ....................................................... 137
ACLI Terminal Settings .................................................. 137
show terminal .......................................................... 137
Setting the Terminal Height ............................................. 138
Setting the Terminal Width ............................................ 138
Controlling the “more” Prompt ........................................ 138
Configuration Mismatch Warning ...................................... 138
Setting the Configuration Mismatch Warning ....................... 139
Save Configuration Warning ........................................... 139

CLI Audit Trail .......................................................... 139
Viewing the CLI Audit Trail ............................................. 140
ACLI Instructions and Examples ....................................... 140

Support for Last Modified By ........................................... 140
EMS derived modification ............................................... 141
ACLI Derived Modification ............................................. 141
Console Access .......................................................... 141
Telnet/SSH Access ..................................................... 141
RADIUS Authentication .................................................. 141
Console Access .......................................................... 141
Telnet/SSH Access ....................................................... 141

FTP/SFTP Session Management ........................................ 141
Viewing Sessions .......................................................... 142
Terminating Sessions ...................................................... 142

Historical Data Recording ................................................... 142
How It Works .............................................................. 142
About the CSV File ....................................................... 143
Collection Interval and Push ............................................. 143
Group Record Types ...................................................... 143
ACLI Instructions and Examples ....................................... 151
Accessing the HDR Configuration Parameters ...................... 151
Global Collection Settings: Boot State, Collection Start and Stop, Sample and Push Intervals 152
Collection Group Settings ............................................... 152
Push Receiver Settings ................................................... 153
Controlling HDR from the Command Line ............................ 154
CPU Core Index Mapping ................................................ 155

NTP Features ................................................................. 155
NTP Application Debugging ............................................. 155
show ntp status .......................................................... 155
show ntp server .......................................................... 156
NTP System Level Debugging .......................................... 157
show task ntp ............................................................. 157
show amp ntpd ............................................................ 157

4 Network Management ...................................................... 159
Network Connections ...................................................... 159
show interfaces .......................................................... 159
show ip connections ...................................................... 160
show ip statistics ........................................................ 161
ARP Statistics ............................................................. 161
show arp commands ..................................................... 161
show arp statistics-by-interface ..................................... 161
show arp statistics-all .................................................. 162
show arp table-all ....................................................... 163
show arp table-by-interface ......................................... 164
show arp info ............................................................. 164
show arp standby ........................................................ 164
Manual ARP Table Changes .......................................... 165
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>check arp</td>
<td>165</td>
</tr>
<tr>
<td>add arp</td>
<td>165</td>
</tr>
<tr>
<td>delete arp</td>
<td>165</td>
</tr>
<tr>
<td>Other ARP Commands</td>
<td>166</td>
</tr>
<tr>
<td><strong>ACL Statistics</strong></td>
<td>166</td>
</tr>
<tr>
<td>Show ACL commands</td>
<td>166</td>
</tr>
<tr>
<td>show acl denied</td>
<td>166</td>
</tr>
<tr>
<td>show acl info</td>
<td>166</td>
</tr>
<tr>
<td>show acl ip</td>
<td>167</td>
</tr>
<tr>
<td>show acl trusted</td>
<td>168</td>
</tr>
<tr>
<td>show acl untrusted</td>
<td>168</td>
</tr>
<tr>
<td>show acl all</td>
<td>168</td>
</tr>
<tr>
<td><strong>NAT Statistics</strong></td>
<td>169</td>
</tr>
<tr>
<td>Show NAT commands</td>
<td>169</td>
</tr>
<tr>
<td>show nat by-addr</td>
<td>169</td>
</tr>
<tr>
<td>show nat by-index</td>
<td>169</td>
</tr>
<tr>
<td>show nat in-tabular</td>
<td>171</td>
</tr>
<tr>
<td>show nat info</td>
<td>172</td>
</tr>
<tr>
<td>show nat standby</td>
<td>172</td>
</tr>
<tr>
<td>show nat statistics</td>
<td>173</td>
</tr>
<tr>
<td>show nat table</td>
<td>173</td>
</tr>
<tr>
<td>Other NAT Commands</td>
<td>174</td>
</tr>
<tr>
<td><strong>Media Interface Statistics</strong></td>
<td>174</td>
</tr>
<tr>
<td>Show media commands</td>
<td>174</td>
</tr>
<tr>
<td>show media classify</td>
<td>174</td>
</tr>
<tr>
<td>show media frame-statistics</td>
<td>175</td>
</tr>
<tr>
<td>show media gmac-statistics</td>
<td>176</td>
</tr>
<tr>
<td>show media host-statistics</td>
<td>177</td>
</tr>
<tr>
<td>show media network</td>
<td>177</td>
</tr>
<tr>
<td>show media phy-statistics</td>
<td>178</td>
</tr>
<tr>
<td>Other Media Commands</td>
<td>178</td>
</tr>
<tr>
<td><strong>HIP Statistics</strong></td>
<td>179</td>
</tr>
<tr>
<td>show hip commands</td>
<td>179</td>
</tr>
<tr>
<td>show hip interfaces</td>
<td>179</td>
</tr>
<tr>
<td>show hip statistics-all</td>
<td>179</td>
</tr>
<tr>
<td>show hip statistics-by-interface</td>
<td>180</td>
</tr>
<tr>
<td>Other HIP Commands</td>
<td>180</td>
</tr>
<tr>
<td><strong>Route Statistics</strong></td>
<td>180</td>
</tr>
<tr>
<td>show routes</td>
<td>180</td>
</tr>
<tr>
<td>show route-stats</td>
<td>181</td>
</tr>
<tr>
<td><strong>Pinging an IP Address</strong></td>
<td>181</td>
</tr>
</tbody>
</table>
Specifying a Source Address for ICMP Pings .......................................................... 181
Configuring a Network Interface for pinging ......................................................... 181

DNS and ENUM Management ................................................................................. 182
DNS Statistics ........................................................................................................... 182
  show dns cache ...................................................................................................... 182
  show dns lookup ................................................................................................... 182
  show dns query ..................................................................................................... 182
  show dns realm ..................................................................................................... 182
  show dns server .................................................................................................... 183
  show dns sip ......................................................................................................... 183
  show dns sockets ................................................................................................. 183
  clear dns .............................................................................................................. 183
ENUM Statistics ....................................................................................................... 183
  show enum cache .................................................................................................. 183
  show enum lookup ............................................................................................... 183
  show enum query .................................................................................................. 183
  show enum server ............................................................................................... 184
  clear enum ........................................................................................................... 184
Clearing ENUM and DNS Statistics ................................................................. 184
ACLI Instructions and Examples ............................................................................. 184
Packet Trace ............................................................................................................ 184
  How It Works ......................................................................................................... 185
  Packet Trace Scenarios ....................................................................................... 186
    Packet Trace for One Endpoint ......................................................................... 186
    Packet Trace for Both Call Legs ....................................................................... 187
    Packet Trace for a Net-Net SBC Signaling Address ............................................ 188
  ACLI Instructions and Examples ........................................................................ 188
    Configuring a Trace Server ................................................................................ 188
    Starting a Packet Trace ...................................................................................... 189
    Stopping a Packet Trace .................................................................................... 189
    Viewing Active Packet Traces ............................................................................ 190

5 Application Management ....................................................................................... 191
SIP Management ...................................................................................................... 191
  SIP Tasks Show Commands .................................................................................. 191
    show sip transport .............................................................................................. 191
    show sip server .................................................................................................. 191
    show sip client ................................................................................................. 192
    show sip codecs ............................................................................................... 192
    show sip core .................................................................................................... 193
    show sip b2bua ............................................................................................... 193
- show sip sessions .......................................................... 193
- show sip cache .............................................................. 194
- show sip policy ............................................................. 194
- show sip media ............................................................. 194
- show sip load ............................................................... 195

**SIP Messages Show Commands** ........................................ 195
- show sip invite ............................................................. 195
- show sip ack ............................................................... 195
- show sip bye ............................................................... 196
- show sip register .......................................................... 196
- show sip cancel ............................................................ 196
- show sip prack ............................................................. 196
- show sip options ........................................................... 196
- show sip info .............................................................. 196
- show sip sub .............................................................. 197
- show sip subscribe ........................................................ 197
- show sip notify ............................................................ 197
- show sip refer ............................................................. 197
- show sip update ............................................................ 197
- show sip message ......................................................... 197
- show sip publish .......................................................... 197
- show sip other .............................................................. 197
- show sip forked ............................................................. 197

**SIP Networking Show Commands** ..................................... 197
- show sip agents ............................................................ 197
- show sip sockets .......................................................... 198
- show sip endpoint ........................................................ 198
- show sip realm ............................................................. 198

**SIP CPU Load Limiting** .................................................. 199

**Call Protocol (SIP) Tracing** .......................................... 199
- SIP Protocol Trace Output ............................................... 199
- Configuration ............................................................. 199

**Displaying and Clearing Registration Cache Entries** .......... 200
- Querying the SIP Registration Cache ................................ 200
  - by-user ................................................................. 201
  - by-realm ............................................................... 202
  - by-route ............................................................... 202
  - by-registrar .......................................................... 203
- Extended Registration Cache Output .................................. 203
- Writing Registration Queries to a File .............................. 204
- Displaying H.323 Registration Cache Entries ...................... 204
  - by-alias ............................................................... 204
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear SIP and H.323 Sessions</td>
<td>219</td>
</tr>
<tr>
<td>Clearing SIP Sessions</td>
<td>219</td>
</tr>
<tr>
<td>Clearing H.323 Sessions</td>
<td>219</td>
</tr>
<tr>
<td>Rate Limiting</td>
<td>219</td>
</tr>
<tr>
<td>System State</td>
<td>219</td>
</tr>
<tr>
<td>ACLI Instructions and Examples</td>
<td>219</td>
</tr>
<tr>
<td>Show sessions and show virtual-interfaces</td>
<td>220</td>
</tr>
<tr>
<td>ACLI Instructions and Examples</td>
<td>220</td>
</tr>
<tr>
<td>Show sessions</td>
<td>220</td>
</tr>
<tr>
<td>Show virtual-interfaces</td>
<td>221</td>
</tr>
<tr>
<td>SIP Media and Transcoding Statistics</td>
<td>221</td>
</tr>
<tr>
<td>Session Based Statistics</td>
<td>221</td>
</tr>
<tr>
<td>Flow Based Statistics</td>
<td>221</td>
</tr>
<tr>
<td>Example 1</td>
<td>222</td>
</tr>
<tr>
<td>Example 2</td>
<td>222</td>
</tr>
<tr>
<td>Example 3</td>
<td>222</td>
</tr>
<tr>
<td>QoS Management</td>
<td>223</td>
</tr>
<tr>
<td>QoS Commands</td>
<td>223</td>
</tr>
<tr>
<td>show qos errors</td>
<td>223</td>
</tr>
<tr>
<td>show qos statistics</td>
<td>224</td>
</tr>
<tr>
<td>show qos flow</td>
<td>224</td>
</tr>
<tr>
<td>Reset QoS Statistics</td>
<td>224</td>
</tr>
<tr>
<td>Application Load Limiting</td>
<td>224</td>
</tr>
<tr>
<td>SIP Load Limiting</td>
<td>224</td>
</tr>
<tr>
<td>MBCD Load Limiting</td>
<td>224</td>
</tr>
<tr>
<td>NATM Load Limiting</td>
<td>225</td>
</tr>
<tr>
<td>SFE Load Limiting</td>
<td>225</td>
</tr>
<tr>
<td>H.323 Load Limiting</td>
<td>225</td>
</tr>
<tr>
<td>Transcoding Management</td>
<td>225</td>
</tr>
<tr>
<td>Xcode Server Commands</td>
<td>225</td>
</tr>
<tr>
<td>show xserv stats</td>
<td>226</td>
</tr>
<tr>
<td>show xserv api_stats</td>
<td>226</td>
</tr>
<tr>
<td>show xserv audit-aloc</td>
<td>227</td>
</tr>
<tr>
<td>show xserv audit-free</td>
<td>227</td>
</tr>
<tr>
<td>show xserv audit-lost</td>
<td>227</td>
</tr>
<tr>
<td>show xserv audit-full</td>
<td>227</td>
</tr>
<tr>
<td>show xserv api-stats</td>
<td>228</td>
</tr>
<tr>
<td>show xserv dbginfo</td>
<td>228</td>
</tr>
<tr>
<td>show xserv session</td>
<td>229</td>
</tr>
<tr>
<td>show xserv sessstats</td>
<td>229</td>
</tr>
<tr>
<td>show xserv sysinfo</td>
<td>230</td>
</tr>
</tbody>
</table>
show xserv red-peers ........................................ 230
show xserv devinfo ........................................ 231
show xserv dsp-events ..................................... 231
show xserv dsp-channel .................................. 231
show xserv dsp-device .................................. 232
show xserv dsp-status ................................ 232

Xcode Client Commands .................................. 233
show xclient status ....................................... 233
show xclient sessions .................................... 233
show xclient xlist ....................................... 233
show xclient session-bitinfo ............................. 234
show xclient session-byid ............................... 234
show xclient session-byipp .............................. 234
show xclient session-cache .............................. 234
show xclient xserv-lock ................................ 234

Realm Management ...................................... 234

Monthly Minutes-Based CAC Data ...................... 234
Realm Specifics ........................................ 235

H.323 Management ....................................... 236

H.323 Show Commands .................................. 236
show h323 agentstats ..................................... 236
show h323 all ........................................ 236
show h323 groupstats .................................. 237
show h323 h323stats .................................... 237
show h323 load .......................................... 237
show h323 registrations ................................ 237
show h323 stackCallstats ............................... 238
show h323 stackDisconnectInstats ...................... 238
show h323 stackDisconnectOutstats ...................... 238
show h323 stackPvtstats ................................ 238
show h323 status ....................................... 238
Resetting H.323 Statistics .............................. 239

H.323 CPU Load Limiting ................................. 239

H.323 Stack Monitoring .................................. 239

ACLI Instructions and Examples ....................... 239
Management: ACLI ..................................... 240
Viewing the Number of Active Calls ................. 240
Viewing Alarm Information .............................. 240
Management: SNMP .................................... 241

External Policy Servers Management .................. 241

Policy Server Show Commands ......................... 241
show policy-server bandwidth ................................................. 241

6 Security Management ....................................................... 243

TLS Maintenance ............................................................... 243
  Viewing Certificates ....................................................... 243
    show security certificate brief .................................... 243
    show security certificate details .................................. 243
    show security certificate list ...................................... 244
  TLS Cache Statistics ..................................................... 244

IPsec Maintenance ............................................................. 244
  show security ipsec sad ............................................... 244
  show security ipsec statistics sad ................................... 246
  Key Generation ............................................................ 247
  IPsec Hardware Statistics ................................................ 247
  show security ipsec statistics gmac .................................. 247
    show security status .................................................. 248

Protected Password Configuration ........................................ 249
  Protected Data ............................................................. 249
  Configuring the PCP ..................................................... 249
  Verifying the PCP ........................................................ 250
  Migrating a PCP-Protected Configuration ............................. 250

SSH Public Key Support ...................................................... 251
  SSHv2 Public Key Authentication ...................................... 251
  Importing an SSH Host Key ............................................. 251
  Importing an SSH Public Key .......................................... 252
  Generating an SSH Key Pair ............................................. 253
  Copying a Client Key or an SSH or SFTP Server ....................... 254
  Viewing SSH Imported Keys ............................................. 255
    Viewing a Brief SSH Imported Key Version .......................... 255
    Viewing a Detailed SSH Imported Key Version ...................... 256
  Deleting a Public Key Record ......................................... 258

7 Configuration Management ................................................ 259

System Configuration Process ............................................ 259
  Net-Net 9200 Configuration ........................................... 259
  Configuration Process .................................................. 259
  Configuration Versions .................................................. 260
  Deleting Configurations ............................................... 260

Displaying Configurations ................................................. 260
  Configuration Show Commands .......................................... 260
8 Upgrade Management ............................................. 285

Overview .......................................................... 285

Net-Net OS S-D7.1.0 Upgrade Prerequisites .................. 285

Automatic Online Upgrade .................................... 285
  Upgrade Overview ............................................ 286
  Upgrade Path ............................................... 286
  Online vs. Offline ......................................... 286
  Duration .................................................... 287

Net-Net 9200 Software Upgrade .............................. 287
  Virtual Management Interface ............................. 287
  Netmask Requirement ...................................... 288
  File Location Prerequisites ............................... 290
  Upgrade from Flash ....................................... 290
  Upgrade from Network .................................... 290
  Process Overview ......................................... 290

Upgrade Procedure Command Syntax ....................... 291
  Boot From Local Image File ............................... 291
  Boot From FTP Server .................................... 291
  Download and Boot From Remote Image File ............... 291
  Redundancy Check ......................................... 292
The *Net-Net Maintenance and Troubleshooting Guide* provides information extending from hardware level functionality through system level tasks to real-time application statistics. This information is applicable for Acme Packet’s Net-Net 9000 session border controllers.

**Who is Acme Packet?**

Acme Packet enables network service providers to deliver premium, interactive communications—voice, video, and multimedia sessions—across IP network borders. Our award-winning Net-Net family of session border controllers satisfies critical security, SLA assurance, and law enforcement requirements in wireline, wireless, and cable networks.

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

**Technical Assistance**

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

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

- From the United States, Canada, and Mexico call: +1 866 226 3758
- From all other locations, call: +1 781 756 6920

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

**Customer Questions, Comments, or Suggestions**

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

Contact Us
Acme Packet, Inc.
100 Crosby Drive
Bedford, MA 01730 USA
t 781-328-4400
f 781-275-8800
http://www.acmepacket.com

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>October 25, 2009</td>
<td>Revision 1.00</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
| December 23, 2011 | Revision 1.05  | Corrects and updates Alarm Table
|                |                 | Corrects and rearranges TCU/TCM Upgrade section       |
| May 01, 2012   | Revision 1.10   | Adds CPU Core Index Mapping table                      |
1 Log File Management

Introduction

This chapter describes the logging system implemented in Net-Net OS D6.0 and higher.

About Log Files

Log files are a critical component of system management. Log files are used to assist with debugging, system management and optimization, and identifying potential security breaches or other nonstandard activities on the system.

Each task that runs on the Net-Net 9200 is capable of outputting log file messages. Because tasks are distributed throughout the Net-Net 9200, across feature cards, CPUs, and cores, the logging system is designed to conveniently centralize the output of all logs.

Net-Net OS Log Types

The Net-Net OS creates and maintains two types of log files:

- The Acmelog—This file is used to aggregate general system events that give an overview of the health and overall operating conditions of the Net-Net 9200.
- The Process Log—The process log is a file stored on a remote Acme Process Log server, on a local (to the task) core, or both. Process logs are a compendium of task log files, which are created by every discrete task that runs on the Net-Net 9200. The process log records as much or as little information as you require based on configuration parameters. The process log, located on a local core, is also available on the Net-Net 9200, accessible via FTP.

Log File Message Levels

Log files capture messages that describe task events. A system of 10 severity codes, the Acme Packet Log Level Enumeration, is used to label events from high to low significance. Emergency represents the most critical system affecting event, while Info represents the least critical system event. In addition, three additional Acme Packet log levels are used for debugging purposes.

Task Event Severities

For a given task, different events quality for different severity levels. The Acme Packet Log Enumeration levels (event severities) are listed in the following table. Emergency is the highest level while Info is the lowest event severity level. The remaining three levels, trace and debug detail are used for highly granular trace logging.

<table>
<thead>
<tr>
<th>Acme Packet Log Enumeration</th>
<th>syslog Severity</th>
<th>syslog Numerical Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMERGENCY</td>
<td>Emergency (system is unusable)</td>
<td>0</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Alert (action must be taken immediately)</td>
<td>1</td>
</tr>
<tr>
<td>MAJOR</td>
<td>Critical (critical conditions)</td>
<td>2</td>
</tr>
</tbody>
</table>
The table above also includes the syslog severity codes and their corresponding numerical codes. When the Net-Net 9200 sends messages to an externally configured Syslog server, the event severity closely matches with the Acme Packet Log Enumeration levels, as shown above.

### Logtype Facilities

A logtype facility is a second filtering criteria used when writing to log files. The facility is a tag that describes the context of the event. Facility messages are filtered by the task and then by the mechanism that writes data to task log files to limit the amount of information that gets written into a task’s log file.

For example, one logtype facility is `DNS`. By configuring a task to deliver `DNS` logtypes, for a given severity level and higher, the resultant log file would only contain messages dealing with DNS activities for the specified log level range.

See the “Facility Type List” section at the end of this chapter for a complete list of logtype facilities.

### Acmelog

The Acmelog is a log file located on CPU0, core 0’s local file system on the active SPU. This file aggregates general system events that give an overview of the health and overall operating conditions of the Net-Net 9200.

The contents of the Acmelog are determined by the `system-log-level` parameter. This configuration dictates which event messages are written to the Acmelog. For example, if you set the `system-log-level` to `Minor`, all events Minor through Emergency are written to the Acmelog.

### ACLI Configurations and Instructions

To set the Acmelog’s system log level:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   
   `ACMEPACKET# configure terminal`

2. Type `system` and press <Enter> to access the system path.

   `ACMEPACKET{configure}# system`

   `ACMEPACKET{system}#`

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   `ACMEPACKET{system}# system-config`

   `ACMEPACKET{system-config}#`
4. Type `select` and press <Enter> to configure the existing system-config.
   ```
   ACMEPACKET(system-config)# select
   ACMEPACKET(system-config)#
   ```

5. `system-log-level`—Set this parameter to the minimum Acme Packet Log Message level you want the Acmelog to record.
   ```
   ACMEPACKET(system-config)# system-log-level info
   ACMEPACKET(system-config)#
   ```

6. Save your work using the ACLI `save` or `done` command.

**File Location**

The Acmelog is created by the logman process that runs on the active SPU’s master core. This is Slot 0, CPU 0, Core 0, in a non-faulted state. Like all other tasks that run in this location, the Acmelog is written to the `/ramdrv/logs/` directory on Slot 0, CPU 0, Core 0’s local file system.

**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. The syslog protocol provides a standardized means to remotely access log files. Net-Net OS’s Syslog implementation conforms to the standard used for logging servers and processes as defined in RFC 3164.

The Net-Net OS’s syslog message functionality lets you configure multiple syslog servers, and set the facility marker value used in the messages sent to that syslog server. The Net-Net SD can send logs to multiple syslog servers on the same host, provided they are running on unique ports.

The contents of the syslog output is identical to the Acmelog’s contents.

**ACLI Configurations and Instructions**

This section describes how to add and remove syslog servers. You can add multiple syslog servers to your configuration.

**Adding a Syslog Servers**

**To add a syslog server:**

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type `system` and press <Enter> to access the system path.
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type `syslog-servers` and a <Space>, then `add` and a <Space>. Then enter the parameters that identify where you want to send logs: IP address, port number, and facility number.
The facility part of your entry is an integer that identifies a user-defined facility value sent in every syslog message from the Net-Net 9200 to the syslog server. This parameter is used only for identifying the source of this syslog message as coming from the Net-Net 9200. It is not identifying an OS daemon or process. The default value for this parameter is 17. RFC 3164 specifies valid facility values.

Make your entry in one command-line using the syntax in the following example:

```
ACMEPACKET(system-config)# syslog-servers add 10.168.192.5:514:17
```

Note: You MUST enter a port number and facility number for this configuration parameter. 514 is the default syslog port number.

5. Save your work using the ACLI done command.

### Removing a Syslog Server

To remove a syslog server:

1. In Superuser mode, type `configure terminal` and press <Enter>.

```
ACMEPACKET# configure terminal
ACMEPACKET#
```

2. Type `system` and press <Enter> to access the system path.

```
ACMEPACKET(configure)# system
ACMEPACKET(system)#
```

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)#
```

4. Type `select` and press <Enter> to configure the existing system-config.

```
ACMEPACKET(system-config)# select
ACMEPACKET(system-config)#
```

5. Type `syslog-server` and a <Space>, then `delete` and a <Space>. Then enter the IP address, port number, and facility number that identify the syslog server you want to remove. Make your entry in one command-line using the syntax in the following example:

```
system-config# syslog-servers delete 10.168.192.5:514:17
```

The syslog server is removed from your list of syslog servers.

6. Save your work using the ACLI done command.

### Process Log Files

Each task may generate task logs to maintain a record of events for data collection and debugging purposes. Because task logs are more data-inclusive than the AcmeLog, their contents usually encompass the AcmeLog contents. All tasks write their log files initially to their local file system, associated with the slot, CPU, and core where they reside.

### Task Log Output

Tasks write their log file to the file system local to the CPU/core where they run. The local destination of a task’s log file is `/ramdrv/logs/` local to that CPU/core.
Process Log Server

The process log server application resides on a remote server. It lets you store task logs remotely. This application is available from your Acme Packet customer support representative in either a binary program or as a perl-script.

Log File Output Locations

A task’s log file output locations are determined by user configuration. The Net-Net OS uses a system of four modes to set the output of a task’s log file.

- local—Writes the log file to the specified task’s local file system. (default)
- remote—Writes the specified task’s log file to the configured Acme Process Log Server.
- both—Writes the specified task’s log file to both the configured Acme Process Log Server and the task’s local file system.
- none—Task does not write to local or remote location. Logging is only sent to Acmealog and potentially syslog, depending on system-log-level setting and syslog-server setting.

Configuring Global Task Logging Level and Process Log Server

Set the following parameters to configure the process log server:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type `system` and press <Enter> to access the system path.
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. `process-log-level`—Set the starting log level for all tasks/process. Each process running on the system has its own process log.
   
   The default value for this parameter is `NOTICE`. Valid values for this parameter are `EMERGENCY`, `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, `NOTICE`, `INFO`, `TRACE`, `DEBUG`.

5. `process-log-mode`—Set the process log mode that you want to use from these available choices:
   
   - remote—Send task logs to the Process log server only
   - local—Send task logs to the local file system only (default)
   - both—Send task logs to the Process log server and to the local file system
   - none—No task logging

6. `process-log-address`—Set the IP address of the process log server.

7. `process-log-port`—Set the port number to use for the process log server.
   Default: 2500.

8. Save your work using the ACLI `done` command.
Task Logging

Apart from the global task logging level, you can configure logging level and log file destination for each unique task. This is accomplished by using the task-loggin sub element.

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type `system` and press <Enter> to access the system path.
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>.
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type `task-logging` and press <Enter>.
   ```
   ACMEPACKET(system-config)# task-logging
   ACMEPACKET(task-logging)#
   ```

5. `task-name`—Set the task name and location of the task you are configuring in the form: `<task>@<slot>.<CPU>.<core>`

6. `level`—Set the log level at which the task will write event messages. If configured, this value supersedes the global RTP startup logging level, defined by the process log-level-parameter.
   Valid values for this parameter are `EMERGENCY`, `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, `NOTICE`, `INFO`, `TRACE`, `DEBUG`.

7. `mode`—Set the mode of outputting the task’s log file that determines the file’s destination. Set the process log mode for the named task from these available choices:
   - `remote`—Send task logs to the Process log server only
   - `local`—Send task logs to the local file system only (default)
   - `both`—Send task logs to the Process log server and to the local file system
   - `none`—No task logging

8. `log-address`—Set the IP address and port of the process log server this task sends its task logs to. This parameter is entered in the form:
   ```
   IP_address:port_number
   ```

9. `internal-trace`—Set this parameter to `enabled` for the Net-Net SBC to save an interprocess message log (AMP traces) for messages to and from this task. The log file will be in the format: `task-name.log`.

10. Save your work using the ACLI `done` command.

Facility Logging

You can configure logging behavior for events of a specific facility type from a specific task. Facility logging is configured as a sub-element of task-logging, thus you must select the task-logging configuration element for the identified task before you set the facility logging parameters.
1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ACMEPACKET# configure terminal
   ACMEPACKET#

2. Type `system` and press <Enter> to access the system path.
   
   ACMEPACKET(configure)# system
   ACMEPACKET(configure)#

3. Type `system-config` and press <Enter>.
   
   ACMEPACKET(configure)# system-config
   ACMEPACKET(system-config)#

4. Type `task-logging` and press <Enter>.
   
   ACMEPACKET(system-config)# task-logging
   ACMEPACKET(task-logging)#

5. Select the task you wish to configure facility logging for and press <Enter>.
   
   ACMEPACKET(task-logging)# select
   <rtp_name>:
   1: sipls level=MINOR mode=BOTH server=0.0.0.0:0: 1 exceptions
   2: sipls level=MINOR mode=-none- server=0.0.0.0:0: no exceptions
   selection:2
   ACMEPACKET(task-logging)#

   **Note:** The number of exceptions reflects the number of facility logging configurations.

6. Type `facility-logging` to enter the facility-logging configuration element for the previously selected task.
   
   ACMEPACKET(task-logging)# facility-logging
   ACMEPACKET(facility-logging)#

7. `facility`—Set the facility type message you want to be logged according to the following parameters. A complete list of facility types is located in the “Facility Type List” section at the end of this chapter.

8. `level`—Set the log level at which the task will write this type of facility message. Valid values for this parameter are EMERGENCY, CRITICAL, MAJOR, MINOR, WARNING, NOTICE, INFO, TRACE, DEBUG.

9. `mode`—Set the mode of outputting the task’s type log file that determines the file’s destination.
   • remote—Send task logs to the Process log server only
   • local—Send task logs to the local file system only (default)
   • both—Send task logs to the Process log server and to the local file system
   • none—No task logging

10. `log-address`—Set the IP address and port of the process log server this task sends its type logs to. This parameter is entered in the form:
    
    IP_address:port_number

11. Save your work using the ACLI `done` command.
Real-time Logging Configuration

The previously discussed logging configurations are part of the Net-Net OS’s system-wide configuration. You can also change a task’s logging parameters in real-time, without reloading the full system configuration. These real-time commands are executed from the Superuser prompt and are as follows:

set log level

The `set log level` command lets you change the log level of a task from the command line without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility. Not supplying a facility argument sets the level for all facility types.

```
ACMEPACKET# set log level <task@slot.CPU.core> <log-level> [<facility> | all]
```

set log mode

The `set log mode` command lets you change where an task’s log files are output to, without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility to the given output location. Not supplying a facility argument sets the log mode for all facility types.

```
ACMEPACKET# set log mode <task@slot.CPU.core> [remote | local | both | default] [<facility> | all]
```

set log server

The `set log server` command lets you change the Process server where an task’s log files are sent to, without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility to the given Process server. Not supplying a facility argument sets the server for all facility types.

```
ACMEPACKET# set log server <task@slot.CPU.core> <server_ipaddress:port> [<facility> | all]
```

Displaying Current Logging Configuration

You can query the current state of a task’s logging configuration from the Superuser command prompt with the following commands:

show log level

The `show log level` command lets you view the log level for a supplied task. You can also specify a facility argument. The `<task@slot.CPU.core>` string can be replaced with `system` to indicate the AcmeLog and Syslog settings.

```
ACMEPACKET# show log level <task@slot.CPU.core> [ all | <facility> ]
```

show log mode

The `show log mode` command lets you view the output mode for a supplied task. You can also specify a facility argument.

```
ACMEPACKET# show log mode <task@slot.CPU.core> [ all | <facility> ]
```

show log server

The `show log server` command lets you view the configured Process log server for a supplied task. You can also specify a facility argument.

```
ACMEPACKET# show log server <task@slot.CPU.core> [ all | <facility> ]
```
Log File Maintenance

Log File Compression

By default, the Net-Net 9200 compresses all task log files using gzip after they are closed by the system (because they reached the 1MB file size limit). You can turn off this behavior if you choose.

To turn off log file compression:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ACMEPACKET# configure terminal
   ACMEPACKET#

2. Type `system` and press <Enter> to access the system path.
   
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#

4. Type `select` and press <Enter> to configure the existing system-config.
   
   ACMEPACKET(system-config)# select
   ACMEPACKET(system-config)#

5. `log-compression`—Set this parameter to `disabled` to disable log file compression.

6. Save your work using the ACCLI `done` command.

set log compression

The previously discussed log compression configurations is part of the Net-Net OS’s system-wide configuration. You can also change logging compression in real-time, without reloading the full system configuration. This real-time command is executed from the Superuser prompt and is as follows:

The `set log compression` command lets you enable or disable log compression from the command line without reloading the full system configuration.

   ACMEPACKET# set log compression [enabled | disabled]

show log compression

The show log compression command lets you view if logs are compressed or not.

   ACMEPACKET# show log compression

Rotating Log Files

Log files are written until they reach 1 MB. The log file is then closed and renamed with a .1 appended to the end of 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 13 of that
task’s log files have been created. When this limit is reached, the oldest file (the one with .12 appended to the name) is overwritten by the previous .11 file.

If flash memory is approaching capacity, less than 12 log files might saved at one time.

**Manually Rotating Log Files**

You can manually rotate a task’s log file by using the following command from the Superuser prompt:

```
ACMEPACKET# reset log <task@slot.CPU.core>
```

To rotate a trace log, you must include its filename at the end of the reset command. To rotate the trace log and the task log, you must include the term “all” at the end of the reset command:

```
ACMEPACKET# reset log <task@slot.CPU.core> [trace-log-filename | all]
```

**Manually Deleting Log Files**

You can manually delete all of a task’s closed log files by using the following command from the Superuser prompt:

```
ACMEPACKET# clear log <task@slot.CPU.core>
```

To delete a trace log, you must include its filename at the end of the close command. To delete a trace log and a task log, you must include the term “all” at the end of the reset command:

```
ACMEPACKET# clear log <task@slot.CPU.core> [trace-log-filename | all]
```

**Inserting Text into a Log File**

You can add a text message to a log file at any point. This can be useful to note a point in the debugging process. To insert text into a log file, use the following command from the Superuser prompt:

```
ACMEPACKET# set log echo <task@slot.CPU.core> <message>
```

For example:

```
ACMEPACKET# set log echo ACLI@0.0.0 BEGINNING BATCH TEST NOW
```

**Note:** This command only works when the task’s mode is set to local, remote, or both.

**Trace Log**

When it is necessary to view every message that a task sends or receives, you can use trace logging. The Net-Net 9200 outputs a protocol trace to a different log file than the aforementioned task log file. The trace log file is only created when the task’s log level is set to TRACE or higher.

**Trace Log Configuration**

1. In Superuser mode, type `configure terminal` and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type `system` and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ```
ACMEPACKET(system-config)#

4. Type **task-logging** and press <Enter>.

5. **rtp-name**—Set the task name and location of the task you are configuring in the form: `<task>@<slot>.<CPU>.<core>`

6. **level**—Set the log level to TRACE.

7. Save your work using the ACLI **done** command.

There are two ways to enable the trace log for a task in real-time, without reloading the full system configuration. These real-time commands are executed from the Superuser prompt and are as follows:

```
ACMEPACKET# debug <task@slot.CPU.core>
ACMEPACKET# set log level <task@slot.CPU.core> trace
```

All commands are equivalent to setting a task to debug, and writing the output to a trace log file. Valid tasks for the debug command are as follows:

<table>
<thead>
<tr>
<th>arpm</th>
<th>auth</th>
<th>broker</th>
<th>cm</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayman</td>
<td>dnsres</td>
<td>ftpdalg</td>
<td>hip</td>
</tr>
<tr>
<td>lcm</td>
<td>lem</td>
<td>logman</td>
<td>mbcd</td>
</tr>
<tr>
<td>natm</td>
<td>sem</td>
<td>sfe</td>
<td>sipc</td>
</tr>
<tr>
<td>sipls</td>
<td>sipt</td>
<td>sm</td>
<td>snmpd</td>
</tr>
<tr>
<td>sptx</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use the nodebug command to disable trace logging for a task.

```
ACMEPACKET# nodebug <task@slot.CPU.core>
```

**Trace Log Output**

The Net-Net OS follows three rules to determine trace log file output location. When trace logging is enabled:

1. If a task's logging mode is set to **remote** or **both**, and there is a configured process log server, then the trace log messages are sent only to the remote server, not to the local file system.

2. If a task’s logging mode is set to **local** or **none**, then the trace log messages are written to the local file system’s trace log message file.

3. If a task’s logging mode is set to **both**, but no Process log server is configured, the trace log message file is written only to the local file system.

**Task and Trace Log Filenames**

A trace log is easily identifiable by its file name. When trace logs are stored remotely, their filenames are in the format:

```
task_name.log@slot.CPU.core
```

Remotely stored task logs are in the format:

```
log.task_name@slot.CPU.core
```

When trace logs are stored locally, their filenames are in the format:
LOG FILE MANAGEMENT

\[ \text{task}\_\text{name.log} \]
When task logs are stored locally, their filenames are in the format:

\[ \text{log.task}\_\text{name} \]

### Debug Logging Timeout

Debug logging timeout disables debug-level logging if it is accidentally left enabled. This feature is a way to protect against accidentally putting an unnecessarily high load on the system. This timer applies to debug logging enabled via the `debug <task>` ACLI command only.

When a timeout occurs, the Net-Net SBC behaves as if the `nodebug sip` command has been implemented and debugging is disabled completely. A message is written to the console, syslog, and acmelog informing the user that debug logging has been disabled for all tasks. The following is an example of what a debug timeout message looks like:

```
Debug logging for lcm@0.0.0 has timed out
```

### ACLI Instructions and Examples

The new configuration parameter, debug-timeout, is part of the `system-config` configuration element. If this field is configured when debugging is already enabled, the timer begins immediately.

**To set a debug logging timeout on the Net-Net SBC:**

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ```
   ACMEPACKET# configure terminal
   ```
2. Type `system` and press <Enter>.
   
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```
3. Type `system-config` and press <Enter>. The prompt changes to let you know you can begin configuring individual parameters.
   
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```
4. `debug-timeout`—Enter the timeout, in seconds, for a debug logging to timeout. The valid range is 0-65535, with 0 (default) disabling the timeout feature.
5. Save and activate your configuration.

### Panic Log Dump

The Net-Net 9200 Panic Log Dump feature ensures that under exceptional system conditions, important debugging information is saved and archived to nonvolatile flash RAM before a card reset. This information can then be used to analyze and troubleshoot intermittent issues that are often hard to reproduce.

Just before a card goes OOS, as initiated by the system, all logs in the `/ramdrv/logs` directory of all of the cores on a TCU are compressed and saved. This may include DSP core dump images (which are often quite large).

Each TCU core zips all of its logs (including rotated backups) and pushes them to the active master core’s flash RAM, in a directory called `/code/dump/SCC`, where SCC stands for Slot, CPU, Core. For example: `/code/dump/411`
Note: Remember to set log levels appropriately, so they maintain a reasonable size.

Archived logs remain on the filesystem until overwritten by newer archives for the same cores, or until cleared by the user. The number of archived logs that can be stored on the system is limited by the size of the flash storage system. If filesystem is exceeded, some or all files will not be archived, but the TCU(s) in question will still be reset.

**Panic Log Dump Configuration**

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ACMEPACKET# configure terminal

2. Type `system` and press <Enter> to access the system path.
   
   ACMEPACKET(Configure)# system

3. Type `system-config` and press <Enter>.
   
   ACMEPACKET(system)# system-config

4. `dump-logs-on-failure`—Set this parameter to enabled to use the panic log dump feature.

5. Save your work using the ACLI `done` command.

**Managing Panic Log Dumps**

To manage log dumps, you can use the `show dumps` and `delete dumps` commands.

**show dumps**

The `show dumps` command lists all dumps present on any SPU present, for any card, cpu, or core. A slot argument is mandatory, or cpu and/or slot can be specified as `show dumps 2 0 1`. For example:

ACMEPACKET# show dumps 2

Log dumps stored on SPU 0 for 2.0.0:

<table>
<thead>
<tr>
<th>log.npm.gz</th>
<th>Dec 10 16:19:06</th>
<th>1972 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>log.lcm.gz</td>
<td>Dec 10 16:19:06</td>
<td>2197 bytes</td>
</tr>
<tr>
<td>log.lcm.gz</td>
<td>Dec 10 16:19:06</td>
<td>896 bytes</td>
</tr>
<tr>
<td>log.lcm.gz</td>
<td>Dec 10 16:19:06</td>
<td>1414 bytes</td>
</tr>
<tr>
<td>log.cm.gz</td>
<td>Dec 10 16:19:06</td>
<td>2944 bytes</td>
</tr>
<tr>
<td>log.broker.gz</td>
<td>Dec 10 16:19:06</td>
<td>855 bytes</td>
</tr>
<tr>
<td>log.kernel.gz</td>
<td>Dec 10 16:19:06</td>
<td>291 bytes</td>
</tr>
<tr>
<td>log.rdp.gz</td>
<td>Dec 10 16:19:06</td>
<td>2121 bytes</td>
</tr>
<tr>
<td>log.i2c.gz</td>
<td>Dec 10 16:19:06</td>
<td>126 bytes</td>
</tr>
<tr>
<td>log.dx240.gz</td>
<td>Dec 10 16:19:08</td>
<td>187 bytes</td>
</tr>
<tr>
<td>log.npsoft.gz</td>
<td>Dec 10 16:19:08</td>
<td>3957 bytes</td>
</tr>
<tr>
<td>log.npu.debug.gz</td>
<td>Dec 10 16:19:08</td>
<td>131 bytes</td>
</tr>
<tr>
<td>log.ftp.gz</td>
<td>Dec 10 16:19:08</td>
<td>125 bytes</td>
</tr>
<tr>
<td>log.arpm.gz</td>
<td>Dec 10 16:19:08</td>
<td>1478 bytes</td>
</tr>
<tr>
<td>log.natm.gz</td>
<td>Dec 10 16:19:08</td>
<td>987 bytes</td>
</tr>
<tr>
<td>log.npcli.gz</td>
<td>Dec 10 16:19:08</td>
<td>898 bytes</td>
</tr>
</tbody>
</table>
LOG FILE MANAGEMENT

Network Maintenance and Troubleshooting Guide Version S-D7.1.0

LOG FILE MANAGEMENT

log.sptx.gz Dec 10 16:19:08 640 bytes

Done.

Log dumps stored on SPU 0 for 2.0.1:

log.lcm.gz Dec 10 16:19:06 2195 bytes
log.lem.gz Dec 10 16:19:06 921 bytes
log.ntpd.gz Dec 10 16:19:06 1409 bytes
log.broker.gz Dec 10 16:19:06 858 bytes
log.kernel.gz Dec 10 16:19:06 254 bytes
log.rdp.gz Dec 10 16:19:06 3539 bytes
log.l2c.gz Dec 10 16:19:06 126 bytes
log.dx240.gz Dec 10 16:19:06 128 bytes
log.fdp.gz Dec 10 16:19:06 125 bytes
log.mbcd.gz Dec 10 16:19:06 3825 bytes

Done.

No log dumps stored on SPU 1 for 2.0.0

No log dumps stored on SPU 1 for 2.0.1

delete dumps

The delete dumps command requires a slot argument, but like show dumps it can also take a CPU, and core argument to delete only the files from that CPU or core.

ACMEPACKET# del dump 2
Delete all dumped files for slot 2 [y/n]? y

removing file /code/dump/200/log.npm.gz
removing file /code/dump/200/log.lcm.gz
removing file /code/dump/200/log.lem.gz
removing file /code/dump/200/log.ntpd.gz
removing file /code/dump/200/log.cm.gz
removing file /code/dump/200/log.broker.gz
removing file /code/dump/200/log.kernel.gz
removing file /code/dump/200/log.rdp.gz
removing file /code/dump/200/log.l2c.gz
removing file /code/dump/200/log.dx240.gz
removing file /code/dump/200/log.npsoft.gz
removing file /code/dump/200/log.npu_debug.gz
removing file /code/dump/200/log.ftp.gz
removing file /code/dump/200/log.arpm.gz
removing file /code/dump/200/log.natm.gz
removing file /code/dump/200/log.npclli.gz
removing file /code/dump/200/log.sptx.gz
deleting directory /code/dump/200
removing file /code/dump/201/log.lcm.gz
removing file /code/dump/201/log.lem.gz
removing file /code/dump/201/log.ntpd.gz
removing file /code/dump/201/log.broker.gz
removing file /code/dump/201/log.kernel.gz
removing file /code/dump/201/log.rdp.gz
removing file /code/dump/201/log.l2c.gz
removing file /code/dump/201/log.dx240.gz
removing file /code/dump/201/log.ftp.gz
removing file /code/dump/201/log.mbcd.gz
deleting directory /code/dump/201

SPU 0 deleting log dump directory /code/dump/200
Done.

SPU 0 deleting log dump directory /code/dump/201
Done.

SPU 1 deleting log dump directory /code/dump/200
Done.

SPU 1 deleting log dump directory /code/dump/201
Done.

**Viewing Logs**

Task and trace log files are located in the logs directory on the root of the local file system. You can access these files in three ways.

**FTP**

The FTPALG task can act as a proxy between the master core and all other cores on the Net-Net 9200. You can FTP directly to the master core and view and retrieve the log files located throughout the system. By FTPing to port 41, you will be redirected to view the desired log files. A system of directory names is used to navigate to the exact log file you wish to retrieve. The format of the directory names is

/ <slot>.<CPU>.<core>/logs

For example, to view the logs in SPU 2's 0-CPU, core-1, you would cd to /1.0.1/logs from the root of the FTPalg.
**AcmeLog**

To retrieve the AcmeLog, you must FTP to port 21 on the active SPU. The AcmeLog is located in `/ramdrv/logs/` directory, along with all other logs belonging to tasks that run on the active SPU’s master core.

**Note:** You can also retrieve the AcmeLog by FTPing to port 41 and then listing the `/0.0.0/logs` directory.
Facility Type List

- ALARM_FILTER
- ALARM_MGR
- ALG
- ANDD
- ARPMLOG
- BROKER
- CAM
- CHASSIS
- CLI
- CLIP
- HIP
- IPC (also trigger for AMP protocol tracing)
- IPFRAG
- IXF1104
- KERNEL
- LICENSE
- LOGECHO
- MEDIA
- MESSAGE
- MGCP
- REDUNDANCY
- SERVICE
- SESSION
- SFE
- SIP
- SIPNAT
- SIPREG
- SLOG_TYPE_CRITICAL
- SLOG_TYPE_EMERGENCY
- SLOG_TYPE_MAJOR
- SWINGLINE
- TAIL
- TCUHA
- TEST
- TESTMAN
- TIMER
- TM
- TRANS
- TRIP
- XC
2 Fault Management

Introduction

This chapter explains fault management on the Net-Net 9200. Topics covered include how to locate faults, communicate faults, determine their causes, and make corrections. Faults are communicated to the system administrator primarily through the following means:

- Alarms
- SNMP traps
- Graphic Display

Alarms

Overview

An alarm is triggered when a condition or event happens within either the Net-Net system’s hardware or software. Alarming is the way in which the Net-Net OS alerts administrators that there are problems with the system, and that the system may or may not need attention.

The Net-Net system’s alarm manager (AM) first receives an alarm message from a specific process. The AM locates the Alarm ID in the alarm table and can then proceed with the appropriate action. The alarm table is a list in the Net-Net OS that contains all of the actions required for acting on the alarm.

Alarming Process

An alarm is triggered when a condition or event happens within either the Net-Net system’s hardware or software. When this event occurs, a fault is identified in a responsible task. The task sends an alarm message to the local card manager (LCM). The LCM notes the alarm and makes a determination of health impact. The alarm message is forwarded to the AM. The AM reads the following alarm message attributes:

- **Alarm ID**—A unique integer that corresponds to a specific error or failure
- **Task ID**—The task and task ID that initiated the error
- **Severity**—The severity level of the condition or system failure
- **Previous Occurrences**—The first and most recent times this alarm type happened
- **Task Location**—Slot, CPU, Core where this task is running
- **Character string**—Textual description of the event or condition
- **Count**—Number of times this alarm has occurred since the system was powered on

When the conditions that triggered the alarm have returned to normal, the AM gets a clear message from the initiating task.
Alarm Categories and Responses

Alarms can fall into one of six categories. These categories let you know where on the Net-Net 9200 a problem has been identified.

<table>
<thead>
<tr>
<th>Alarm Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Hardware | This category of alarms is generated when there is a problem with the Net-Net 9200 chassis, feature or interface cards, power supplies, or cooling system. The following list provides some hardware alarm examples:  
  • Emergency/Critical—Extreme over temperature condition  
  • Major—Major over temperature condition  
  • Minor—Minor over temperature condition, Fan failure, Low voltage. |
| System | This category of alarms accounts for problems related to the Net-Net OS. It also includes low-level system calls as well as link status alarms (e.g., insufficient memory available, no file descriptors available, link down detected). |
| Network | This category of alarms accounts for problems related to low level network issues. This category of alarm might occur when code is unable to communicate with the hardware. It also includes alarms related to the following:  
  • Network processor management  
  • NAT  
  • CAM |
| Media | This category of alarm accounts for problems related to the MBCD, MBCD clients, and the functionality of ARP on the Net-Net 9200 system. It also includes alarms related to flows and bandwidth. |
| Application | This category of alarm accounts for problems related to applications (i.e., problems that involve protocols). The application alarm category also includes security breeches, session failures, and problems related to accounting. |
| Configuration | This category of alarm accounts for problems with the system, including any type of database issues that might arise. |

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>
<tr>
<td>Major</td>
<td>Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net system will suffer no physical harm, but it will cease to function.</td>
</tr>
</tbody>
</table>
Alarm Severity

Based on the system affected, and the severity of alarm fired, a specified health deduction occurs.

<table>
<thead>
<tr>
<th>Alarm Severity</th>
<th>Hardware Health Deduction</th>
<th>System Health Deduction</th>
<th>Network Health Deduction</th>
<th>Media Alarm Deduction</th>
<th>Application Alarm Deduction</th>
<th>Configuration Alarm Deduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>100</td>
<td>100</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Critical</td>
<td>75</td>
<td>75</td>
<td>37</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Major</td>
<td>50</td>
<td>50</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Minor</td>
<td>25</td>
<td>20</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Warning</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Response to Alarms

The Net-Net system is capable of taking a range of actions in response to an alarm. There are five actions the Net-Net system can take:

- Write messages to remote syslog server
- Create an SNMP trap
- Close hardware dry-contact
- Display a message on the Graphic Display
- Reboot the system

The Net-Net system maintains a table that lists the actions to take when an event of specific category and severity occurs.
### Alarm Table

Based on the alarm category and severity, the following table shows the Net-Net system’s response.

<table>
<thead>
<tr>
<th>Category</th>
<th>Emergency</th>
<th>Critical</th>
<th>Major</th>
<th>Minor</th>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>Trap Critical dry contact</td>
<td>Trap Critical dry contact</td>
<td>Trap Major dry contact</td>
<td>Trap Minor dry contact</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Graphic display Syslog</td>
<td>Graphic display Syslog</td>
<td>Syslog</td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Trap Reboot*</td>
<td>Trap Critical dry contact</td>
<td>Trap Major dry contact</td>
<td>Trap Syslog</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Trap Critical dry contact</td>
<td>Graphic display Syslog</td>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Graphic display Syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Trap Critical dry contact</td>
<td>Trap Critical dry contact</td>
<td>Trap Minor dry contact</td>
<td>Trap Syslog</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td>Graphic display Syslog</td>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td><strong>Media</strong></td>
<td>Trap Critical dry contact</td>
<td>Trap Critical dry contact</td>
<td>Trap Major dry contact</td>
<td>Trap Syslog</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td>Graphic display Syslog</td>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Trap Critical dry contact</td>
<td>Trap Critical dry contact</td>
<td>Trap Minor dry contact</td>
<td>Trap Syslog</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td>Graphic display Syslog</td>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>Trap Critical dry contact</td>
<td>Trap Critical dry contact</td>
<td>Trap Minor dry contact</td>
<td>Trap Syslog</td>
<td>Trap Syslog</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td>Graphic display Syslog</td>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
</tbody>
</table>

**Syslog / Acmelog**
The AM can write a record of the event to the syslog and Acmelog files.

**SNMP Traps**
The AM can send the appropriate SNMP trap to a configured trap receiver. An SNMP trap is an automatic event notification that the Net-Net system sends to external SNMP trap receivers. See this chapter's "Supported Standard Traps" for more details.

**Dry Contacts**
The Net-Net system supports three relays configured as an alarm port on the MIU card on the rear of the Net-Net 9200 chassis. The alarm port has three open circuits that each close when an alarm of a given level is active on the Net-Net system. The following alarm severity levels correspond directly to an individual circuit on the alarm port:
- Critical
- Major
- Minor

**Graphic Display**
The Net-Net system features a four line graphic display on the front panel of the chassis. The Net-Net OS displays messages concerning current alarm conditions on the graphic display window.
During an alarm condition, 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.

1 HW ALARM
2 LINK ALARMS

When an alarm condition is cleared, the base display replaces the alarm display. For more information about the alarm port and the graphic display, see the *Net-Net 9200 Hardware Installation Guide*.

**Card Reset**

Under certain, highly rare conditions, the Net-Net system can reset a card. The path to this happening is: failure event -> health degradation -> card switchover -> failed card reset.

**Operating Status Alarms**

The following system elements are periodically checked for health:

**Task Status**

If a task suspends or stops, it results in an EMERGENCY alarm along with a 100 point drop in the associated core's health score. When the task resumes, the EMERGENCY alarm is cleared and the core's health is restored.

**CPU Core Usage**

When the CPU load is greater than or equal to 95 percent, a NOTICE alarm is generated. When CPU load is greater than or equal to 99%, a WARNING alarm is generated. This degrades the core’s health by 5 points. Successive high CPU usage evaluations add additional 5 point health degradations. When the processor returns to less than 95 percent usage, health is restored based upon the CPU deductions previously accumulated.

This behavior can be overridden by setting the user-defined alarm thresholds.

**CPU Core Memory Usage**

When a core's memory usage is greater than or equal to 90%, a NOTICE alarm is generated. When a core's memory usage is greater than or equal to 95%, the core's health is degraded by 5 points and a MINOR alarm is generated. Successive high memory use evaluations result in continuing 5 point health degradations. When memory usage returns to < 95% usage, health is restored based upon the memory deductions previously accumulated.

This behavior can be overridden by setting the user-defined alarm thresholds.

**SPU Status**

The Net-Net 9200 periodically checks the health of the 24 port Ethernet switch that interconnects the system's internal network. Port and link status are checked for each connected core including connectivity to the standby SPU.

This SPU check occurs every 5 seconds and a WARNING alarm (5 point health degradation) is issued for a downed port or link on a serviceable core.

**NPU Status**

The Net-Net 9200 periodically checks the health of the 24 port switch that interconnects the NPUs to the NIUs used for valid external communication. Port and link status are assessed based upon interrupts received from the driver in response to link state changes. Link down conditions indicate an interruption in the network path and result in the generation of a MINOR alarm (20 point deduction).
The proportion of functioning ports to those configured is used to determine an overall health score for an NIU so its role (Active/Standby) may be ascertained. If a standby NIU has a higher percentage of functioning ports (configured + link active) than its redundant NIU, there will be a switchover.

**User Configured Alarms**

Some alarm thresholds are user-configured, overriding the default. These configurable alarms are for:

- CPU usage
- Memory usage
- Licensed session capacity

For each type of configurable alarms, you can set triggers for any combination of MINOR, MAJOR, and CRITICAL alarms severities based on the event reaching a specific level. Once triggered, the respective alarm’s health deduction is removed in the affected system.

Default alarm thresholds are set to generally permissive (high) levels and degrade system health less than the amount listed for their default alarm types (link). This provides built-in warning on a system without configured thresholds, and only causes failover in extreme cases.

**CPU alarms**

CPU usage alarms fall into the system category. High CPU usage will generate WARNING, and NOTICE alarms by default.

**Memory alarms**

Memory usage alarms fall into the system category. The Net-Net 9200 generates MINOR and NOTICE alarms by default. A user-configured MINOR threshold will override the built in MINOR threshold if set lower.

**License threshold**

License usage alarms fall into the application category. Session usage approaching the license capacity generates a MAJOR alarm when it exceeds 98 of the maximum number of sessions. A user-configured MAJOR threshold will override the built in MAJOR threshold.

**ACLI Instructions**

To manually configure alarm thresholds:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ```

2. Type `system` and press <Enter>.
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>.
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type `alarm-threshold` and press <Enter>.
   ```
   ACMEPACKET(system-config)# alarm-threshold
   ACMEPACKET(alarm-threshold)#
   ```
The system prompt changes to let you know that you can begin configuring individual parameters.

5. **type**—Enter the type of threshold you wish to configure. Valid types are CPU, memory, or sessions.

6. **severity**—Enter the severity level you will configure a custom health deduction for. Valid severity are MINOR, MAJOR, and CRITICAL.

7. **value**—Enter the percent of resource (type) in use that triggers the configured alarm (severity).

8. Save your work using the ACLI **done** command.

---

### Displaying and Clearing Alarms

Alarms are managed using the following ACLI commands:

- `show alarm`

#### Displaying Alarms

Besides writing to various log files and sending SNMP traps, the Net-Net system can indicate the presence of an alarm in three ways:

- Commands executed on the ACLI
- On the front-panel graphic display
- Via the alarm port on an MIU

For more information about the alarm port and the graphic display, see the *Net-Net 9200 Hardware Installation Guide*.

#### show alarm current

The **show alarm current** command is used to display the current alarms on the screen.

**To display Net-Net system alarms:**

1. Enter the **show alarm current** command.

```
ACMEPACKET# show alarm current
```

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

```
2 alarms to show

Alarm Id Task Id Severity Last Occurrence Count Description
-------- ------- -------- ------------- ----- redni

22620222 tSMq2.0.0 NOTICE 2007-11-05 15:48:10.500 1 NPU0 Switchover to Active Role
22611222 tSMq1.0.0 NOTICE 2007-11-02 19:08:26.683 1 SPU1 Switchover to Active Role
```

#### Filtering Alarms

Some error conditions continually send alarms to the AM until the problem is fixed. To keep the alarm table from becoming overwhelmed by redundant messages from the LCM, you can set a filter. You must supply the category of alarm to filter and the time period of arrival in which redundant messages are ignored. The set command usage is as follows:

```
ACMEPACKET# set alarm filter <task@location> [hardware | system | network | media | appl | config | all] <redundancy window in ms>
```
For example:

```
ACMEPACKET# set alarm filter lcm@0.0.0 hardware 200
```

The companion `show alarm filtered` command displays the total number of instances of redundant alarms received from a specified LCM. For example:

```
ACMEPACKET# show alarm filtered lcm@
ACMEPACKET# show alarm filtered lcm@0.0.0
LCM Alarm Filter List on 0.0.0
Alarm Id          Process Id          Severity           Instances
.........................  ............  ............  ............
No entries found in the Alarm Filter List.
```

### Clearing Alarms

Alarms can be cleared from the Net-Net system in three ways:

- The AM clears the alarm when an indication (clear alarm message) is received from the task where the alarming condition occurred.
- The system administrator manually clears the alarm via the ACLI or EMS.
- The AM clears the alarm after receiving an indication from the display manager that the Alarm Silence button was pressed.

When a task generates an alarm, it can clear that alarm too. For the AM to clear the alarm, the event or condition that caused the alarm must revert or correct itself. For instance, if an alarm is generated because the system’s temperature is high, and later the temperature returns to normal, the process that monitors these conditions sends a message to clear the alarm.

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.

### Automatic Alarm Clearing

When a task automatically clears an alarm because either the event has been remedied or something else has caused the task to return to baseline operation, you do not need to perform any action to remove the alarm.

### ACLI Instructions

You can clear an alarm manually, but you must first identify the alarm ID, task ID, and severity by using the `show alarms` command. The alarm ID is the number listed in the first column of that display.

**To clear a specific Net-Net system alarm:**

1. Ensure you are in Superuser Mode by noting the pound (#) sign at the end of the prompt. For example:
   
   `ACMEPACKET#`

2. Enter `show alarm current` 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. Type `clear alarm` followed by a <Space>, the alarm ID, another <Space>, the task ID, <space>, and severity of the task that generated the alarm, and press the <Enter> key.

   `ACMEPACKET# clear alarm 22620222 tSM@2.0.0 NOTICE`
You can use the Silence Alarms button located to the left of the graphic display on the front of the Net-Net 9200 chassis. Pressing this button silences the alarm port on the Net-Net 9200’s MIU. This button does not clear alarms from the alarm table.

### Configurable Alarm Thresholds

#### User-configured Alarms

Some alarm thresholds are user-configured, overriding the default thresholds at which alarms are triggered. These configurable alarms are for:

- CPU usage
- Memory usage
- Licensed session capacity

For each type of configurable alarms, you can set triggers for any combination of MINOR, MAJOR, and CRITICAL alarms severities based on the event reaching a specific level.

Default alarm thresholds are set to generally permissive (high) levels and degrade system health less than the amount listed for their default alarm types. This provides built-in warning on a system without configured thresholds, and only causes failover in extreme cases.

User-defined CPU and memory alarms are limited to degrading health by only 5 percent per health cycle, just like the higher of the two built-in alarm thresholds. This can still can reset the cards if left alone long enough, but allows enough time between resets for an administrator to remove the offending threshold and allow the system to recover. License capacity alarms do not affect system health.

#### CPU alarms

CPU usage alarms fall into the system category. High CPU usage will generate WARNING, and NOTICE alarms by default.

#### Memory alarms

Memory usage alarms fall into the system category. The Net-Net 9200 generates MINOR and NOTICE alarms by default. A user-configured MINOR threshold will override the built in MINOR threshold if set lower.

#### License threshold

License usage alarms fall into the application category. Session usage approaching the license capacity generates a MAJOR alarm when it exceeds 98% of the maximum number of sessions. A user-configured MAJOR threshold will override the built in MAJOR threshold.

#### ACLI Instructions

To manually configure alarm thresholds:

1. In Superuser mode, type `configure terminal` and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```
2. Type `system` and press <Enter>.
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```
3. Type `system-config` and press <Enter>.
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```
4. Type `alarm-threshold` and press <Enter>.
   ```
   ACMEPACKET(system-config)# alarm-threshold
   ACMEPACKET(alarm-threshold)#
   ```

   The system prompt changes to let you know that you can begin configuring individual parameters.

5. `type`—Enter the type of threshold you wish to configure. Valid types are `cpu`, `memory`, or `sessions`.

6. `severity`—Enter the severity level you will configure a custom health deduction for. Valid severity are `minor`, `major`, and `critical`.

7. `value`—Enter the percent of resource (type) in use that triggers the configured alarm (severity).

8. Save your work using the ACLI `done` command.

### SNMP Traps

An SNMP agent can notify an NMS of significant events by way of an unsolicited SNMP trap. SNMP traps are triggered by the AM, which decides, based on configuration, the appropriate trap to be sent. The Net-Net OS conforms to SNMPv2c.

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 *Acme Packet MIB Reference Guide*.

### Supported Standard Traps

The Net-Net OS supports standard traps and Acme Packet enterprise traps. See the *Acme Packet MIB Reference Guide* for specific information about each trap.

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>Trap Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</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.</td>
</tr>
</tbody>
</table>
Alarm Descriptions

This section describes the range of alarms the Net-Net 9200 uses to describe its operating conditions. Alarms are divided into six categories: hardware, system, media, network, media, application and configuration.

When alarms are displayed on the ACLI using the `show alarm current` command, the list includes the following columns:

- **Alarm Id**—An internally interpreted hexadecimal value.
- **Task Id**—The `task@card.cpu.core` which generated this alarm.
- **Severity**—The severity of the alarm created.
- **Last Occurrence**—The last occurrence of this alarm.
- **Count**—The number of times this alarm has been retriggered.
- **Description**—A textual description of the alarm.

The alarm tables below use the ZZ notation to denote the character positions that are variable values depending on the exact location (based on slot, CPU, port, core, or location) of the alarm.

Hardware Alarms

Hardware alarms include information about fans, system power, system temperature, internal devices, MIU cards, and NIU cards on 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 9200.

I2C Hardware Alarms

The following table lists the I2C hardware alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>Trap Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>I2C Failure/11900200</td>
<td>MAJOR/50</td>
<td>The environmental sensor component detects a failure.</td>
<td>apEnvMonI2CFailNotification OR apSyslogMessageGenerated (See Note 1)</td>
<td></td>
</tr>
<tr>
<td>I2C CARD FAILURE/118ZZ200</td>
<td>MAJOR/50</td>
<td>The environmental sensor component detects a card failure</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
<td></td>
</tr>
</tbody>
</table>
### Card Presence Alarms

The following table lists the card presence alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Trap Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>CARD REMOVED/127Z100</td>
<td>NOTICE/0</td>
<td>A card has been removed.</td>
<td>Card in Slot XX has been Removed.</td>
<td>entConfigChange</td>
</tr>
</tbody>
</table>

### I2C Alarm Types

The following table lists the I2C alarm types.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>I2C FAN FAULT/1186ZZ210</td>
<td>MAJOR/50</td>
<td>Fan fault detected.</td>
<td>Fan Fault on FAN Controller X - Affected fans are: Y.</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td>NORMAL/0</td>
<td>Fan fault cleared.</td>
<td>Clearing Fan Fault on FAN Controller X - Fan Mask Y.</td>
<td></td>
</tr>
<tr>
<td>I2C COMM LOSS/1186ZZ211</td>
<td>MINOR/20</td>
<td>Communication error detected.</td>
<td>• Comm Error Detected on X in Slot N.</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Comm Fault on FAN Controller X</td>
<td></td>
</tr>
<tr>
<td>I2C POWER WARNING/118ZZ220</td>
<td>MAJOR/50, MINOR/20</td>
<td>Power fault detected.</td>
<td>Power Warning on X in slot N</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Power Fault on X in slot N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Power not Present on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Voltage Input Fault detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Voltage Input Warning detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Temperature Fault detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Temperature Warning detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Fan Fault detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Voltage Output Fault detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Current Output Fault detected on Power Supply X</td>
<td></td>
</tr>
<tr>
<td>I2C TRACKING FAULT/118ZZ2250</td>
<td>MAJOR/50</td>
<td>Tracking fault detected</td>
<td>Tracking Fault on X in slot N</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>I2C CRC ERROR/118ZZ2251</td>
<td>MAJOR/50</td>
<td>Power CRC error detected.</td>
<td>Power CRC Error on X in Slot N</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
</tbody>
</table>
## I2C Link and Temperature Alarms

The following table lists the link and temperature alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>I2C TX FAULT/</td>
<td>MAJOR/50</td>
<td>Power transmission error detected.</td>
<td>Power Transmission Error in X on slot N</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>118ZZ252</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I2C SPEED FAULT/</td>
<td>MINOR/20</td>
<td>Fan speed fault detected.</td>
<td>Inconsistent Speed Setting on FAN Controller</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>118ZZ212</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| I2C LINK FAULT/    | MINOR/20                   | Link fault has been detected.                                            | • Tx Fault on Fiber PHY X::Port N  
• Bandwidth differs from value set on Fiber PHY X::Port N  
• Tx Disable differs from value set on Fiber PHY X::Port N  
• SFE has been removed on Fiber PHY X::Port N | apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1) |
| 118ZZ260           |                            |                                                                          |                                                                                                                      |                                                              |
| I2C TEMP WARNING/  | MINOR/20                   | • Temperature fault detected.                                            | • Temperature Warning on X in Slot N  
• Setting Minor Temperature Fault on FAN Controller X. Temp is XX.                                                      | apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1) |
| 128ZZ270           |                            |                                                                          |                                                                                                                      |                                                              |
| I2C TEMP HIGH/     | MAJOR/50                   | • Temperature fault detected.                                            | • Over Temperature Fault on X in slot N  
• Setting Major Temperature Fault on FAN Controller X. Temp is XX.                                                      | apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1) |
| 128ZZ280           |                            |                                                                          |                                                                                                                      |                                                              |
Voltage Alarms

The following table lists the voltage alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>I2C VOLTAGE FAULT/129ZZ230</td>
<td>MAJOR/50</td>
<td>Voltage fault detected.</td>
<td>Voltage Fault on X in slot N.</td>
<td>apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>I2C UNDER VOLTAGE/129ZZ231</td>
<td>MAJOR/50</td>
<td>Under voltage fault detected.</td>
<td>Under Voltage Fault on X in slot N</td>
<td>apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>I2C OVER VOLTAGE/129ZZ232</td>
<td>MAJOR/50</td>
<td>Over voltage fault detected.</td>
<td>Over Voltage Fault on something in slot N</td>
<td>apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td>I2C OVER CURRENT/118ZZ241</td>
<td>MAJOR/50</td>
<td>Over current fault detected.</td>
<td>Over Current Fault on X in slot N</td>
<td>apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
</tbody>
</table>

Specific Card Alarms

The following table lists the card specific failure alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY0 UNKNOWN TYPE/11450401</td>
<td>CRITICAL/100</td>
<td>Cannot identify PHY card type.</td>
<td>PHY 0 Unknown Type</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>PHY1 UNKNOWN TYPE/11451402</td>
<td>CRITICAL/100</td>
<td>Cannot identify PHY card type.</td>
<td>PHY 1 Unknown Type</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>PHY2 UNKNOWN TYPE/11452403</td>
<td>CRITICAL/100</td>
<td>Cannot identify PHY card type.</td>
<td>PHY 2 Unknown Type</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>PHY3 UNKNOWN TYPE/11453404</td>
<td>CRITICAL/100</td>
<td>Cannot identify PHY card type.</td>
<td>PHY 3 Unknown Type</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>PARITY ERROR/11420402</td>
<td>MAJOR/50</td>
<td>Parity error detected.</td>
<td>• Hardware Error in HSTRL: X, HINTR: Y</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware Error in HRSTR: X</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware Error in HPER: X</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware Error in CPER: X</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware Error in MPER: X</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware Error in XPER: X</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Testing Alarm for PE/CAM exceptions</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
</tbody>
</table>
FAULT MANAGEMENT

Miscellaneous Hardware Alarms

The following table lists the miscellaneous hardware alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/ Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAM EXCEPTION/</td>
<td>MAJOR/ First time alarm is posted</td>
<td>CAM exception detected.</td>
<td>Cam Search Semaphore Error, Err Code X, Err: Y</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>11420403</td>
<td>CRITICAL/ Second time alarm is posted without a clear</td>
<td></td>
<td>Cam Operation Failure, Err Code X, Err: Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMERGENCY/ Third time alarm is posted without a clear</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50, 100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS ERROR/</td>
<td>MAJOR/ QoS error detected.</td>
<td></td>
<td>Hardware Error in QoS_FPGA_config ( )</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>11420404</td>
<td>50</td>
<td></td>
<td>Error in QoS_daemon_init ()</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hardware Error: QoS FPGAs initialized in failed state</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gimp HW Error, Err: X, Gimp: Y ISR_Vector: Z</td>
<td></td>
</tr>
<tr>
<td>NPM FAILURE/</td>
<td>MAJOR/ NPM failure detected.</td>
<td>Media Startup failed</td>
<td>apSysMgmtHardwareErrorTrap</td>
<td></td>
</tr>
<tr>
<td>11420405</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPT Failure/</td>
<td>EMERGENCY IPT test failure</td>
<td>IPT NP path Runtime Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11420406</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSP FAILURE TCUX</td>
<td>MINOR DSP failed in TCU.</td>
<td></td>
<td>DSP device N failed to boot</td>
<td>None</td>
</tr>
<tr>
<td>BASE/ 1003XSZZ</td>
<td>CRITICAL/ DSP device N failed to INITIALIZE</td>
<td></td>
<td>DSP device N failed to INITIALIZE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20, 100</td>
<td></td>
<td>DSP DEVICE CRASHED</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DSPComms Timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rebooted DSP device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VAPI Request Timeout</td>
<td></td>
</tr>
</tbody>
</table>

System Alarms

System alarms include information about NIU and MIU port status, hardware threshold status, redundancy status and other system operating conditions on the Net-Net 9200.
## NIU Link Alarms

The following table lists the NIU link alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINK DOWN ALARM GIGPORT/20250016-20250031</td>
<td>CRITICAL/75</td>
<td>Gigabit Ethernet interface goes down.</td>
<td>PHY X::Port N Link State is Inactive</td>
<td>linkDown</td>
</tr>
</tbody>
</table>

## MIU Link Alarms

The following table lists the MIU link alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINK DOWN ALARM VXINTF 0/20240003</td>
<td>CRITICAL/75</td>
<td>MIU 0 goes down.</td>
<td>MIU X Link Is Down</td>
<td>linkDown</td>
</tr>
<tr>
<td>LINK DOWN ALARM VXINTF 1/20240003</td>
<td>CRITICAL/75</td>
<td>MIU 1 goes down.</td>
<td>MIU X Link Is Down</td>
<td>linkDown</td>
</tr>
<tr>
<td>LINK DOWN ALARM VXINTF 2/20240003</td>
<td>CRITICAL/75</td>
<td>MIU 2 goes down.</td>
<td>MIU X Link Is Down</td>
<td>linkDown</td>
</tr>
</tbody>
</table>

## NPU Link Alarms

The following table lists the NPU link alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWING VIX ALARM/21420301</td>
<td>MINOR/20</td>
<td>Status check failed.</td>
<td>VIX Status Check Failed</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING VIX ALARM DOWN IN PORT A/21420302</td>
<td>WARNING/0</td>
<td>Inbound port A is down.</td>
<td>VIX In-Port-A Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING VIX ALARM DOWN IN PORT B/21420303</td>
<td>WARNING/0</td>
<td>Inbound port B is down</td>
<td>VIX In-Port-B Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING VIX ALARM DOWN IN PORT A/21420304</td>
<td>WARNING/0</td>
<td>Outbound port B is down.</td>
<td>VIX Out-Port-A Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING VIX ALARM DOWN IN PORT B/21420305</td>
<td>WARNING/0</td>
<td>Outbound port B is down.</td>
<td>VIX Out-Port-B Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING PLL ALARM/21420306</td>
<td>MINOR/20</td>
<td>Status check failed.</td>
<td>PLL Status Check Failed</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING PLL ALARM DOWN PORT A/21420307</td>
<td>WARNING/0</td>
<td>Port A is down.</td>
<td>PLL Port A Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
<tr>
<td>SWING PLL ALARM DOWN PORT B/21420308</td>
<td>WARNING/0</td>
<td>Port B is down</td>
<td>PLL Port B Down</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
</tbody>
</table>
### FAULT MANAGEMENT

#### TCU Link Alarms

The following table lists the TCU link alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLAIR SWING ALARM/ 21430301</td>
<td>MINOR/20</td>
<td>FLAIR driver was not set to the active NPU.</td>
<td>TCU XX Failed to Set FLAIR Driver to Active NPU YY.</td>
<td>apSysMgmtHardwareErrorTrap</td>
</tr>
</tbody>
</table>

#### Utilization Alarms

The following table lists the system utilization alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEM UTIL OVER THRESHOLD/ 21E00104</td>
<td>MINOR WARNING NOTICE/5</td>
<td>Memory usage has changed. Memory usage was XX percent and now is YY percent</td>
<td>apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)</td>
<td></td>
</tr>
<tr>
<td>CPU UTIL OVER THRESHOLD/ 21E00103</td>
<td>WARNING NOTICE/5</td>
<td>CPU usage has changed. CPU usage was XX percent and now is YY percent</td>
<td>apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)</td>
<td></td>
</tr>
</tbody>
</table>
### Fault Management

#### Health Score Alarms

The following table lists the health score alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
</table>
| SYS HEALTH ALERT/200X0201 | EMERGENCY/CRITICAL/MINOR/100, 75, 20 | • Boot timeout occurs  
• Register timeout occurs  
• Manifest timeout occurs  
• Ready timeout occurs  
• Becoming Active timeout occurs  
• Becoming Standby timeout occurs  
• Becoming OOS timeout occurs | • Boot Timeout on slot XX  
• Register Timeout on slot XX  
• Manifest Timeout on slot XX  
• Ready Timeout on slot XX  
• Becoming Active Timeout on slot XX  
• Becoming Standby Timeout on slot XX  
• Becoming OOS Timeout on slot XX | apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2) |
| SYS HEALTH UNDER THRESHOLD/21EX0210 | NOTICE/0 | Net-Net system’s health is under threshold 50. | Health Score Dropped to XX on Card YYY | apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2) |
| SYS HEALTH TIMEOUT/200X0202 | MINOR/20 | Health check timeout occurs | Health Check Timeout on Card XX | apSyslogMessageGenerated |
| SYS HEALTH RESET/200Z0203 | EMERGENCY/100 | A card has failed to boot. | Card XX has failed to boot | apSyslogMessageGenerated |

#### Redundancy Alarms

The following table lists the redundancy alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS SWITCH TO UNASSIGNED/226ZZ221</td>
<td>NOTICE/0</td>
<td>A state transition occurred to Unassigned.</td>
<td>&lt;Name of HA peer&gt; Switch to Unassigned Role</td>
<td>apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)</td>
</tr>
<tr>
<td>SYS SWITCH TO ACTIVE/226ZZ222</td>
<td>NOTICE/0</td>
<td>A state transition occurred from Standby/BecomingStandby to BecomingActive.</td>
<td>&lt;Name of HA peer&gt; Switch to Active Role</td>
<td>apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)</td>
</tr>
</tbody>
</table>
## System Task Alarms

The following table lists the system task alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS TASK SUSPENDED/20A00101</td>
<td>MAJOR/50</td>
<td>A Net-Net system task (process) suspends or fails.</td>
<td>Task XX Failed to Spawn</td>
<td>apSysMgmtTaskSuspendTrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMERGENCY/100</td>
<td></td>
<td>Task XX with PID YY is Suspended</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMERGENCY/100</td>
<td></td>
<td>Task XX with PID YY is Stopped</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMERGENCY/100</td>
<td></td>
<td>Task XX no longer Running</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WARNING/5</td>
<td></td>
<td>Task XX not ready</td>
<td></td>
</tr>
</tbody>
</table>

## System State Alarms

The following table lists the system state alarm information.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
</table>
| SYS SNMP AUTH FAILURE/20110233 | MAJOR/0                     | SNMP authentication failure                        | SNMP Agent got improper request from community XXX at address YYY
SNMP Agent received bad community string XXX from address YYY | authenticationFailure (See Note 3) |
| SYS PASSWORD RESET/20000236    | NOTICE/0                    | Password reset to factory defaults                 | SA Status Change                   | None                                                                            |
**System Miscellaneous Alarms**

The following table lists miscellaneous system alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU NONE ACTIVE/20020401</td>
<td>EMERGENCY/100</td>
<td>No NPUs active or present.</td>
<td>• System Unable to Run - No NPUs Active&lt;br&gt;• System Unable to Run - No NPUs present</td>
<td>apSyslogMessageGenerator</td>
</tr>
<tr>
<td>PHY NONE ACTIVE/20050402</td>
<td>EMERGENCY/100</td>
<td>No PHYs active or configured.</td>
<td>• No PHYs Active to Pass Media&lt;br&gt;• No PHYs Configured to Pass Media</td>
<td>apSyslogMessageGenerator</td>
</tr>
<tr>
<td>RDP LINK DOWN ALARM/20ZZ0001</td>
<td>EMERGENCY NOTICE/0, 100</td>
<td>The core is non-responsive.</td>
<td>• Core X.X.X Link is Non-Responsive&lt;br&gt;• Internal Communication Link Down (XX = =&gt; YY)</td>
<td>apSyslogMessageGenerator</td>
</tr>
<tr>
<td>IFSTRUCT CORRUPT ALARM/20000501</td>
<td>MAJOR/50</td>
<td>The interface structure is corrupt.</td>
<td>• An internal data structure is corrupt and the system may not behave properly – Error Code &lt;X&gt;</td>
<td>apSyslogMessageGenerator</td>
</tr>
</tbody>
</table>

**Low Disk Space Alarm**

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPACE_LOW_THRES_ALARM_PCMIA/24400100</td>
<td>User configurable/Non-health affecting</td>
<td>Storage space on the PCMCIA FLASH card is low; thresholds are configurable.</td>
<td></td>
<td>apSysMgmtSpaceAvailThresholdTrap</td>
</tr>
</tbody>
</table>
# Switch Alarms

## NPU Switch

The following table lists the alarms for the NPU switch.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>DX240 ERROR/10020300</td>
<td>MINOR/MAJOR/20</td>
<td>NPU failed to switch over.</td>
<td>• NPU nn Failed to Switchover to Active Status</td>
<td>apSyslogMessageGenerated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NPU nn Failed to Switchover to Standby Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NPU nn Failed to Switchover to OOS Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NPU nn Switch Failed to Perform Health Check</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NPU nn Failed to initialize PHY YY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NPU nn Failed to connect to Active PHY YY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DX240 Phy Reg Read Failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DX240 Phy Reg Write Failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DX240 Reg Write Failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DX240 Reg Read Failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Fatal Dx240 Interrupt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Minor DX240 Error</td>
<td></td>
</tr>
<tr>
<td>DX240 DOWN ALARM GMAC 0/10020302-1002030A</td>
<td>MAJOR/50</td>
<td>GMAC port link state is inactive.</td>
<td>GMAC Port nn Link State is Inactive</td>
<td>apSyslogMessageGenerated</td>
</tr>
</tbody>
</table>

## SPU Switch

The following table lists the alarms for the SPU switch.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM56K PCI BUS ERR/10010300</td>
<td>MAJOR/50</td>
<td>PCI Error</td>
<td>BROADCOM 56304 sysconf_attach</td>
<td>apSyslogMessageGenerated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PCI error on soc_unit X</td>
<td></td>
</tr>
</tbody>
</table>

## Network Alarms

The following table lists the network alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIA GATEWAY ALARM/31020ZZZ</td>
<td>MAJOR/25</td>
<td>Gateway is unreachable.</td>
<td>Gateway N.N.N.N unreachable on slot X, port Y, subport Z</td>
<td>apSysMgmtGatewayUnreachableTrap OR apSyslogMessageGenerated</td>
</tr>
</tbody>
</table>
### Media Alarms

Media alarms include events related to MBCD exception conditions. The following table lists the MBCD media alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
</table>
| MBCD ALARM OUT OF MEMORY/40E00001 | CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)/0 | No further memory can be allocated for MBCD. | • Flow: Cannot create free port list for realm ‘XXX’.  
• Failed to allocate new context  
• Media XX Timer Expired: camid=YY: unable to allocate request, context or command! dropping Flow. | apSysMgmtMediaOutOfMemory OR apSyslogMessageGenerated (See Note 2) |
| MBCD ALARM INTERNAL/40000002 | MAJOR MINOR/0 | An internal software error. | Internal Error. No agent for socket <IPPort>. | apSyslogMessageGenerated |
| MBCD ALARM UNKNOWN REALM/40F00003 | MINOR/0 | Media server is unable to find realm interface. | • ingress realm XXX not found  
• egress realm XXX not found | apSysMgmtMediaUnknownRealm OR apSyslogMessageGenerated (See Note 2) |
| MBCD ALARM OUT OF BANDWIDTH/40D00005 | CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%/0 | The realm is out of bandwidth. | out of bandwidth | spSysMgmtMediaBandwidthTrap OR apSyslogMessageGenerated (See Note 2) |
| MBCD ALARM OUT OF PORTS/40C00006 | CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%/0 | The realm is out of steering ports. | out of steering ports | apSysMgmtMediaPortsTrap OR apSyslogMessageGenerated (See Note 2) |
Application Alarms

Application alarms include events related to application exceptions on the Net-Net system.

RADIUS Connection Down Alarm

The following table lists the RADIUS connection down alarm.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP ALARM LOST ACCT CONN/51100001</td>
<td>CRITICAL: if all enabled and configured RADIUS accounting server connections have timed-out without response from the RADIUS server. MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server.</td>
<td>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.</td>
<td>apSysMgmtRadiusDownTrap OR apSyslogMessageGenerated (See Note 2)</td>
<td></td>
</tr>
<tr>
<td>APP_ALARM_EPS_RA CF_CONN_FAIL</td>
<td>MINOR/0</td>
<td>Connection to External Policy Server has been lost.</td>
<td>Connection to External Policy Server (RACF) has been lost!!!</td>
<td>apSysMgmtExtPolicyServerConnDownTrap</td>
</tr>
</tbody>
</table>

Application Alarms

The following table lists the application alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP ALARM APPROACH LIC SESS CAP/51B00004</td>
<td>MAJOR/1</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>apSyslogMessageGenerated or apLicenseApproachingCapacityNotification (See Note 2)</td>
</tr>
<tr>
<td>COLLECT_ALARM_PUSH_FAIL /</td>
<td>MAJOR if all push receivers are unreachable MINOR if a push receiver is unreachable while other(s) are still reachable.</td>
<td>The push receivers are unreachable. &quot;Some or all of collector's push receivers are down&quot; &quot;All of collector's push receivers are down&quot;</td>
<td>apSysMgmtPushServerUnreachableTrap apSysMgmtPushServerUnreachableClearTrap</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Alarms

The following table lists the configuration alarms.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Example Log Message</th>
<th>SNMP Traps Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG ALARM SAVE FAILED/61300001</td>
<td>MAJOR/1</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</td>
<td>apSysMgmtCfgSaveFailTrap</td>
</tr>
</tbody>
</table>

**Note:** 1. If the “enable-env-monitor-traps” parameter under the system-config configuration element is enabled, this trap is sent. If the parameter is disabled, the “asSyslogMessageGenerated” trap is sent instead.

**Note:** 2. If the “enable-snmp-monitor-traps” parameter under the system-config configuration element is enabled, this trap will be sent. If the parameter is disabled, the “apSyslogMessageGenerated” trap is sent instead if configured to enable-syslog-notify.

**Note:** 3. If the “enable-snmp-auth-traps” option under system-config is disabled, this trap will not be sent.

Graphic Display

The graphic display lets you view information about the system’s operational status and current alarms at a glance. In addition, you can silence alarms from the front panel of the Net-Net 9200 chassis.

For a complete description of the graphic display operation, please see the *Net-Net 9200 Hardware Guide* for more information.
3 System Management

Commands discussed in this chapter are used for Net-Net OS management and system administration.

Global System Parameters

This section contains information about global system show commands.

System State

The following show commands are explained in this section:

- uptime
- state
- version
- clock
- bootparams

show uptime

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

```
ACMEPACKET# show uptime
System Uptime:      5 Days, 14 Hours 23 Minutes 30 Seconds
```

show system

The show system command displays environmental, uptime, and memory information about the Net-Net system. For example:

```
ACMEPACKET# show system
System Uptime:      5 Days, 14 Hours 23 Minutes 52 Seconds
Temperature Status: Normal
Voltage Status:     Normal
Fan Status:         Alarm
CPU Status:         Normal
Memory Status:      Normal
```

show version

The show version command displays the Net-Net OS version currently running on the hardware. This command also displays the current configuration version and the running configuration version. For example:

```
ACMEPACKET# show version
NN9200 Software Version: 5.0.0 Beta Workspace (Build 19)
NN9200 Software Build Date: 06/30/06
Built in /home/NEOBETA on acme33

Current config version: 761
Running config version: 761
```
**show clock**

The show clock command displays the current UTC system time and date. For example:

```
ACMEPACKET# show clock
System Time: 11:51:02 - Thu Jul 06 2006
```

**show bootparams**

The show bootparams command displays the boot parameters for both SPUs.

- boot device and unit number—describe the Net-Net 9200’s management interface that is used to boot from the network
- processor number—only used for administrative purposes
- inet on ethernet—IP address of the MIU Ethernet boot interface
- host inet (h)—network TFTP server’s IP address that hosts the boot image file
- gateway inet (g)—gateway IP address for the management network, where the boot image is located.
- user (u) and ftp password (pw)—user and password pair for connecting the TFTP server.
- flags (f)—only used for administrative purposes
- target name (tn)—name that appears behind the > or # at the system prompt.

The virtual management interface and gateway are also displayed. A virtual management interface IP Address is assigned to the MIU’s Ethernet port on the active SPU/MIU pair. This means that you can Telnet to the configured virtual address, and you will be connected to the active SPU, regardless of which physical SPU is active.

All parameters visible in the bootparams are configurable by using the set bootparams command.

For example:

```
ACMEPACKET# show bootparams

Boot parameters stored on ACTIVE SPU:

--- Slot 0 Boot Parameters ---
boot device          : eth
unit number          : 2
processor number     : 0
file name            : sd4xx.tar
inet on ethernet (e) : 172.30.92.94
host inet (h)        : 172.30.0.25
gateway inet (g)     : 172.30.0.1
user (u)             : *****
ftp password (pw)    : *****
flags (f)            : 0x0
target name (tn)     : ACMEPACKET

--- Slot 1 Boot Parameters ---
```

--- End of Document ---
boot device : eth
unit number  : 2
processor number  : 0
file name       : sd4xx.tar
inet on ethernet (e) : 172.30.92.92
host inet (h)   : 172.30.0.25
gateway inet (g) : 172.30.0.1
user (u)        : *****
ftp password (pw) : *****
flags (f)       : 0x0
target name (tn) : ACMEPACKET

--- Virtual Management Interface Parameters ---

Interface IP Address: 172.30.92.96
Gateway IP Address: 172.30.0.1

### Installed Features

You can audit the enabled features on the Net-Net 9200 by using the `show features` command. For example:

```
ACMEPACKET# show features
64000 SIP sessions
SIP, QOS, Routing, Load Balancing, Accounting
```

The same information is found by watching the boot process of the Net-Net 9200, however this command can be invoked without a system reboot.
**Task Overview**

Tasks run across the Net-Net system’s multiple CPUs and cores. To aid in debugging, the following information is essential.

- For a given core, show the local tasks
- Show the core where each major application runs

**Note:** SPU2/NPU2-based systems may reflect tasks running on different CPUs/Cores than the following SPU1/NPU1-based examples.

**show cpu**

The `show cpu` command displays the top 15 tasks active on a specified core. Enter the `show cpu` command with the slot.cpu.core location in dotted notation. The output of this 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 task’s CPU usage.
- **Status**—Status of the task’s CPU usage.
- **Total CPU**—Task’s total CPU usage since last reboot.
- **Avg**—Displays percentage of CPU usage since the Net-Net system was last rebooted.
- **Now**—Task’s CPU usage in the latest sample (1-2 seconds).

**Note:** Adding the `all` argument after the core location returns the load for all tasks on the given core.

For example:

```
ACMEPACKET# show cpu 0.0.0
CORE=0.0.0

----------------------------  -------- --- ---------- -------------- ----- ----- 
Task Name       Task Id  Pri Status          Total CPU   Avg   Now  
----------------------------  -------- --- ---------- -------------- ----- ----- 
iAcli           c4c7eb50 100 READY               4.198   0.0   1.2  
bcmL2X.0        c477b050  50 PEND+T          27:35.258   0.3   0.4  
tNetTask        c1a12010  50 PEND            26:11.257   0.3   0.3  
bcmCNTR.0       c474e200  50 PEND+T          15:57.280   0.1   0.2  
iCm             c4d1f260 100 PEND+T           6:33.093   0.0   0.1  
iNtpd           c4cf7c00 100 PEND+T           2:10.053   0.0   0.0  
tTffsPTask      c1a15010  100 DELAY            1:43.432   0.0   0.0  
iTestman        c4d9e020 100 PEND+T           1:35.513   0.0   0.0  
iSm             c4b8b6e0 100 PEND+T           1:33.421   0.0   0.0  
iLogman         c4caebf0 100 PEND+T           1:25.082   0.0   0.0  
tEth0CpuRx      c1a8f030  50 PEND            1:12.983   0.0   0.0  
tDcacheUpd      c458d780  250 DELAY              59.307   0.0   0.0  
ilcm            c4769450  60 READY       131:59:12.790  98.1  96.9  
tSSH            c4c9c1b0  55 PEND+T           42.808   0.0   0.0  
tIdle           c1a15350  255 READY       131:59:12.790  98.1  96.9  
```

72 Net-Net 9000 Maintenance and Troubleshooting Guide

Proprietary & Confidential
By using the optional **summary** argument, the command returns the total and current CPU load for each core. In addition, the two tasks with the current highest CPU usage per listed core are displayed. For example:

```
ACMEPACKET# show cpu summary

Core  Cur/Total       Task: Current/Total       Task: Current/Total
------  ---------   ----------------------   --------------------------
0.0.0    2.0/20.2   bcmLSM:  0.9/0.9         tNetTask:  0.4/3.3
0.0.1    0.2/0.2    tNetTask:  0.1/0.0      tLCM:  0.0/0.0
```

- **Cur (Current)**—CPU usage in the latest sample (1-2 seconds)
- **Total**—Total CPU percentage is computed as follows:

\[
\text{Total CPU \%} = \frac{\text{Core Uptime} - \text{tIdle time}}{\text{Core Uptime}}
\]

**show manifest**

The **show manifest** command displays application tasks, their location, and internal address and socket used for communication. For example:

```
ACMEPACKET# show manifest

Location  Task       IPPort
0.0.0     snmpd      169.254.160.0:8031
0.0.1     dnsres     169.254.160.1:8022
0.0.1     rasm       169.254.160.1:8030
0.1.0     sipt       169.254.160.16:8008
0.2.0     sipc       169.254.160.32:8010
0.4.1     sipls      169.254.160.65:8009
1.0.0     snmpd      169.254.161.0:8031
1.0.1     dnsres     169.254.161.1:8022
1.0.1     rasm       169.254.161.1:8030
1.1.0     sipt       169.254.161.16:8008
1.2.0     sipc       169.254.161.32:8010
1.4.1     sipls      169.254.161.65:8009
2.0.0     mbcd       169.254.162.0:8011
2.0.0     sfe        169.254.162.0:8013
3.0.0     mbcd       169.254.163.0:8011
3.0.0     sfe        169.254.163.0:8013
```
User Sessions

Multiple Telnet, SSH, FTP, or SFTP sessions can be active on the Net-Net 9200 simultaneously. You can view the status of each session and terminate (kill) an active session from the ACLI.

show users

The **show users** command displays all active sessions on the Net-Net 9200. For example:

```
ACMEPACKET# show users
Index remote-address IdNum duration type state redirect
----- -------------- ----- -------- ---- --------
0            1 2:40:01 console0 priv*
1 10.1.20.105:2844 2 2:39:25 telnet0 user
2            3 2:39:17 console1 login
3 10.1.20.105:2848 5 2:36:41 ssh0 priv C
```

The IdNum of each session is used for identifying which session to terminate. The session with an asterisk, *, trailing the state is the one you are logged in from. The session with a C trailing the state is in configuration mode. Any session with a trailing caret, ^, is dead and must be manually terminated.

Identifying Config Sessions

If you are denied from entering configuration mode because another session is in configuration mode, the ACLI will print the following warning:

```
ACMEPACKET# configure terminal
Configuration menu in use.
ACMEPACKET#
```

To identify which session is in configure mode, use the **show users** command. In the following example, the session with IdNum 5 is in config mode as noted by the C next to its state column:

```
ACMEPACKET# show users
Index remote-address IdNum duration type state redirect
----- -------------- ----- -------- ---- --------
0            1 2:40:01 console0 priv*
1 10.1.20.105:2844 2 2:39:25 telnet0 user
2            3 2:39:17 console1 login
3 10.1.20.105:2848 5 2:36:41 ssh0 priv C
```

Terminating Sessions

In order to manually terminate a Telnet or SSH session on the Net-Net 9200, the **kill** command is used. The **kill** command is used in conjunction with a session IdNum, obtained from the output of the show users command. For example:

```
ACMEPACKET# kill 5
```

After executing the **kill** command, the chosen session is terminated immediately without any warning or confirmation message.

Management Applications

The Net-Net 9200 runs Telnet, FTP, and SSH applications as a means to be configured and for file retrieval. Each of these applications
Show Telnet

The `show telnet` command displays whether the telnet daemon is enabled or not. For example:

```
ACMEPACKET# show telnet
Telnet is enabled
```

Show Ftp

The `show ftp` command displays whether the FTP daemon is enabled or not. For example:

```
ACMEPACKET# show ftp
Ftp is enabled
```

Show Ssh

The `show ssh` command displays SSH operating parameters for each slot on the Net-Net SBC. For example:

```
ACMEPACKET# show ssh
slot 0 :
   cnum            0
   mastrFD         397
   slaveFD         398
   pipe            /pipe/ssh0
   pipeFD          396
   sesID           0
   socket          -1
   sshHdl          0
   outTID          -1
   waitTID         -1
```

Statistic Counts Explained

Statistical counts are based on the Net-Net OS defining a period as 100 seconds. The Recent window represents the previous complete period (100 seconds) plus the time incurred into the current period.

When you execute a `show` command, a timestamp and the period count are displayed. The period count, the number after the dash, indicates the number of seconds into the recent period. Therefore, the recent window ranges from 100 to 199 seconds. For example:

```
ACMEPACKET# show amp lcm@0.0.0
12:10:21-175 (lcm@0.0.0) ID=10000
```

In the diagram below, the Net-Net OS is 75 seconds into the current period. The Recent window includes the previous 75 seconds, plus an extra 100 seconds (1
period) before that. After period 3 is entered (not pictured below), the Recent window will begin at the 100 second mark.

For statistical displays, the columns are defined as follows:
- **Active** represents the current number of active counts.
- **Recent High** represents the highest number during the recent window.
- **Recent Total** represents the total accumulated count during the recent window.

The three lifetime statistics begin accumulating since the last reboot.
- **Lifetime Total** represents the total accumulated count.
- **Lifetime PerMax** represents the maximum recorded in one period.
- **Lifetime High** represents the highest momentary count.

### Task Statistics

The commands listed in this section are used to view task statistics and related information.

#### Task Statistic Overviews

The following `show` commands display high-level statics for tasks based on their active or standby status.

**show task active**

The `show task active` command displays overview statistics for all active application tasks on all cores. For example:

```
ACMEPACKET# show task active

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Per</th>
<th>Msgs</th>
<th>Trans</th>
<th>Timers</th>
<th>TOQs</th>
<th>PerCPU</th>
<th>Total-CPU</th>
<th>MaxCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>sipt@0.0.0</td>
<td>118</td>
<td>4</td>
<td>0</td>
<td>20</td>
<td>1</td>
<td>0.0</td>
<td>6.10</td>
<td>0.0</td>
</tr>
<tr>
<td>sipc@0.0.0</td>
<td>118</td>
<td>3</td>
<td>0</td>
<td>20</td>
<td>1</td>
<td>0.0</td>
<td>3.77</td>
<td>0.0</td>
</tr>
<tr>
<td>sips@0.0.0</td>
<td>118</td>
<td>3</td>
<td>0</td>
<td>20</td>
<td>1</td>
<td>0.0</td>
<td>3.74</td>
<td>0.0</td>
</tr>
<tr>
<td>dnsres@0.0.0</td>
<td>118</td>
<td>4</td>
<td>0</td>
<td>17</td>
<td>0</td>
<td>0.0</td>
<td>1.74</td>
<td>0.0</td>
</tr>
<tr>
<td>rasm@0.0.0</td>
<td>118</td>
<td>3</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0.0</td>
<td>1.61</td>
<td>0.0</td>
</tr>
<tr>
<td>mbcd@2.0.0</td>
<td>194</td>
<td>4</td>
<td>0</td>
<td>20</td>
<td>1</td>
<td>0.0</td>
<td>108.80</td>
<td>0.0</td>
</tr>
<tr>
<td>sfe@2.0.0</td>
<td>194</td>
<td>4</td>
<td>0</td>
<td>21</td>
<td>0</td>
<td>0.0</td>
<td>20.59</td>
<td>1.1</td>
</tr>
<tr>
<td>natm@2.0.0</td>
<td>194</td>
<td>5</td>
<td>0</td>
<td>21</td>
<td>1</td>
<td>0.0</td>
<td>2.60</td>
<td>0.1</td>
</tr>
<tr>
<td>arpm@2.0.0</td>
<td>194</td>
<td>5</td>
<td>0</td>
<td>23</td>
<td>1</td>
<td>0.0</td>
<td>21.47</td>
<td>0.0</td>
</tr>
<tr>
<td>npmg@2.0.0</td>
<td>194</td>
<td>5</td>
<td>0</td>
<td>23</td>
<td>1</td>
<td>0.0</td>
<td>21.05</td>
<td>1.5</td>
</tr>
<tr>
<td>sptx@2.0.0</td>
<td>194</td>
<td>4</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>0.0</td>
<td>6.42</td>
<td>0.0</td>
</tr>
</tbody>
</table>
```
show task standby

The `show task standby` command displays overview statistics for all application tasks on all standby cores. For example:

```
ACMEPACKET# show task standby

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Per</th>
<th>Msgs</th>
<th>Trans</th>
<th>Timers</th>
<th>TOQs</th>
<th>PerCPU</th>
<th>Total-CPU</th>
<th>MaxCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>logman@1.0.0</td>
<td>136</td>
<td>5</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0.0</td>
<td>0.65</td>
<td>0.0</td>
</tr>
<tr>
<td>rasm@1.0.0</td>
<td>136</td>
<td>3</td>
<td>0</td>
<td>19</td>
<td>1</td>
<td>0.0</td>
<td>12.92</td>
<td>0.0</td>
</tr>
<tr>
<td>snmpd@1.0.0</td>
<td>136</td>
<td>3</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0.0</td>
<td>0.10</td>
<td>0.0</td>
</tr>
<tr>
<td>sshd@1.0.0</td>
<td>136</td>
<td>3</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0.0</td>
<td>0.08</td>
<td>0.0</td>
</tr>
<tr>
<td>auth@1.0.0</td>
<td>136</td>
<td>3</td>
<td>0</td>
<td>22</td>
<td>1</td>
<td>0.0</td>
<td>12.80</td>
<td>0.0</td>
</tr>
<tr>
<td>sfeg1.0.0</td>
<td>136</td>
<td>4</td>
<td>0</td>
<td>18</td>
<td>1</td>
<td>0.0</td>
<td>17.25</td>
<td>0.0</td>
</tr>
<tr>
<td>sfe@1.0.1</td>
<td>133</td>
<td>4</td>
<td>0</td>
<td>5018</td>
<td>1</td>
<td>0.0</td>
<td>15.07</td>
<td>0.3</td>
</tr>
<tr>
<td>dnsres@1.0.1</td>
<td>133</td>
<td>4</td>
<td>0</td>
<td>17</td>
<td>0</td>
<td>0.0</td>
<td>0.14</td>
<td>0.0</td>
</tr>
<tr>
<td>soapd@1.0.0</td>
<td>133</td>
<td>4</td>
<td>0</td>
<td>19</td>
<td>1</td>
<td>0.0</td>
<td>2.93</td>
<td>0.0</td>
</tr>
<tr>
<td>sipt@1.1.0</td>
<td>197</td>
<td>5</td>
<td>0</td>
<td>16</td>
<td>1</td>
<td>0.0</td>
<td>3.11</td>
<td>0.0</td>
</tr>
<tr>
<td>sipc@1.1.1</td>
<td>195</td>
<td>3</td>
<td>0</td>
<td>15</td>
<td>1</td>
<td>0.0</td>
<td>5.44</td>
<td>0.0</td>
</tr>
<tr>
<td>sipt@1.2.0</td>
<td>198</td>
<td>5</td>
<td>0</td>
<td>16</td>
<td>1</td>
<td>0.0</td>
<td>3.10</td>
<td>0.0</td>
</tr>
<tr>
<td>sipc@1.2.1</td>
<td>195</td>
<td>3</td>
<td>0</td>
<td>15</td>
<td>1</td>
<td>0.0</td>
<td>5.44</td>
<td>0.0</td>
</tr>
<tr>
<td>sipls@1.3.0</td>
<td>198</td>
<td>3</td>
<td>0</td>
<td>16</td>
<td>2</td>
<td>0.0</td>
<td>3.60</td>
<td>0.0</td>
</tr>
<tr>
<td>sipc@1.3.1</td>
<td>195</td>
<td>3</td>
<td>0</td>
<td>15</td>
<td>1</td>
<td>0.0</td>
<td>5.48</td>
<td>0.0</td>
</tr>
<tr>
<td>natm@2.0.0</td>
<td>141</td>
<td>5</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>0.0</td>
<td>0.13</td>
<td>0.0</td>
</tr>
<tr>
<td>arpm@2.0.0</td>
<td>141</td>
<td>5</td>
<td>0</td>
<td>19</td>
<td>1</td>
<td>0.0</td>
<td>11.44</td>
<td>0.0</td>
</tr>
<tr>
<td>npm@2.0.0</td>
<td>141</td>
<td>4</td>
<td>0</td>
<td>18</td>
<td>1</td>
<td>0.0</td>
<td>5.15</td>
<td>2.3</td>
</tr>
<tr>
<td>npcli@2.0.0</td>
<td>141</td>
<td>3</td>
<td>0</td>
<td>18</td>
<td>1</td>
<td>0.0</td>
<td>5.40</td>
<td>0.0</td>
</tr>
<tr>
<td>mbcd@2.0.1</td>
<td>138</td>
<td>4</td>
<td>0</td>
<td>25</td>
<td>1</td>
<td>0.0</td>
<td>6.73</td>
<td>0.2</td>
</tr>
<tr>
<td>xserv@6.0.0</td>
<td>144</td>
<td>4</td>
<td>0</td>
<td>24</td>
<td>2</td>
<td>0.2</td>
<td>97.85</td>
<td>0.2</td>
</tr>
</tbody>
</table>
```

Individual Task Statistics

The `show task` command is used to display statistics about a supplied task. This command only accepts a pre-defined set of tasks as arguments.

The `show task` command usage is as follows:

```
ACMEPACKET# show task <task>
```

where task is:

```
<name>@<card>.<cpu>.<core>
```

You may use wildcards anywhere in the task argument. For example:

```
ACMEPACKET# show task sip*@*
```

The above command returns all tasks that begin with sip at all slot/cpu/core locations on the Net-Net system.

In each task’s show command output, the following statistics are displayed:

- Services—Number of times the process performs actions for different services
- Messages—Number of messages the process created and processed
- Alloc Buffers—
- Free Buffers—
- Transactions—Number of client or server transactions, both sending and receiving, for a particular process
- Timed Objects—Number of objects with timers associated with them
• TOQ Entries—Number of active timers (in the Timed Objects) placed in the timeout queue
• Operations—Number of times the process is prompted (or polled) to perform an action
• Messages Received—Number of messages received by the task
• Messages Sent—Number of messages sent by the task
• Partial Message—Number of partial messages
• Part Msg Expired—Number of times the process set a timer for a partial message and that timer expired, prompting the process to make a decision about whether to process the partial message or drop it
• Part Msg Dropped—Number of times the process set a timer for a partial message and that timer expired, prompting the process to drop the partial message
• Timed Events—Number of times a TOQ Entry timed out
• Alarms—Number of alarms the process sent
• System Logs—Number of times the process wrote to the system log
• Process Logs—Number of times the process wrote to the process log
• Remote Logs—
• Load Rate—This statistic shows an approximation (in a percentage) of time that the process has been processing

show task acli

The ACLI task statistics are displayed as follows:

```
ACMEPACKET# show task acli
09:48:56-130 (acli@0.0.0) ID=10000

Task Status   Recent   Lifetime

<table>
<thead>
<tr>
<th>Services</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>5</td>
<td>5</td>
<td>70</td>
<td>4439</td>
<td>241</td>
<td>6</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
<td>0</td>
<td>48</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>0</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>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>17</td>
<td>17</td>
<td>0</td>
<td>17</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU Slices</td>
<td>1</td>
<td>1</td>
<td>92</td>
<td>2516</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
<td>28</td>
<td>2085</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>34</td>
<td>2219</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>34</td>
<td>2223</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</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>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Max Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>8</td>
<td>113</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>4.08</td>
<td>0.1%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ACMESYSTEM#
```
**show task arpm**

The ARP Manager (ARPM) task statistics are displayed as follows:

```
ACMEPACKET# show task arpm
12:20:16-154 (arpm@2.0.0) ID=d46f4000

Task Status       Active High Total PerMax    High
Services          16   16   0    16    16    16
Messages          5    5    308   62568   198    6
Alloc Buffers     48   48    0    48    48    48
Free Buffers      0    0    0    0    0    0
Transactions      0    1    153  31277    99    2
Timed Objects     19   20    153  31296    99   21
TOQ Entries       1    1    306  62552   198    1
Operations        -    -    308  62857   199
Messages Received -    -    154  31284    99
Messages Sent     -    -    153  31286    99
Partial Message   -    -    0    0    0    0
Part Msg Expired  -    -    0    0    0    0
Part Msg Dropped  -    -    0    0    0    0
Timed Events      -    -    153  31274    99
Alarms            -    -    0    0    0    0
System Logs       -    -    0    1    1
Process Logs      -    -    4    709    73
Remote Logs       -    -    0    0    0
Load Rate         0.0% 13.02 0.0%
```

**show task auth**

The user authentication task statistics are displayed as follows:

```
ACMEPACKET# show task auth
12:20:49-120 (auth@0.0.0) ID=e23c11a0

Task Status       Active High Total PerMax    High
Services          18   18    0    18    17    18
Messages          1175 1175   260  65250   235  1175
Alloc Buffers     48   48    0    48    48    48
Free Buffers      0    0    0    0    0    0
Transactions      32   32   119  31506   106   38
Timed Objects     54   54   119  31529   107   60
TOQ Entries       34   34   128  32609   112   40
Operations        -    -   258  65364   212
Messages Received -    -   130  32624   117
Messages Sent     -    -   129  32628   120
Partial Message   -    -    0    0    0    0
Part Msg Expired  -    -    0    0    0    0
Part Msg Dropped  -    -    0    0    0    0
Timed Events      -    -   128  32575   107
Alarms            -    -    0    0    0    0
System Logs       -    -    0    3    2
Process Logs      -    -   226  57
Remote Logs       -    -    0    0    0
Load Rate         0.0% 13.02 0.0%
```

**show task broker**

The broker daemon (broker) task statistics are displayed as follows:

```
ACMEPACKET# show task broker0.0.0
```

Proprietary & Confidential
### show task cm

The card manager (CM) task statistics are displayed as follows:

**ACMEPACKET# show task cm@0.0.0**

```
12:21:34-165 (cm@0.0.0) ID=e1840610
```

<table>
<thead>
<tr>
<th>Task 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>16</td>
<td>16</td>
<td>0</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Messages</td>
<td>3</td>
<td>3</td>
<td>363</td>
<td>70275</td>
<td>235</td>
<td>3</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
<td>48</td>
<td>48</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>0</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>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>11</td>
<td>11</td>
<td>361</td>
<td>70248</td>
<td>239</td>
<td>11</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
<td>331</td>
<td>64210</td>
<td>216</td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>330</td>
<td>63864</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>32</td>
<td>64444</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
<td>32</td>
<td>6301</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>830</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>26.03</td>
<td>0.0%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### show task collect

The HDR collection task statistics are displayed as follows:

**ACMEPACKET# show task collect**

```
09:49:41-175 (collect@0.0.0) ID=e4e21f40
```

<table>
<thead>
<tr>
<th>Task 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>17</td>
<td>17</td>
<td>0</td>
<td>17</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Messages</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>48</td>
<td>33</td>
<td>3</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>49</td>
<td>49</td>
<td>49</td>
<td>49</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>0</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>
<td>0</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>18</td>
<td>18</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>33</td>
<td>33</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
<td>77</td>
<td>16829</td>
<td>583</td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>64</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>32</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>75</td>
<td>16630</td>
<td>602</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>2.90</td>
<td>0.1%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### show task dnsres

The DNS Resolution Server (DNSRES) task statistics are displayed as follows:

```
ACMEPACKET# show task dnsres
12:21:56-180 (dnsres@0.0.1) ID=d431a180
```

<table>
<thead>
<tr>
<th>Task Status</th>
<th>---- Recent ----</th>
<th>---------</th>
<th>---- Lifetime ---------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>High</td>
<td>Total</td>
<td>Total</td>
</tr>
<tr>
<td>Services</td>
<td>16</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>Messages</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
<td>0</td>
</tr>
<tr>
<td>Free Buffers</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>19</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>CPU Slices</td>
<td>37</td>
<td>3</td>
<td>2193</td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>Max Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>0.24%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

### show task ftpdalg

The FTP ALG task statistics are displayed as follows:

```
ACMEPACKET# show task ftpdalg
```

<table>
<thead>
<tr>
<th>Task Status</th>
<th>---- Recent ----</th>
<th>---------</th>
<th>---- Lifetime ---------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>High</td>
<td>Total</td>
<td>Total</td>
</tr>
<tr>
<td>Services</td>
<td>16</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>Messages</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
<td>0</td>
</tr>
<tr>
<td>Free Buffers</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>17</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>0.14%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
show task h323GkGw

The H.323 Gatekeeper/Gateway task statistics are displayed as follows:

show task h323RasGk

The H.323 RAS Gatekeeper task statistics are displayed as follows:
show task h323RasGk

ACMEPACKET# show task h323RasGk
14:39:23-168 (h323RasGk@0.4.1) | ID=d54b0c90
Task Status          Recent Lifetime
Active    High   Total   PerMax    High
Services      13    13    0      13    13    13
Messages      20    20    86     173784  66    24
Alloc Buffers 39    39    0      39    39    39
Free Buffers  39    39    0      39    39    39
Transactions  8     8     42     86860   25    11
Timed Objects 24    24    42     86876   25    27
TOQ Entries   9     9     75     156790  45    12
CPU Slices    -     -     113    240801  75
Operations    1     2    118    243504  77    2
Messages Received -   -   43     86892   33
Messages Sent  -   -   42     86891   33
Partial Message -   -   0      0      0
Part Msg Expired -   -   0      0      0
Part Msg Dropped -   -   0      0      0
Buffer Overflow -   -   0      0      0
Timed Events   0     1    75     156781  45    2
Max Timed Events 0    0    0      0      0
Operations     -   -   54     7291    341
Messages Received -   -   20     575     331
Messages Sent  -   -   53     6719    103
Partial Message -   -   0      0      0
Part Msg Expired -   -   0      0      0
Part Msg Dropped -   -   0      0      0
Timed Events   -   -   34     6403    20
Alarms         -   -   0      0      0
System Logs    -   -   0      3      2
Process Logs   -   -   4      893    159
Remote Logs    -   -   0      0      0
Load Rate      0.0%  37.53  0.0%

show task lcm

The local core manager (LCM) task statistics are displayed as follows:

ACMEPACKET# show task lcm@0.0.0
12:23:20-171 (lcm@0.0.0) | ID=e0709050
Task Status          Recent Lifetime
Active    High   Total   PerMax    High
Services      17    17    0      17    17    17
Messages      3     3    55     6989    345    3
Alloc Buffers 48    48    0      48    48    48
Free Buffers  0     0    0      0      0
Transactions  0     0    0      0      0
Timed Objects 34    34    0      35    35    34
TOQ Entries   1     1    34     6424    33    3
Operations    -   -   54     7291    341
Messages Received -   -   20     575     331
Messages Sent  -   -   53     6719    103
Partial Message -   -   0      0
Part Msg Expired -   -   0      0
Part Msg Dropped -   -   0      0
Timed Events   -   -   34     6403    20
Alarms         -   -   0      0
System Logs    -   -   0      3
Process Logs   -   -   4      893    159
Remote Logs    -   -   0      0
Load Rate      0.0%  4.99  2.1%

show task lem

The local element manager (LEM) task statistics are displayed as follows:
ACMEPACKET# show task lem@0.0.0
12:23:44.195 {lem@0.0.0} ID=e12da1b0

Task Status ---- Recent ---- -------- Lifetime --------

Active High Total Total PerMax High

Services 16 16 0 16 16 16
Messages 3 3 2 42 37 3
Alloc Buffers 48 48 0 48 48 48
Free Buffers 0 0 0 0 0 0
Transactions 0 0 0 0 0 0
Timed Objects 17 17 0 17 17 17
TOQ Entries 0 0 0 38 38 1
Operations - - 2 361 37
Messages Received - - 1 3 2
Messages Sent - - 0 38 37
Partial Message - - 0 0 0
Part Msg Expired - - 0 0 0
Part Msg Dropped - - 0 0 0
Timed Events - - 0 37 37
Alarms - - 0 0 0
System Logs - - 6 1781 237
Process Logs - - 5 1465 238
Remote Logs - - 0 0 0
Load Rate 0.0% 0.12 0.0%

show task logman

The Acmelog log manager (logman) task statistics are displayed as follows:

ACMEPACKET# show task logman@0.0.0
12:24:08.119 {logman@0.0.0} ID=e1657e30

Task Status ---- Recent ---- -------- Lifetime --------

Active High Total Total PerMax High

Services 17 17 0 18 18 18
Messages 6 6 10 2283 129 7
Alloc Buffers 48 48 0 48 48 48
Free Buffers 0 0 0 0 0 0
Transactions 0 0 0 0 0 0
Timed Objects 18 18 0 19 19 19
TOQ Entries 0 0 0 0 0 0
Operations - - 6 1781 237
Messages Received - - 5 1465 238
Messages Sent - - 0 8 4
Partial Message - - 0 0 0
Part Msg Expired - - 0 0 0
Part Msg Dropped - - 0 0 0
Timed Events - - 0 0 0
Alarms - - 0 0 0
System Logs - - 4 702 51
Load Rate 0.0% 0.76 0.1%

show task mbcd

The middlebox control daemon (MBCD) task statistics are displayed as follows:

ACMEPACKET# show task mbcd
12:24:22.198 {mbcd@2.0.1} ID=d3dc14c0
show task msfe

The MSFE task statistics are displayed as follows:

```
ACMEPACKET# show task msfe
12:24:37-148 (sfe@0.0.0) ID=e20a7900

Task Status

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Messages</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Free Buffers</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>25</td>
<td>25</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>6.49</td>
</tr>
</tbody>
</table>
```

show task natm

The NAT manager (NATM) task statistics are displayed as follows:

```
ACMEPACKET# show task natm
12:24:37-148 (natm@2.0.0) ID=d53298c0

Task Status

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>High</td>
</tr>
<tr>
<td>Services</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Messages</td>
<td>66</td>
<td>66</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>49</td>
<td>50</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>17.46</td>
</tr>
</tbody>
</table>
```
**SYSTEM MANAGEMENT**

| Services  | 16 | 16 | 0 | 16 | 16 | 16 |
| Messages  | 5  | 5  | 2 | 21 | 19 | 6  |
| Alloc Buffers | 48 | 48 | 0 | 48 | 48 | 48 |
| Free Buffers | 0  | 0  | 0 | 0  | 0  | 0  |
| Transactions | 0  | 0  | 0 | 0  | 0  | 0  |
| Timed Objects | 19 | 19 | 0 | 19 | 19 | 19 |
| TOQ Entries | 0  | 0  | 1 | 1  | 1  | 1  |
| Operations  | -  | -  | 2 | 326| 326| 5  |
| Messages Received | - | - | 1 | 11 | 10 |
| Messages Sent | - | - | 12 | 12 |
| Partial Message | - | - | 0 | 0  | 0  | 0  |
| Part Msg Expired | - | - | 0 | 0  | 0  | 0  |
| Part Msg Dropped | - | - | 0 | 0  | 0  | 0  |
| Timed Events  | -  | -  | 0 | 0  | 0  | 0  |
| Alarms      | -  | -  | 0 | 0  | 0  | 0  |
| System Logs | -  | -  | 0 | 0  | 0  | 0  |
| Process Logs | -  | -  | 4 | 704| 62 |
| Remote Logs | -  | -  | 0 | 0  | 0  | 0  |
| Load Rate    | 0.0%| 0.13%| 0.0%|

**Note:** natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

**show task npm**

The NPM task statistics are displayed as follows:

```
ACMEPACKET# show task npm
14:39:40-100 (npm@2.0.0) ID=c4950010
Task Status  Recent     Lifetime
Services     16 | 0 | 16 | 16 | 16 | 16 |
Messages     4  | 4  | 2  | 187| 67 | 5  |
Alloc Buffers 48 | 48 | 0  | 48 | 48 | 48 |
Free Buffers  0  | 0  | 0  | 0  | 0  | 0  |
Transactions  0  | 0  | 0  | 0  | 0  | 0  |
Timed Objects 18 | 18 | 0  | 18 | 18 | 18 |
TOQ Entries   1  | 1  | 100| 348826| 125| 2  |
CPU Slices    -  | -  | 102| 352279| 105|
Operations    1  | 1  | 101| 348810| 105| 3  |
Messages Received - - | 1  | 0  | 71 | 28 |
Messages Sent  - - | 0  | 0  | 117| 46 |
Partial Message - - | 0  | 0  | 0  | 0  |
Part Msg Expired - - | 0  | 0  | 0  | 0  |
Part Msg Dropped - - | 0  | 0  | 0  | 0  |
Buffer Overflow - - | 0  | 0  | 0  | 0  |
Timed Events   0  | 1  | 100| 348823| 125| 2  |
Max Timed Events 0  | 0  | 0  | 0  | 0  | 0  |
Alarms        - - | 0  | 0  | 0  | 0  |
System Logs   - - | 0  | 3  | 3  | 3  |
Process Logs  - - | 2  | 1264| 57 |
Remote Logs   - - | 0  | 0  | 0  | 0  |
Load Rate     0.0%| 31.88%| 2.3%|
```

**show task ntpd**

The NTP task statistics are displayed as follows:
### show task ntpd

```plaintext
ACMEPACKET# show task ntpd
09:51:14-169 (ntpd@0.0.0) ID=c767e310
Task Status      ---- Recent ---- -------- Lifetime --------

<table>
<thead>
<tr>
<th>Services</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>17</td>
<td>17</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>Messages</td>
<td>4</td>
<td>4</td>
<td>19</td>
<td>1462</td>
<td>48</td>
<td>4</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>50</td>
<td>50</td>
<td>0</td>
<td>52</td>
<td>52</td>
<td>52</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>2</td>
<td>2</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>19</td>
<td>19</td>
<td>0</td>
<td>21</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>1</td>
<td>1</td>
<td>169</td>
<td>10507</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>CPU Slices</td>
<td>-</td>
<td>-</td>
<td>186</td>
<td>11831</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>1</td>
<td>2</td>
<td>187</td>
<td>11964</td>
<td>143</td>
<td>9</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>18</td>
<td>1459</td>
<td>47</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>0</td>
<td>1</td>
<td>169</td>
<td>10506</td>
<td>100</td>
<td>2</td>
</tr>
<tr>
<td>Max Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>82</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>-</td>
<td></td>
<td></td>
<td>0.0%</td>
<td>1.92</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
```

### show task rasm

The Radius Accounting System Manager (RASM) task statistics are displayed as follows:

```plaintext
ACMEPACKET# show task rasm
12:42:13-104 (rasm@0.0.0) ID=e2a73160
Task Status      ---- Recent ---- -------- Lifetime --------

<table>
<thead>
<tr>
<th>Services</th>
<th>Active</th>
<th>High</th>
<th>Total</th>
<th>Total</th>
<th>PerMax</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16</td>
<td>16</td>
<td>0</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Messages</td>
<td>65</td>
<td>65</td>
<td>206</td>
<td>65559</td>
<td>207</td>
<td>69</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>48</td>
<td>48</td>
<td>0</td>
<td>48</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Free Buffers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transactions</td>
<td>31</td>
<td>32</td>
<td>102</td>
<td>32761</td>
<td>101</td>
<td>34</td>
</tr>
<tr>
<td>Timed Objects</td>
<td>50</td>
<td>51</td>
<td>102</td>
<td>32780</td>
<td>101</td>
<td>53</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>31</td>
<td>32</td>
<td>102</td>
<td>32787</td>
<td>101</td>
<td>34</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
<td>207</td>
<td>65815</td>
<td>199</td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>103</td>
<td>32767</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>102</td>
<td>32792</td>
<td>103</td>
<td></td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
<td>103</td>
<td>32755</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>Max Timed Events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>740</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Load Rate</td>
<td>-</td>
<td></td>
<td></td>
<td>0.0%</td>
<td>13.06</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
```

### show task secured

The Security Daemon task statistics are displayed as follows:

```plaintext
ACMEPACKET# show task secured
```

Proprietary & Confidential
show task secured

The system element manager (SEM) task statistics are displayed as follows:

show task sem

The socket front end (SFE) task statistics are displayed as follows:
### show task sfe

```
ACMEPACKET# show task sfe
12:42:38-122 (sfe@0.0.1) ID=cb0ce030
Task Status  ---- Recent ---- -------- Lifetime --------
                 Active   High   Total   Total  PerMax    High
Services         16       16       0      16     16     16
Messages        68       68     244     65630   200    76
Alloc Buffers    48       48       0      48     48     48
Free Buffers     0        0        0       0     0     0
Transactions     32       32     121     32879   99    37
Timed Objects    5050     5050     121    37807   5030   5055
TOQ Entries      32       32     121     32829   99    37
Operations       -        -     244     65886   199
Messages Received -       -     122     32798  100
Messages Sent    -        -     121     32833  100
Partial Message  -        -       0       0     0     0
Part Msg Expired -        -       0       0     0     0
Part Msg Dropped -        -       0       0     0     0
Timed Events     -        -     121     32796  99
Alarms           -        -       0       0     0     0
System Logs      -        -       0       3     3
Process Logs     -        -       0       182   72
Remote Logs      -        -       0       0     0     0
Load Rate        0.0%     16.22    0.3%
```

### show task sipc

The SIP Core (SIPC) task statistics are displayed as follows:

```
ACMEPACKET# show task sipc
12:42:56-105 (sipc@0.1.1) ID=cfcff470
Task Status  ---- Recent ---- -------- Lifetime --------
                 Active   High   Total   Total  PerMax    High
Services         13       13       0      13     13     13
Messages        33       33     104     32843  191    39
Alloc Buffers    39       39       0      39     39    39
Free Buffers     0        0        0       0     0     0
Transactions     15       16      51     16347   50    19
Timed Objects    31       32      51     16366   50    35
TOQ Entries      15       16      51     16369   50    19
Operations       -        -     114     35854  109
Messages Received -       -     52      16411   85
Messages Sent    -        -     51      16432  107
Partial Message  -        -       0       0     0     0
Part Msg Expired -        -       0       0     0     0
Part Msg Dropped -        -       0       0     0     0
Timed Events     -        -     52      16353  50
Alarms           -        -       0       0     0     0
System Logs      -        -       0       1     1
Process Logs     -        -       8      1512  176
Remote Logs      -        -       0       0     0     0
Load Rate        0.0%     5.79     0.0%
```

### show task sipls

The SIP Location Server (SIPLS) task statistics are displayed as follows:

```
ACMEPACKET# show task sipls
12:43:10-122 (sipls@0.3.0) ID=c62bd010
```

*Proprietary & Confidential*
### show task sipt

The SIP Transport (SIPT) task statistics are displayed as follows:

```
ACMEPACKET# show task sipt
12:43:22-133 (sipt@0.1.0) ID=c631d950
Task Status       ---- Recent ---- -------- Lifetime --------
Active   High   Total      Total  PerMax    High
Services       14      14       0         14      14      14
Messages       21      21       0         21      21      21
Alloc Buffers  39      39       0         39      39      39
Free Buffers   0       0        0         0       0       0
Transactions   8       8      33       8273      25      11
Timed Objects  25      25      33       8293      33      28
TOQ Entries    8       8      54      14931      54      54
Operations     -       -      79      19819      61
Messages Received -      - 34    8334        72
Messages Sent  -       - 33    8357        96
Partial Message -      -    0    0          0
Part Msg Expired -      -    0    0          0
Part Msg Dropped -      -    0    0          0
Timed Events   -       - 33    8288        27
Alarms         -       -    0    0          0
System Logs    -       -    0    1          1
Process Logs   -       -    8    1527       191
Remote Logs    -       -    0    0          0
Load Rate      0.0%    3.78     0.0%
```

### show task sm

The system manager (SM) task statistics are displayed as follows:

```
ACMEPACKET# show task sm@0.0.0
12:43:38-189 (sm@0.0.0) ID=e19fead0
Task Status       ---- Recent ---- -------- Lifetime --------
Active   High   Total      Total  PerMax    High
Services       13      13       0         13      13      13
Messages       19      19       62  16713     181      23
Alloc Buffers  39      39       0         39      39      39
Free Buffers   0       0        0         0       0       0
Transactions   8       8      30       8277      25      11
Timed Objects  25      25      30       8297      33      28
TOQ Entries    9       9      54      14941      56      12
Operations     -       -      95      26191      80
Messages Received -      - 31    8347        81
Messages Sent  -       - 30    8368       103
Partial Message -      -    0    0          0
Part Msg Expired -      -    0    0          0
Part Msg Dropped -      -    0    0          0
Timed Events   -       - 54    14931       46
Alarms         -       -    0    0          0
System Logs    -       -    0    1          1
Process Logs   -       -    8    1527       191
Remote Logs    -       -    0    0          0
Load Rate      0.0%    3.28     0.0%
```
show task snmpd

The SNMP daemon task statistics are displayed as follows:

```
ACMEPACKET# show task snmpd
12:43:48-199 (snmpd@0.0.0) ID=e20fb6e0
Task Status

<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>17</td>
<td>17</td>
<td>0</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Messages</td>
<td>4</td>
<td>4</td>
<td>321</td>
<td>49279</td>
<td>827</td>
</tr>
<tr>
<td>Alloc Buffers</td>
<td>49</td>
<td>49</td>
<td>0</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td>Free Buffers</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>49</td>
<td>49</td>
<td>0</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td>TOQ Entries</td>
<td>8</td>
<td>8</td>
<td>269</td>
<td>47617</td>
<td>159</td>
</tr>
<tr>
<td>Operations</td>
<td>-</td>
<td>-</td>
<td>296</td>
<td>48595</td>
<td>405</td>
</tr>
<tr>
<td>Messages Received</td>
<td>-</td>
<td>-</td>
<td>289</td>
<td>47242</td>
<td>393</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>-</td>
<td>-</td>
<td>74</td>
<td>9814</td>
<td>444</td>
</tr>
<tr>
<td>Partial Message</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Expired</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Part Msg Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timed Events</td>
<td>-</td>
<td>-</td>
<td>1093</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Process Logs</td>
<td>-</td>
<td>-</td>
<td>1663</td>
<td>627</td>
<td></td>
</tr>
<tr>
<td>Remote Logs</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Load Rate</td>
<td>0.0%</td>
<td>13.00</td>
<td>0.3%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

show task soapd

The SOAP daemon task statistics are displayed as follows:

```
ACMEPACKET# show task soapd
12:44:05-109 (soapd@0.0.1) ID=d431a9e0
Task Status

<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>16</td>
<td>16</td>
<td>0</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Messages</td>
<td>20</td>
<td>20</td>
<td>56</td>
<td>16595</td>
<td>50</td>
</tr>
</tbody>
</table>
```
show task sshd

The SSH daemon task statistics are displayed as follows:

```
ACMEPACKET# show task sshd
12:44:16-127 (sshd@0.0.0) ID=e1e82b80
Task Status         ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
Services                  17      17       0         17      17      17
Messages                   3       3       2          8       3       3
Alloc Buffers             48      48       0         48      48      48
Free Buffers               0       0       0          0       0       0
Transactions               0       0       0          0       0       0
Timed Objects             18      18       0         18      18      18
TOQ Entries                0       0       0          0       0       0
Operations                 -       -       2        339       3
Messages Received          -       -       1          4       2
Messages Sent              -       -       0          4       2
Partial Message            -       -       0          0       0
Part Msg Expired           -       -       0          0       0
Part Msg Dropped           -       -       0          0       0
Timed Events               -       -       0          0       0
Alarms                     -       -       0          0       0
System Logs                -       -       0          1       1
Process Logs               -       -       0        159      43
Remote Logs                -       -       0          0       0
Load Rate                                0.0%      0.08     0.0%
```

show task xserv

The Transcoder Server task statistics are displayed as follows:

```
ACMEPACKET# show task xserv
12:45:13-154 (xserv@4.0.0) ID=d4185120
Task Status         ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
Services                  21      21       0         21      21      21
Messages                 299     299    1466    317217     949     301
Alloc Buffers            60       60       0         60      60      60
Free Buffers             0        0        0          0       0       0
```
### Chassis Management Application Statistics

The show commands described in this section relate to system-level tasks and processes on the Net-Net system. These tasks generally do not have any direct involvement with passing traffic or other media and signaling applications.

### Socket Front End (SFE)

The Socket Front End (SFE) manages TCP streams and connectionless UDP sessions within the Net-Net 9200 signaling plane. It is used by signaling components to communicate bi-directionally with addressable entities accessible via the external network. You can view SFE statistics with the `show sfe` command.

```
ACMEPACKET# show sfe [summary | pending | clients | socket]
```

#### show sfe summary

The `show sfe summary` command is displayed as follows:

```
ACMEPACKET# show sfe summary
************************************************
SFE at 169.254.160.1:8013
************************************************
Handles                     2(free:249998)
Host Path Transmit Port     169.254.177.0:8016
Server State                Active
12:49:31-135
Summary                         ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
UDP Sockets                    2       2       0          2       2       2
TCP Listen Sockets             0       0       0          0       0       0
TCP Inbound Connections        0       0       0          0       0       0
TCP Outbound Connections       0       0       0          0       0       0
Free TCP Timers             5000    5000       0       5000    5000    5000
Alloc TCP Timers             0       0       0          0       0       0
Internal Errors                -       -       0          0       0
RDP Send Errors                -       -       0          0       0
No Socket For Net Packet      -       -       0          0       0
Bad Packet From Network       -       -       0          0       0
Send to Network Failed        -       -       0          0       0
Rcvd Fragments                -       -       0          0       0
```
show sfe pending

The show sfe pending command displays pending socket open requests.

```
ACMEPACKET# show sfe pending

<ENTER>  no further known parameters
```

show sfe clients

The show sfe clients command displays the SFE’s current clients (as tasks) and the number of sockets each client has opened to the SFE. For example:

```
ACMEPACKET# show sfe clients

------------------- ----------
Client              SockCount
------------------- ----------
  dnsres@0.0.1        2
  sipt@0.1.0          2
------------------- ----------
Total Active Clients: 2
```

show sfe load

The show sfe load command displays the SFE’s current load as well as its load limit. For example:

```
ACMEPACKET# show sfe load

sfe@0.1.0: Load is 0.1; Limit is 95
```

show sfe sockets

The show sfe sockets command displays the SFE’s open sockets in detail. This display includes the task, protocol, IP address and port, and number of messages received, sent, and errors. In addition, details about the recorded errors are listed. For example:

```
ACMEPACKET# show sfe sockets

Server State                Active
------ ------------------------------------- ---------- ---------- ---
Handle Socket                                          MsgRcvd    MsgSent    Err
------ ------------------------------------- ---------- ---------- ---
  1      sipt@0.2.0 UDP[0:3/0]172.16.0.77:5060           0          0          0
  2      sipt@0.1.0 UDP[0:0/0]192.168.0.77:5060          0          0          0

12:50:48-112
Summary                         ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
UDP Sockets                    2       2       0          2       2       2
TCP Listen Sockets             0       0       0          0       0       0
TCP Inbound Connections        0       0       0          0       0       0
TCP Outbound Connections       0       0       0          0       0       0
Free TCP Timers                5000    5000       0      5000    5000    5000
Alloc TCP Timers               0       0       0          0       0       0
Internal Errors                -       -       0          0       0       0
```
Management Socket Front End (MSFE)

The Management Socket Front End (SFE) manages TCP streams and connectionless UDP sessions within the Net-Net 9200 management plane. It is used by components to communicate bi-directionally with addressable entities accessible via the external network. You can view MSFE statistics with the show msfe command.

```
ACMEPACKET# show msfe [summary | pending | clients | sockets]
```

**show msfe summary**

The `show msfe summary` command is displayed as follows:

```
ACMEPACKET# show msfe summary
************************************************
msFE at 169.254.160.0:8037
************************************************
Handles                     0(free:1000)
Management Utility Address  172.30.92.92
Management Virtual Address  172.30.92.96
Server State                Active

12:51:45-176
Summary                         ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
UDP Sockets                    0       0       0          0       0       0
TCP Listen Sockets             0       0       0          0       0       0
TCP Inbound Connections        0       0       0          0       0       0
TCP Outbound Connections       0       0       0          0       0       0
Free TCP Timers                0       0       0          0       0       0
Alloc TCP Timers               0       0       0          0       0       0
Internal Errors                -       -       0          0       0       0
RDP Send Errors                -       -       0          0       0       0
No Socket For Net Packet       -       -       0          0       0       0
Bad Packet From Network        -       -       0          0       0       0
Send to Network Failed         -       -       0          0       0       0
Rcvd Fragments                 -       -       0          0       0       0
Rcvd Fragment Errors           -       -       0          0       0       0
Sent Fragments                 -       -       0          0       0       0
Sent Fragment Errors           -       -       0          0       0       0

Total Active Clients        0
```

**show msfe pending**

The `show msfe pending` command displays pending socket open requests.

**show msfe clients**

The `show msfe clients` command displays the MSFE’s current clients (as tasks) and the number of sockets each client has opened to the MSFE. For example:
**show msfe clients**

```
ACMEPACKET# show msfe clients
Client          SockCount
----------------- ----------
Total Active Clients 0
```

**show msfe load**

The `show msfe load` command displays the MSFE’s current load as well as its load limit. For example:

```
ACMEPACKET# show msfe load
sfe@0.0.0: Load is 2.6; Limit is 80
```

**show msfe sockets**

The `show msfe sockets` command displays the MSFE’s open sockets in detail. This display includes the task, protocol, IP address and port, and number of messages received, sent, and errors. In addition, details about the recorded errors are listed. For example:

```
ACME_SYSTEM# show msfe sockets
Server State          Active
------------------------
Handle Socket          MsgRcvd MsgSent Err
------------------------
09:58:53-127
Summary               Recent Lifetime
UDP Sockets           0 0 0 0 0 0
TCP Listen Sockets    0 0 0 0 0 0
TCP Inbound Connections 0 0 0 0 0 0
TCP Outbound Connections 0 0 0 0 0 0
Free TCP Timers       0 0 0 0 0 0
Alloc TCP Timers      0 0 0 0 0 0
Internal Errors       - - 0 0 0 0
RDP Send Errors       - - 0 0 0 0
No Socket For Net Packet - - 0 0 0 0
Bad Packet From Network - - 0 0 0 0
Send to Network Failed - - 0 0 0 0
Rcvd Fragments        - - 0 0 0 0
Rcvd Fragment Errors  - - 0 0 0 0
Sent Fragments        - - 0 0 0 0
Sent Fragment Errors  - - 0 0 0 0
```

**Acme Messaging Protocol (AMP)**

AMP is the messaging protocol used by all application tasks to communicate with each other. The Net-Net system provides counts of AMP message protocol types as sent or received by a supplied task. Counts are further delineated by Recent, Lifetime Total, and Lifetime Period Maximum. The Net-Net OS displays the appropriate AMP message counts for the task you specify.

Additionally, if one task makes synchronous communication with another task, the ACLI displays counts for the synchronous interprocess communication in the **ToServer** section of a specific task instance.
The `show amp` command usage is as follows:

```
ACMEPACKET# show amp <task>
```

where task is:

- `<name>@<card>.<cpu>.<core>`
- `acli`
- `arpm`
- `auth`

### show amp aclи

The `show amp aclи` command displays AMP message statistics for the ACLI. For example:

```
ACMEPACKET# show amp aclи
10:00:27-121 (aclи@0.0.0) | ID=10000

+-----------------+------------+------------+-------------+------------+------------+------------+
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>34</td>
<td>2395</td>
<td>120</td>
<td>33</td>
<td>2397</td>
<td>123</td>
</tr>
<tr>
<td>SNR</td>
<td>3</td>
<td>106</td>
<td>89</td>
<td>3</td>
<td>106</td>
<td>89</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>CLIP</td>
<td>4</td>
<td>20</td>
<td>4</td>
<td>3</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>CFG</td>
<td>2</td>
<td>43</td>
<td>16</td>
<td>2</td>
<td>43</td>
<td>16</td>
</tr>
<tr>
<td>AUTH</td>
<td>25</td>
<td>2223</td>
<td>24</td>
<td>25</td>
<td>2223</td>
<td>24</td>
</tr>
</tbody>
</table>

ToServer     5  159  107
Retries     0  0  0
Rejects      0  0  0
Timeouts    0  0  0
Stray        0  0  0
```

### show amp arpm

The `show amp arpm` command displays AMP message statistics for the ARP manager (ARPM). For example:

```
ACMEPACKET# show amp arpm@2.0.0
13:16:27-126 (arpm@2.0.0) | ID=d46f4000

+-----------------+------------+------------+-------------+------------+------------+------------+
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>126</td>
<td>34604</td>
<td>100</td>
<td>124</td>
<td>34606</td>
<td>100</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>ARP</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>125</td>
<td>34593</td>
<td>99</td>
<td>124</td>
<td>34593</td>
<td>99</td>
</tr>
</tbody>
</table>

ToServer     0  2  2
Retries     0  0  0
Rejects      0  0  0
Timeouts    0  0  0
Stray        0  0  0
```

### show amp auth

The `show amp auth` command displays AMP message statistics for the user authentication process. For example:
ACMEPACKET# show amp auth@0.0.0
13:16:45-176 (auth@0.0.0) | ID=e23c11a0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>180</td>
<td>36103</td>
<td>117</td>
<td>179</td>
<td>36109</td>
<td>120</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>AUTH</td>
<td>6</td>
<td>1287</td>
<td>9</td>
<td>6</td>
<td>1291</td>
<td>11</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>173</td>
<td>34807</td>
<td>106</td>
<td>173</td>
<td>34807</td>
<td>106</td>
</tr>
</tbody>
</table>

ToServer 0 2 1
Retries 0 0 0
Rejects 0 0 0
Timeouts 0 0 0
Stray 0 0 0

show amp broker

The `show amp broker` command displays AMP message statistics for the broker daemon. For example:

ACMEPACKET# show amp broker@0.0.1
13:16:59-183 (broker@0.0.1) | ID=d40a7e50

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>38</td>
<td>37</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

ToServer 0 1 1
Retries 0 0 0
Rejects 0 0 0
Timeouts 0 0 0
Stray 0 0 0

show amp cm

The `show amp cm` command displays AMP message statistics for the chassis manager (CM). For example:

ACMEPACKET# show amp cm@0.0.0
13:18:09-128 (cm@2.0.0) | ID=d3b191b0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>53</td>
<td>14043</td>
<td>42</td>
<td>26</td>
<td>7028</td>
<td>27</td>
</tr>
<tr>
<td>MAN</td>
<td>51</td>
<td>14036</td>
<td>40</td>
<td>25</td>
<td>7017</td>
<td>20</td>
</tr>
<tr>
<td>CLIP</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ARP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>ALARM</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
show amp collect

The `show amp collect` command displays AMP message statistics for the HDR collector application. For example:

```
ACME SYSTEM# show amp collect
10:02:09-123 (collect@0.0.0) ID=e4e21f40

-------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  -----
Total            1          5       3        0          5       2
MAN              0          3       3        0          3       2
CLIP             1          2       1        0          1       1
LOG              0          0       0        0          0       0
ToServer         0          0       0
Retries        0          0       0
 Rejects        0          0       0
Timeouts       0          0       0
Stray          0          0       0
```

show amp dnsres

The `show amp dnsres` command displays AMP message statistics for the DNS resolution server. For example:

```
ACMEPACKET# show amp dnsres@0.0.1
13:18:42-186 (dnsres@0.0.1) ID=d431a180

-------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  -----
Total            1         26      23        0         55      53
SNR              0          2       2        0          2       2
MAN              0          5       5        0          34      34
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          0       0
CFG              0         16      16        0         16      16
ToServer         0         21      21
Retries        0          0       0
 Rejects        0          0       0
Timeouts       0          0       0
Stray          0          0       0
```

show amp ftpdalg

The `show amp ftpdalg` command displays AMP message statistics for the FTP ALG server. For example:

```
ACMEPACKET# show amp ftpdalg@0.0.0
13:19:39-150 (ftpdalg@0.0.0) ID=e19fe510

-------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  -----
Total            1         21      17        0         30      30
MAN              0          2       2        0          2       2
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          0       0
CFG              0         16      16        0         16      16
ToServer         0         11      11
Retries        0          0       0
 Rejects        0          0       0
Timeouts       0          0       0
Stray          0          0       0
```

ToServer: 0  4  4
Retries: 0  0  0
Rejects: 0  0  0
Timeouts: 0  0  0
Stray: 0  0  0
show amp h323GkGw

The `show amp h323GkGw` command displays H.323 Gatekeeper/Gateway AMP statistics. For example:

```
ACMEPACKET# show amp h323GkGw
14:18:09-193 (h323GkGw@0.1.1) ID=d54af390

-------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
-------  ---------  ------   ------  ---------  -----
Total            1         16       8        0         15       7
SNR              0          3       3        0          3       3
MAN              0          3       2        0          2       1
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0          7       4        0          7       4

ToServer          0         10       6
Retries          0          0       0
Rejects          0          0       0
Timeouts         0          0       0
Stray            0          0       0
```

show amp h323RasGk

The `show amp h323RasGk` command displays H.323 RAS Gatekeeper AMP statistics. For example:

```
ACMEPACKET# show amp h323RasGk
14:21:09-175 (h323RasGk@0.4.1) ID=d54b0c90

-------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
-------  ---------  ------   ------  ---------  -----
Total           45      86608      30       44      86607      29
SNR              0          3       3        0          3       3
MAN              0          3       2        0          2       1
CLIP             2          7       4        1          6       4
LOG              0          0       0        0          1       1
CFG              0          7       4        0          7       4
REDUNDANCY      43      86588      25       43      86588      25

ToServer          0         10       6
Retries          0          0       0
Rejects          0          0       0
Timeouts         0          0       0
Stray            0          0       0
```

show amp ipc

The `show amp ipc` command takes a task name as a final argument. This command displays AMP send/recieve statistics for the identified task. The `show amp ipc` command usage is as follows:

```
ACMEPACKET# show amp ipc <task>
```

For example:
show amp lc

The `show amp lc` command displays AMP message statistics for the local core manager (LCM). For example:

```
ACMEPACKET# show amp lc@0.0.0
13:15:08-172 (lcm@0.0.0) ID=d3a9dec0
---------- Received ----------  ----------- Sent *********
Protocol           Recent Total   PerMax Recent Total   PerMax
-------  --------  ------  -----  --------  ------  -----  -----
Total       4 169 160  37 7056  40
SNR          0  5  5   5   5
MAN          0 153 153  34 7039  31
CLIP         4  9  4   3   8
LOG          0  0  0   0   2
CFG          0  2  2   0   2
ToServer     0  2  2
Retries      0  0  0
Rejects      0  0  0
Timeouts     0  0  0
Stray        0  0  0
```

show amp lem

The `show amp lem` command displays AMP message statistics for the local element manager (LEM). For example:

```
ACMEPACKET# show amp lem@0.0.0
13:20:58-122 (lem@0.0.0) ID=d3b54110
---------- Received ----------  ----------- Sent *********
Protocol           Recent Total   PerMax Recent Total   PerMax
-------  --------  ------  -----  --------  ------  -----  -----
Total       2  43  40   1   80   78
MAN          0  2  2   0   39  39
CLIP         2  3  1   1   2
LOG          0  0  0   0   1
CFG          0  38  38  0   38  38
ToServer     0  2  2
Retries      0  0  0
```
show amp logman

The `show amp logman` command displays AMP message statistics for the log manager. For example:

```
ACMEPACKET# show amp logman 0.0.0
13:49:20-131 (logman@0.0.0) | ID=e1657e30

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>6</td>
<td>1633</td>
<td>23</td>
<td>0</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>284</td>
<td>225</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ALARM</td>
<td>5</td>
<td>1342</td>
<td>87</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
```

show amp mbcd

The `show amp mbcd` command displays AMP message statistics for the middlebox control daemon (MBCD). For example:

```
ACMEPACKET# show amp mbcd 2.0.1
13:49:41-118 (mbcd@2.0.1) | ID=d3dc14c0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>29</td>
<td>9060</td>
<td>77</td>
<td>114</td>
<td>36091</td>
<td>167</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>XCODE</td>
<td>28</td>
<td>9002</td>
<td>25</td>
<td>114</td>
<td>36012</td>
<td>97</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NAT</td>
<td>0</td>
<td>42</td>
<td>42</td>
<td>0</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ToServer</td>
<td>0</td>
<td>49</td>
<td>49</td>
<td>0</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td>Retries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rejects</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stray</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

show amp msfe

The `show amp msfe` command displays AMP message statistics for the management socket front end process. For example:

```
ACMEPACKET# show amp msfe 0.0.0
13:50:01-172 (sfe@0.0.0) | ID=e20a7900

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>171</td>
<td>36772</td>
<td>104</td>
<td>170</td>
<td>36806</td>
<td>104</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>35</td>
<td>33</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>8</td>
<td>6</td>
</tr>
</tbody>
</table>
```
show amp natm

The `show amp natm` command displays AMP message statistics for the NAT manager. For example:

```
ACMEPACKET# show amp natm@2.0.0
13:50:26-165 (natm@2.0.0) ID=d53298c0
---------------------------Received---------------------------

Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------
Total            1         13      10        0         14      12
SNR              0          2       2        0          2       2
MAN              0          1       1        0          2       2
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
NAT              0          4       4        0          4       4
CFG              0          3       3        0          3       3
ToServer         0          5       5
Retries        0          0       0
Rejects        0          0       0
Timeouts       0          0       0
Stray          0          0       0
```

**Note:** natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

show amp npm

The `show amp npm` command displays AMP message statistics for NPM. For example:

```
ACMEPACKET# show amp npm
14:22:03-143 (npm@2.0.0) ID=c4950010
---------------------------Received---------------------------

Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------
Total            1         70      28        0        116      46
SNR              0          5       5        0          5       5
MAN              0         15       7        0         55      31
CLIP             1          1       1        0          0       0
LOG              0          0       0        0          3       3
ARP              0          0       0        0          2       2
CFG              0          49      24        0         51      24
ToServer         0         62      27
Retries        0          2       2
Rejects        0          0       0
Timeouts       0          0       0
```
**show amp ntpd**

The `show amp ntpd` command displays AMP message statistics for the NTP application. For example:

```
ACMESYSTEM# show amp ntpd
10:01:48-102 (ntpd@0.0.0) I.D=c767e310

-------------------------- Received --------------------------
Protocol          Recent | Total | PerMax | Recent | Total | PerMax
------            --------  ------  ------  --------  ------  ------
Total             1        4      2       0        3      1
MAN                0        2      2       0        2      1
CLIP               1        2      1       0        1      1

10:01:48-195 (ntpd@0.0.1) I.D=cfcfeaf0

-------------------------- Received --------------------------
Protocol          Recent | Total | PerMax | Recent | Total | PerMax
------            --------  ------  ------  --------  ------  ------
Total             1        5      2       0        5      3
MAN                0        2      2       0         2      1
CLIP               1        2      1       0        1      1
LOG                0        0      0       0        1      1
CFG                0        1      1       0        1      1
```

**show amp rasm**

The `show amp rasm` command displays AMP message statistics for the RADIUS Accounting System Manager (RASM). For example:

```
ACMEPACKET# show amp rasm@0.0.0
13:50:43-114 (rasm@0.0.0) I.D=e2a73160

-------------------------- Received --------------------------
Protocol          Recent | Total | PerMax | Recent | Total | PerMax
------            --------  ------  ------  --------  ------  ------
Total            114      36811     104      113      36836     103
MAN               0        2      2       0        25      26
CLIP              1        3      1       0        2      1
LOG               0        0      0       0        1      1
CFG               0        2      1       0        2      1
REDUNDANCY        113      36804     101      113      36804     101

```

**show amp secured**

The `show amp secured` command Displays Security Daemon AMP statistics. For example:

```
ACMEPACKET# show amp secured
```
14:22:21-148 (secured@0.2.0) ID=d54c4910

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>149</td>
<td>346461</td>
<td>121</td>
<td>148</td>
<td>346455</td>
<td>120</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>35</td>
<td>18</td>
<td>0</td>
<td>35</td>
<td>18</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>148</td>
<td>346412</td>
<td>100</td>
<td>148</td>
<td>346412</td>
<td>100</td>
</tr>
<tr>
<td>AMP-Unk</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

ToServer    0     41    20
Retries     0     0     0
Rejects     0     0     0
Timeouts    0     0     0
Stray       0     0     0

show amp sem

The show amp sem command displays AMP message statistics for the system element manager (SEM). For example:

ACMEPACKET# show amp sem@0.0.0
13:20:58-122 (lem@0.0.1) ID=d3b54110

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>2</td>
<td>43</td>
<td>40</td>
<td>1</td>
<td>80</td>
<td>78</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>39</td>
<td>39</td>
</tr>
<tr>
<td>CLIP</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>38</td>
<td>38</td>
<td>0</td>
<td>38</td>
<td>38</td>
</tr>
</tbody>
</table>

ToServer    0     2     2
Retries     0     0     0
Rejects     0     0     0
Timeouts    0     0     0
Stray       0     0     0

show amp sfe

The show amp sfe command displays AMP message statistics for the socket front end (SFE). For example:

ACMEPACKET# show amp sfe@0.0.1
13:58:26-170 (sfe@0.0.1) ID=cb0ce030

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>169</td>
<td>37276</td>
<td>100</td>
<td>168</td>
<td>37313</td>
<td>101</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>38</td>
<td>38</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>RDPCNTRL</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SFE</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>168</td>
<td>37262</td>
<td>99</td>
<td>168</td>
<td>37262</td>
<td>99</td>
</tr>
</tbody>
</table>
**show amp sipc**

The `show amp sipc` command displays AMP message statistics for the SIP core function. For example:

```plaintext
ACMEPACKET# show amp sipc@0.1.1
13:58:40-149 (sipc@0.1.1) ID=cfcff470

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>75</td>
<td>18640</td>
<td>85</td>
<td>74</td>
<td>18661</td>
<td>107</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>11</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>46</td>
<td>46</td>
<td>0</td>
<td>46</td>
<td>46</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>74</td>
<td>18575</td>
<td>50</td>
<td>74</td>
<td>18575</td>
<td>50</td>
</tr>
<tr>
<td>ToServer</td>
<td>0</td>
<td>60</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rejects</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stray</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**show amp sipls**

The `show amp sipls` command displays AMP message statistics for the SIP location server. For example:

```plaintext
ACMEPACKET# show amp sipls@0.3.0
13:58:55-167 (sipls@0.3.0) ID=c62bd010

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>42</td>
<td>9478</td>
<td>81</td>
<td>41</td>
<td>9499</td>
<td>103</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>52</td>
<td>52</td>
<td>0</td>
<td>52</td>
<td>52</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>41</td>
<td>9405</td>
<td>25</td>
<td>41</td>
<td>9405</td>
<td>25</td>
</tr>
<tr>
<td>PEG</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ToServer</td>
<td>0</td>
<td>64</td>
<td>64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rejects</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stray</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**show amp sipt**

The `show amp sipt` command displays AMP message statistics for the SIP transport function. For example:

```plaintext
ACMEPACKET# show amp sipt@0.1.0
13:59:02-173 (sipt@0.1.0) ID=c631d950

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>44</td>
<td>9460</td>
<td>72</td>
<td>43</td>
<td>9483</td>
<td>96</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>12</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>
```

---

**System Management**

106 Net-Net 9000 Maintenance and Troubleshooting Guide  Version S-D7.1.0
### show amp sm

The `show amp sm` command displays AMP message statistics for the system manager (SM). For example:

```
ACMEPACKET# show amp sm@0.0.0
13:59:21-132 (sm@0.0.0) ID=e19fead0

-------- Received --------   ---------- Sent  ----------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------

Total          204      53777     393       53      11229     444
SNR             19        783     218       19        783     218
MAN            184      52977     176       26       7888     221
CLIP             1         12       4        0         15       8
LOG              0          0       0        0          4       3
RDPCNTRL         0          2       1        0          0       0
ALARM            0          0       0        8       2536      45
CHASSIS          0          3       2        0          3       2
```

### show amp snmpd

The `show amp snmpd` command displays AMP message statistics for the SNMP daemon. For example.

```
ACMEPACKET# show amp snmpd@0.0.0
13:59:37-148 (snmpd@0.0.0) ID=e20fb6e0

-------- Received --------   ---------- Sent  ----------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------

Total            1         11       4        0          9       3
MAN              0          2       2        0          2       1
CLIP             1         3       1        0          2       1
LOG              0          0       0        0          1       1
SNMP             0          2       2        0          0       0
```
The `show amp soapd` command displays AMP message statistics for the SOAP daemon. For example:

```
ACMEPACKET# show amp soapd@0.0.1
13:59:51-155 (soapd@0.0.1) ID=d431a9e0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>39</td>
<td>9425</td>
<td>25</td>
<td>38</td>
<td>9426</td>
<td>25</td>
</tr>
<tr>
<td>SNR</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>38</td>
<td>9415</td>
<td>25</td>
<td>38</td>
<td>9415</td>
<td>25</td>
</tr>
</tbody>
</table>

ToServer  0  5  5
Retries   0  0  0
Rejects   0  0  0
Timeouts  0  0  0
Stray     0  0  0
```

The `show amp sshd` command displays AMP message statistics for the SSH daemon. For example:

```
ACMEPACKET# show amp sshd@0.0.0
14:00:06-177 (sshd@0.0.0) ID=e1e82b80

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```

The `show amp xserv` command displays AMP message statistics for the transcoder server. For example:

```
ACMEPACKET# show amp xserv
14:00:14-154 (xserv@4.0.0) ID=d4185120

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>753</td>
<td>184522</td>
<td>487</td>
<td>715</td>
<td>175334</td>
<td>464</td>
</tr>
<tr>
<td>MAN</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CLIP</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>XCODE</td>
<td>37</td>
<td>9195</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>CFG</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>REDUNDANCY</td>
<td>715</td>
<td>175321</td>
<td>462</td>
<td>715</td>
<td>175321</td>
<td>462</td>
</tr>
</tbody>
</table>

ToServer  0  1  1
Retries   0  0  0
Rejects   0  0  0
Timeouts  0  0  0
Reliable Datagram Protocol (RDP)

RDP is the transport protocol that carries AMP. Tasks use RDP to transport AMP messages among each other.

The `show rdp` command usage is as follows:

```
ACMEPACKET# show rdp <slot #> <cpu #> <core #> [all | links <peer> | linkstats <peer> | serv <task> | servstats <task> | conn <task> | connstats <task>]
```

### show rdp

The `show rdp` command with only core location as an argument presents a quick summary and current links. For example:

```
ACMEPACKET# show rdp 0 0 0

******************************* 0.0.0 Summary ***************************
RxTotal    :    7356723   TxTotal    :    7349011   LclTotal   :      12684
RxBadHdrLen:          0   RxCksumErr :          0   RxBadLen   :          0
TxlIpErrs   :          0   RxNoPort   :          8   RxFullSock :          0
TxRej      :          0   LclNoPort  :          0   LclFullSock:          0
TxTooBig   :          0   TxWrongNet :          0   TxLinkDown :          0
LclFcBlock :          0   LclFcErSelf:          0   LclFcTmout :          0
TxFcBlock  :          0   TxOlflowQBlk:          0   TxFcTimeout:          0
TxWouldBlk :          0   LclWouldBlk:          0
Servers    :        144   LogCount   :        266   LogDropCnt :          0
Errors     :          0   AlarmSet   :          0   AlarmClear :          0
*************************************************************************
```

```
169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP
169.254.160.0  ==> 169.254.160.1   0.0.1/vc    Resets: 0   Conn: 3    UP
```

### show rdp all

The `show rdp all` command displays the RDP stack information for a given CPU/core. In addition, the command shows all connections on the specified core and statistics for that connection. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 all

***************************** 0.0.0 Summary ****************************
RxTotal    :    8853100   TxTotal    :    8844130   LclTotal   :     15242
RxBadHdrLen:          0   RxCksumErr :          0   RxBadLen   :          0
TxlIpErrs   :          0   RxNoPort   :          8   RxFullSock :          0
TxRej      :          0   LclNoPort  :          0   LclFullSock:          0
TxTooBig   :          0   TxWrongNet :          0   TxLinkDown :          0
LclFcBlock :          0   LclFcErSelf:          0   LclFcTmout :          0
TxFcBlock  :          0   TxOlflowQBlk:          0   TxFcTimeout:          0
TxWouldBlk :          0   LclWouldBlk:          0
Servers    :        144   LogCount   :        347   LogDropCnt :          0
Errors     :          0   AlarmSet   :          0   AlarmClear :          0
*************************************************************************
```

```
169.254.96.0 ==>
```
### show rdp links

The `show rdp links` command displays the RDP link information from a supplied CPU/core to all external sockets within the chassis. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 links

169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP

TX                                     RX

Total Packets            : 290115  Total Packets            : 290114
SYNs                     :       1  SYNs                     :       1
ACKs                     :       1  ACKs                     :       1
NAKs                     :       0  NAKs                     :       0
Keepalives               : 290112  Keepalives               : 290111
GRatAcks                 :       0  Rej ConnDel              :       0
Rejects                  :       0  Rejects                  :       0
Conn Deletes             :       0  Conn Deletes             :       1
FC Asserts               :       0  FC Asserts               :       0
FC Deasserts             :       0  FC Deasserts             :       0
RxDups      :       0  RxSockDeliv :       1  RxFullSock :       0
RxOflProtect:       0  RxDropFull :       0  RxOoOSeqs :       0
TxPendQFull :       0  TxWouldBlock :       0
RxBadCcbs :       0  RxBadCcbsSeqs:       0  RxSeqTooFar :       0
InactInterv :       0  MissInterv :       1  TxSeqNum :       2
Rx1stExpSeq :       3  ExpRxSeqNum :       3  LastRxAcks :       2
OflowHead :       0  OflowTail :       0  OflowQDepth :       0
PendQHead :       0  PendQTail :       0  PendQDepth :       0
LinkFlags :       24  RxOnDelCcbs :       0  Reliable Tx :       1
```

### show rdp linkstats

The `show rdp linkstats` command displays the RDP link information from a supplied CPU/core to all external sockets within the chassis. This show command includes the show rdp links command plus additional statistics. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 linkstats

TX                                     RX

Total Packets            : 290115  Total Packets            : 290114
SYNs                     :       1  SYNs                     :       1
ACKs                     :       1  ACKs                     :       1
NAKs                     :       0  NAKs                     :       0
Keepalives               : 290112  Keepalives               : 290111
GRatAcks                 :       0  Rej ConnDel              :       0
Rejects                  :       0  Rejects                  :       0
Conn Deletes             :       0  Conn Deletes             :       1
FC Asserts               :       0  FC Asserts               :       0
FC Deasserts             :       0  FC Deasserts             :       0
RxDups      :       0  RxSockDeliv :       1  RxFullSock :       0
RxOflProtect:       0  RxDropFull :       0  RxOoOSeqs :       0
TxPendQFull :       0  TxWouldBlock :       0
RxBadCcbs :       0  RxBadCcbsSeqs:       0  RxSeqTooFar :       0
```
show rdp serv

The `show rdp serv` command displays the RDP server socket information from a supplied CPU/core to all external sockets within the chassis. Specifying a task name at the end of this command filters for the supplied task. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 serv acl

<table>
<thead>
<tr>
<th>Local Address</th>
<th>TaskId</th>
<th>Task</th>
<th>Fd</th>
<th>FC</th>
<th>Blk</th>
<th>Conn</th>
<th>ChrCnt</th>
<th>RSpace</th>
</tr>
</thead>
<tbody>
<tr>
<td>a9fe6000:1095</td>
<td>e3697850</td>
<td>iAcli</td>
<td>18</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>166400</td>
</tr>
<tr>
<td>a9fe6000:8006</td>
<td>e3697850</td>
<td>iAcli</td>
<td>16</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>262144</td>
</tr>
<tr>
<td>a9fe2000:1094</td>
<td>e3697850</td>
<td>iAcli</td>
<td>14</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>166400</td>
</tr>
<tr>
<td>a9fe2000:8006</td>
<td>e3697850</td>
<td>iAcli</td>
<td>12</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>262144</td>
</tr>
<tr>
<td>a9feb000:1093</td>
<td>e3697850</td>
<td>iAcli</td>
<td>10</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>166400</td>
</tr>
<tr>
<td>a9feb000:8006</td>
<td>e3697850</td>
<td>iAcli</td>
<td>8</td>
<td>no</td>
<td>yes</td>
<td>0</td>
<td>0</td>
<td>262144</td>
</tr>
<tr>
<td>a9fea000:1092</td>
<td>e3697850</td>
<td>iAcli</td>
<td>6</td>
<td>no</td>
<td>yes</td>
<td>5</td>
<td>0</td>
<td>166400</td>
</tr>
<tr>
<td>a9fea000:8006</td>
<td>e3697850</td>
<td>iAcli</td>
<td>4</td>
<td>no</td>
<td>yes</td>
<td>2</td>
<td>0</td>
<td>262144</td>
</tr>
</tbody>
</table>
```

**show rdp servstats**

The `show rdp servstats` command displays the same data as the `show rdp serv` command. In addition, the following counts are displayed for each local address:
**System Management**

- RxDeliver
- RxFullSock
- TxFcAssert
- TxFcDAsser
- LclDeliver
- LclFullSock
- LclWouldBl
- LclFcBlock
- LclFcDisca
- hiwat
- mbcnt
- mbmax
- maxCc

**show rdp conn**

The **show rdp conn** command displays the RDP connection information between tasks running on a supplied CPU/core to all external sockets within the chassis. Specifying a task name at the end of this command filters for the supplied task. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 conn iacli

---------------------------------  ----------------------------------
Local Address TaskId Task        Fd  FC  Blk Conn ChrCnt RSpace
---------------------------------  ----------------------------------
 a9fe6000:1095  e3697850 iAcli       18  no  yes 0    0      166400
 a9fe6000:8006  e3697850 iAcli       16  no  yes 0    0      262144
 a9fe2000:1094  e3697850 iAcli       14  no  yes 0    0      166400
 a9fe2000:8006  e3697850 iAcli       12  no  yes 0    0      262144
 a9feb000:1093  e3697850 iAcli       10  no  yes 0    0      166400
 a9feb000:8006  e3697850 iAcli       8   no  yes 0    0      262144
 a9fea000:1092  e3697850 iAcli       6   no  yes 5    0      166400
---------------------------------  ----------------------------------
Foreign Addr  SNR Name fefc
---------------------------------  ----------------------------------
 a9fe0100:8034           no
 a9feb000:8034           no
 a9feb000:8003  sm       no
 a9fea000:8003  sm       no
 a9feb000:8004  sem      no
---------------------------------  ----------------------------------
Local Address TaskId Task        Fd  FC  Blk Conn ChrCnt RSpace
---------------------------------  ----------------------------------
 a9fea000:8006  e3697850 iAcli       4   no  yes 2    0      262144
---------------------------------  ----------------------------------
Foreign Addr  SNR Name fefc
---------------------------------  ----------------------------------
 a9feb000:8034           no
 a9feb000:8020  logman   no
```

Proprietary & Confidential
**show rdp connstats**

The `show rdp connstats` command displays the same data as the `show rdp conn` command. In addition, the following counts are displayed for each address:

- **RxDeliver** (local address only)
- **RxFullSock**
- **TxFcAssert**
- **TxFcDAsser**
- **LclDeliver** (local address only)
- **LclFullSok** (local address only)
- **LclWouldBl** (local address only)
- **LclFcBlock** (local address only)
- **LclFcDisca** (local address only)
- **hiwat** (local address only)
- **mbcnt** (local address only)
- **mbmax** (local address only)
- **Rx** (foreign address only)
- **Tx** (foreign address only)
- **RxFcAssert** (foreign address only)
- **RxFcDAsser** (foreign address only)
- **TxWouldBlk** (foreign address only)
- **RxRejects** (foreign address only)
- **RxDropFull** (foreign address only)
- **RxOProtect** (foreign address only)
- **DeadlkProt** (foreign address only)

**System Name Registry (SNR)**

The SNR is a service provided by the SM, CM and LCM. Applications can register a mapping of a name to a transport address with their local LCM. The LCM stores these registrations, and forwards them to CM, which stores and forwards them to SM.

The `show snr` command usage is as follows:

```
ACMEPACKET# show snr [core | relay]
```

**show snr core**

The SNR core display shows all tasks active on the Net-Net system and their mapping to an IP address and socket pair. The following is an abbreviated display of this show command:

```
ACMEPACKET# show snr core
122 Names
arpm@2.0.0 169.254.162.0:8014
bcm56k@0.0.0 169.254.160.0:8025
broker@0.0.0 169.254.160.0:8025
broker@0.1.0 169.254.160.1:8025
broker@0.1.0 169.254.160.16:8025
broker@0.1.1 169.254.160.17:8025
```
show snr relay

The SNR relay display shows the SNR relay (lookup) counters.

ACMEPACKET# show snr relay
Rx Request Msgs 307 Request Msg Failures 0
Rx Register Msgs 2 Register Msg Failures 0
Rx Deregister Msgs 2 Deregister Msg Failures 0
Tx Relayed Msgs 311 Rx Unexpected Msgs 0

Redundancy Statistics

The Net-Net 9200 needs to share task information between redundant cards in order for failovers to occur without any system state or call loss.

The show redundancy command is used to display statistics and counts for transactions that occur between cards. This command takes a task as an arguments. The command is entered as follows:

```
show redundancy [arp | auth | cache | collect | configuration | core | mbcd | rasm | sfe | soapd | standby | transport | xserv <slot> <core> <cpu>]
```

Each task you use as an argument returns the same set of statistics. Client transactions are from the perspective of the tasks on the active card. Server transactions are from the perspective of the tasks on the standby card. For example:

ACMEPACKET: show redundancy cache
07:26:16-127 sipls@0.3.0 Redundancy Statistics

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Records</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Records Queued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Records Dropped</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show redundancy standby

By adding the standby argument to the show redundancy command, the ACLI displays the redundancy statistics for the task you identify that exists on the standby card. The command is entered as follows:

```
show redundancy standby [arp | auth | cache | collect | configuration | core | mbcd | rasm | sfe | soapd | transport]
```

For example:

```
ACMEPACKET> show redundancy standby arp
17:18:08-102 arpm@3.0.0 Redundancy Statistics

<table>
<thead>
<tr>
<th></th>
<th>Recent</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>High</td>
<td>Total</td>
</tr>
<tr>
<td>Total Records</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Records Queued</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Records Dropped</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Client Transactions</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Requests Sent</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Requests Re-Trans</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sync Resp Received</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Syncing Resp Receive</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Errors Received</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Server Transactions</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Chassis Hardware Statistics

The show commands described in this section provide information about the Net-Net 9200 chassis hardware.

Card and Hardware Status

The Net-Net OS keeps track of operational status of all major component. These components include all of the possible 13 feature and interface cards, and power and cooling components.
**show status**

The **show status** command lists all possible feature and interface cards, power supplies, and fan trays. For each of these components, State, HA role, environmental conditions, and a memory usage summary are given. For example:

```
ACMEPACKET# show status
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>FANCTRL 0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>14</td>
<td>FANCTRL 1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>15</td>
<td>POWER0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>16</td>
<td>POWER1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>17</td>
<td>POWER2</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>18</td>
<td>POWER3</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**show health**

The **show health** command displays health information for major system components:

- System
- Feature / Interface card
- CPU
- Core

In addition, you can view health information for the power supplies and fan units at the system level.

The show health command displays the Redundancy Event List, which is a log of all major events associated with card switchovers. This is followed by a list of all current alarms at the component level you are viewing.

- If you type show health at the system level, all alarms will be displayed
- If you type show health at the card level, all alarms for that card will be displayed
- If you type show health at the CPU level, all alarms for that CPU will be displayed
- If you type show health at the core level, all alarms for that core will be displayed

The show health command usage follows:

```
show health [<slot #> [CPU #] [core #]]
```
The following example displays system-wide health with redundancy and current alarm information:

```
ACMEPACKET> show health

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>Health Score</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>0</td>
<td>RECOVERY</td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>50</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>100</td>
<td>UNASSIGNED</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>FANCTRL 0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>14</td>
<td>FANCTRL 1</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>15</td>
<td>POWER0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>16</td>
<td>POWER1</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>17</td>
<td>POWER2</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>18</td>
<td>POWER3</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
```

Redundancy Event List

```
Event  Card  Time                      Description                      Reason
1      NPU0   2008-08-22 14:56:17       Assumed Active from NPU0         Gateway Unreachable
```

done

8 alarms to show

```
<table>
<thead>
<tr>
<th>Alarm Id</th>
<th>Task Id</th>
<th>Severity</th>
<th>Last Occurrence</th>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21e11210</td>
<td>tSM@1.0.0</td>
<td>NOTICE</td>
<td>2008-08-22 14:57:24.241</td>
<td>1</td>
<td>Health Score 0 on Card SPU1</td>
</tr>
<tr>
<td>20a00101</td>
<td>tLCM@1.0.0</td>
<td>EMERGENCY</td>
<td>2008-08-22 14:57:23.943</td>
<td>1</td>
<td>Task tLOGMAN on 1.0.0 with PID</td>
</tr>
<tr>
<td>31000134</td>
<td>tBROKER@3.0.0</td>
<td>MAJOR</td>
<td>2008-08-22 14:56:17.842</td>
<td>1</td>
<td>gateway 10.10.140.1 unreachable</td>
</tr>
<tr>
<td>22621222</td>
<td>tSM@3.0.0</td>
<td>NOTICE</td>
<td>2008-08-22 14:56:17.784</td>
<td>1</td>
<td>NPU1 Switch to Active Role</td>
</tr>
</tbody>
</table>
```

**Temperature and I2C Status and Alarms**

When the Net-Net 9200 chassis or any of its components exceeds temperature thresholds, it triggers an alarm and an SNMP trap. When the temperature returns to an acceptable level, the system immediately clears the alarm. There are two types of temperature sensors in the Net-Net 9200 chassis: LM84 sensors and LM75 sensors.

The `show i2c` command displays temperature properties for all i2c devices.

LM84 sensors monitor the temperature of individual CPUs and FPGAs. These sensors take both a local reading and a remote reading. The local reading indicates the temperature of the sensor itself, while the remote reading indicates the temperature of the CPU or FPGA it monitors. LM84 sensors use a single threshold to trigger and clear an alarm; when the temperature rises above the Minor threshold value, an alarm is triggered. An alarm is cleared when the temperature falls below this threshold.

LM75 sensors monitor the temperature of a particular site within the Net-Net 9200 chassis. These sensors have a separate threshold to clear an alarm.

For both sensors, the temperature thresholds are fixed - as detailed in the tables below. The thresholds are determined by the sensor's position on the feature card,
and the feature card’s position within the chassis. These thresholds can not be modified, and are pre-programmed based upon thermal chamber testing.

**SPU Sensors**

The following table identifies LM85 sensors and corresponding temperature thresholds for SPU cards.

<table>
<thead>
<tr>
<th>LM84 Sensor Type</th>
<th>Local Temperature Threshold</th>
<th>Remote Temperature Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>SPU CPU 0 Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
<tr>
<td>SPU CPU 1 Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
<tr>
<td>SPU CPU 2 Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
<tr>
<td>SPU CPU 3 Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
<tr>
<td>SPU CPU 4 Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
</tbody>
</table>

The following table identifies LM75 sensors and corresponding temperature thresholds for SPU cards.

<table>
<thead>
<tr>
<th>LM75 Sensor Type</th>
<th>Temperature Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>SPU Board Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>SPU Board Left Center Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>SPU Board Back Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>SPU Board Middle Back Temp Sensor</td>
<td>60</td>
</tr>
</tbody>
</table>

**NPU Sensors**

The following table identifies LM85 sensors and corresponding temperature thresholds for NPU cards.

<table>
<thead>
<tr>
<th>LM84 Sensor Type</th>
<th>Local Temperature Threshold</th>
<th>Remote Temperature Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>NPU CPU Temp Sensor</td>
<td>70</td>
<td>85</td>
</tr>
<tr>
<td>NPU FPGA Temp Sensor</td>
<td>65</td>
<td>75</td>
</tr>
</tbody>
</table>

The following table identifies LM75 sensors and corresponding temperature thresholds for NPU cards.

<table>
<thead>
<tr>
<th>LM75 Sensor Type</th>
<th>Temperature Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>NPU Board Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>NPU NPO Temp Sensor</td>
<td>60</td>
</tr>
</tbody>
</table>
## TCU Sensors

The following table identifies LM85 sensors and corresponding temperature thresholds for TCU cards.

<table>
<thead>
<tr>
<th>LM85 Sensor Type</th>
<th>Temperature Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>NPU NP1 Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>NPU DX240 Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>NPU CAM Temp Sensor</td>
<td>60</td>
</tr>
</tbody>
</table>

## Interface Card and Fan Sensors

The following table identifies LM75 sensors and corresponding temperature thresholds for interface cards and fan temperature.

<table>
<thead>
<tr>
<th>LM75 Sensor Type</th>
<th>Temperature Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>TCU Board Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>TCU Fpga Temp Sensor</td>
<td>70</td>
</tr>
<tr>
<td>TCU CPU 0 Temp Sensor</td>
<td>85</td>
</tr>
<tr>
<td>TCU CPU 1 Temp Sensor</td>
<td>85</td>
</tr>
<tr>
<td>TCU CPU 2 Temp Sensor</td>
<td>88</td>
</tr>
<tr>
<td>TCU TCM 0 Temp Sensor</td>
<td>93</td>
</tr>
<tr>
<td>TCU TCM 1 Temp Sensor</td>
<td>96</td>
</tr>
<tr>
<td>TCU TCM 2 Temp Sensor</td>
<td>67</td>
</tr>
<tr>
<td>TCU TCM 3 Temp Sensor</td>
<td>67</td>
</tr>
</tbody>
</table>

The following table identifies LM75 sensors and corresponding temperature thresholds for TCU cards.

<table>
<thead>
<tr>
<th>LM75 Sensor Type</th>
<th>Temperature Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>MIU Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>PHY Temp Sensor</td>
<td>60</td>
</tr>
<tr>
<td>Fan Temp Sensor</td>
<td>55</td>
</tr>
</tbody>
</table>
MIB Information

The following table lists the temperature alarms and the traps generated.

<table>
<thead>
<tr>
<th>Name/ID</th>
<th>Severity/Health Degradation</th>
<th>Cause(s)</th>
<th>Log Message</th>
<th>Traps Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>I2C TEMP WARNING/128XX270</td>
<td>MINOR/20</td>
<td>• Temperature fault detected.</td>
<td>• Temperature Warning on X in Slot N</td>
<td>apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minor temperature fault detected on fan controller.</td>
<td>• Setting Minor Temperature Fault on FAN Controller X. Temp is XX.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Temperature Warning on X in Slot N</td>
<td>apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Setting Minor Temperature Fault on FAN Controller X. Temp is XX.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Temperature Warning on X in Slot N</td>
<td>apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Setting Minor Temperature Fault on FAN Controller X. Temp is XX.</td>
<td></td>
</tr>
</tbody>
</table>

show i2c

The **show i2c** command displays temperature properties for all i2c devices.

**LM75 TEMPERATURE PROPERTIES** lists Over Temp values, Trigger Level values, and Reset Level values to support the separate thresholds for triggering and resetting an alarm. Over Temp is a Boolean value which is set when there is an active temperature alarm. The Trigger Level is the high temperature threshold; when temperatures exceed this value, a minor temperature alarm is generated. The Reset Level is the threshold that clears a minor temperature alarm.

An example of the **show i2c** output is shown below:
ACMESYSTEM# show i2c

**SPU0 I2C PROPERTIES**

### LM84 TEMPERATURE PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Temp</th>
<th>Remote Temp</th>
<th>Loc/Rem/Open Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPU CPU 0 Temp Sensor</td>
<td>39</td>
<td>40</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SPU CPU 1 Temp Sensor</td>
<td>39</td>
<td>40</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SPU CPU 2 Temp Sensor</td>
<td>37</td>
<td>38</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SPU CPU 3 Temp Sensor</td>
<td>37</td>
<td>38</td>
<td>0/0/0</td>
</tr>
<tr>
<td>SPU CPU 4 Temp Sensor</td>
<td>36</td>
<td>37</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

### LM75 TEMPERATURE PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Temperature</th>
<th>Over Temp Trigger Level</th>
<th>Reset Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPU Board Temp Sensor</td>
<td>36.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>SPU Board Left Center Temp Sensor</td>
<td>28.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>SPU Board Back Temp Sensor</td>
<td>33.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>SPU Board Middle Temp Sensor</td>
<td>34.5</td>
<td>0</td>
<td>65</td>
</tr>
</tbody>
</table>

### DIGITAL POWER PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Uptime</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPU DPM Temp Sensor</td>
<td>3895594</td>
<td>Group A: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group B: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group C: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group D: Normal</td>
</tr>
</tbody>
</table>

**NPU0 I2C PROPERTIES**

### LM84 TEMPERATURE PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Temp</th>
<th>Remote Temp</th>
<th>Loc/Rem/Open Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU CPU Temp Sensor</td>
<td>40</td>
<td>42</td>
<td>0/0/0</td>
</tr>
<tr>
<td>NPU FPGA Temp Sensor</td>
<td>32</td>
<td>33</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

### LM75 TEMPERATURE PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Temperature</th>
<th>Over Temp Trigger Level</th>
<th>Reset Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU Temp Sensor</td>
<td>36</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU NP0 Temp Sensor</td>
<td>28.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU NP1 Temp Sensor</td>
<td>32.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU DX240 Temp Sensor</td>
<td>26.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU CAM Temp Sensor</td>
<td>32</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### DIGITAL POWER PROPERTIES

<table>
<thead>
<tr>
<th>Name</th>
<th>Uptime</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU DPM Sensor</td>
<td>3634813</td>
<td>Group A: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group B: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group C: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group D: Normal</td>
</tr>
</tbody>
</table>
### NPU I2C Properties

#### LM84 Temperature Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Temp</th>
<th>Remote Temp</th>
<th>Loc/Rem/Open Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU CPU Temp Sensor</td>
<td>40</td>
<td>42</td>
<td>0/0/0</td>
</tr>
<tr>
<td>NPU FPGA Temp Sensor</td>
<td>32</td>
<td>33</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

#### LM75 Temperature Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Temperature</th>
<th>Over Temp Trigger Level</th>
<th>Reset Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU Temp Sensor</td>
<td>36</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU NP0 Temp Sensor</td>
<td>28.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU NP1 Temp Sensor</td>
<td>32.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU DX240 Temp Sensor</td>
<td>26.5</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>NPU CAM Temp Sensor</td>
<td>32</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Digital Power Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Uptime</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPU DPM Sensor</td>
<td>3634813</td>
<td>Group A: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group B: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group C: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group D: Normal</td>
</tr>
</tbody>
</table>

### TCU I2C Properties

#### LM84 Temperature Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Temp</th>
<th>Remote Temp</th>
<th>Loc/Rem/Open Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCU CPU 0 Temp Sensor</td>
<td>39</td>
<td>40</td>
<td>0/0/0</td>
</tr>
<tr>
<td>TCU CPU 1 Temp Sensor</td>
<td>39</td>
<td>40</td>
<td>0/0/0</td>
</tr>
<tr>
<td>TCU FPGA Temp Sensor</td>
<td>0</td>
<td>0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>TCU DPM Sensor</td>
<td>616820</td>
<td>Group A: Normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group B: Normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group C: Normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group D: Normal</td>
<td></td>
</tr>
</tbody>
</table>

#### LM75 Temperature Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Temperature</th>
<th>Over Temp Trigger Level</th>
<th>Reset Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCU Board Temp Sensor</td>
<td>46</td>
<td>0</td>
<td>65</td>
</tr>
<tr>
<td>TCU Board Corner Temp</td>
<td>39</td>
<td>0</td>
<td>78</td>
</tr>
<tr>
<td>TCU TCM 0 Temp Sensor</td>
<td>65</td>
<td>0</td>
<td>93</td>
</tr>
<tr>
<td>TCU TCM 1 Temp Sensor</td>
<td>Device Not Installed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCU TCM 2 Temp Sensor</td>
<td>46</td>
<td>0</td>
<td>67</td>
</tr>
<tr>
<td>TCU TCM 3 Temp Sensor</td>
<td>43.5</td>
<td>0</td>
<td>67</td>
</tr>
</tbody>
</table>

#### Digital Power Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Uptime</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCU DPM Sensor</td>
<td>616820</td>
<td>Group A: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group B: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group C: Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group D: Normal</td>
</tr>
</tbody>
</table>
**Network Processor Card Statistics**

The Network Processor Unit (NPU) is responsible for forwarding media packets along the data plane and propagating signaling packets up to the control plane. Traffic that crosses the NPU’s internal GigE switch (DX240) is purely network traffic,
and is not used by system tasks as they talk to each other. A series of low-level statistics for the NPU’s GigE switch are available.

**show npu phy-port**

The show npu port command displays the port configuration on the phy side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# npu phy-port 0 0 (fiber phy)
  :14034200 00051c3e 00003748 000078cc

DX240 P00 MAC: fiber disabled linkDOWN 1000M FD FC
SYNC Fail Hi PCS Err PLL Locked

ACMEPACKET# show npu phy-port 1 0 (copper phy)
NPU240 PHY-Side Slot 0
P00 MAC: copper enabled linkUP 100M HD
Copper PHY: linkUP 100M HD AN Cmpl
FORCE link pass
```

**show npu phy-stats**

The show npu phy-stats command displays Ethernet statistics on the phy side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu phy-stats 0 0
NPU 240 PHY-side Slot 0 Port 0 Counters:
goodOctetsSent 192 goodOctetsRcv 1635293
goodPktsSent 3 goodPktsRcv 36289
brdcPktsSent 3 brdcPktsRcv 535
mcPktsSent 0 mcPktsRcv 0
badPktsRcv 14 pkts64Octets 736
pkts65to127Octets 1239 pkts128to255Octets 270
pkts256to511Octets 22703 pkts512to1023Octets 11341
pkts1024tomaxOctets 0 badOctetsRcv 15
macTransmitErr 0 excessiveCollisions 0
unrecogMacCntrRcv 0 fcSent 0
goodFcRcv 0 dropEvents 0
undersizePkts 0 fragmentsPkts 14
oversizePkts 0 jumberPkts 0
macRcvError 0 badCrc 0
collisions 0 lateCollisions 0
badFcRcv 0
```

**show npu phy-registers**

The show npu phy-registers command displays register contents for each port on the NPU’s DX240 switch. This command is ONLY applicable when a trispeed copper NIU is connected to the queried port. This command takes a media slot and port argument. Typing this command without any argument displays the NPU stats for port 0. This command is entered as:

```
ACMEPACKET# show npu phy-registers <slot> <port>
```

For example:

```
ACMEPACKET# show npu phy-registers 0 0
PHY Port 0 Page 0 regs:
Reg 00->1140 Reg 01->7949 Reg 02->0141 Reg 03->0cd4
Reg 04->05e1 Reg 05->0000 Reg 06->0004 Reg 07->2001
```

124 Net-Net 9000 Maintenance and Troubleshooting Guide
show npu gmac-port

The `show npu gmac-port` command displays the port configuration on the GMAC side of the DX240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu gmac-port 0 0

NPU240 GMAC-Side Slot 0
P00 MAC: copper enabled linkUP 1000M FD FC
```

show npu gmac-stats

The `show npu gmac-stats` command displays statistics on the GMAC side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu gmac-stats 0 0

NPU 240 GMAC-Side Slot 0 Port 0 Counters:
goodOctetsSent 183459 goodOctetsRcv 14946
goodPktsSent 1541 goodPktsRcv 159
brdcPktsSent 535 brdcPktsRcv 0
mcPktsSent 0 mcPktsRcv 0
badPktsRcv 0 pkts640ctets 0
pkts65to127Octets 159 pkts128to255Octets 0
pkts256to511Octets 0 pkts512to1023Octets 0
pkts1024tomaxOctets 0 badOctetsRcv 0
macTransmitErr 0 excessiveCollisions 0
unrecogMacCntrRcv 0 fcSent 0
goodFcRcv 0 dropEvents 0
undersizePkts 0 fragmentsPkts 0
oversizePkts 0 jabberPkts 0
macRcvError 0 badCrc 0
collisions 0 lateCollisions 0
badFcRcv 0
```

show npu cpu-stats

The `show npu cpu-stats` command displays statistics for the CPU port on the DX240. This is the interface port between the DX240 and the NPU’s CPU. For example:

```
ACMEPACKET# show npu cpu-stats

Good Frames Sent 34559
MAC Tx Error Frames 0
Good Octets Sent 3416567
```
Good Frames Rxd 409
Bad Frames Rxd 0
Good Octets Rxd 46769
Bad Octets Rxd 0

**show npu registers**

The **show npu registers** command displays four key register contents for each of the DX240’s ports. For example:

```
ACMEPACKET# show npu registers
DX240 00000000->00066003 00000004->204ca120 00000004c->0000d141
00000a8->0e03943f 00000a4->0001001d
DX240 P00 Ctrl 04000000->14030201 Stat   P00 04000004->00073009
DX240 P00 Auto 04000008->000033ec Serdes P00 04000010->000078cc
DX240 P01 Ctrl 04000100->14030203 Stat   P01 04000104->00071000
DX240 P01 Auto 04000108->000033ec Serdes P01 04000110->000078cc
DX240 P02 Ctrl 04000200->14030205 Stat   P02 04000204->00071000
DX240 P02 Auto 04000208->000033ec Serdes P02 04000210->000078cc
DX240 P03 Ctrl 04000300->14030207 Stat   P03 04000304->00071000
DX240 P03 Auto 04000308->000033ec Serdes P03 04000310->000078cc
DX240 P04 Ctrl 04000400->14030209 Stat   P04 04000404->00051c3e
DX240 P04 Auto 04000408->000033ec Serdes P04 04000410->000078cc
DX240 P05 Ctrl 04000500->1403020b Stat   P05 04000504->00051c3e
DX240 P05 Auto 04000508->000033ec Serdes P05 04000510->000078cc
DX240 P06 Ctrl 04800000->1403020d Stat   P06 04800004->00051c3e
DX240 P06 Auto 04800008->000033ec Serdes P06 04800010->000078cc
DX240 P07 Ctrl 04800100->1403020f Stat   P07 04800104->00051c3e
DX240 P07 Auto 04800108->000033ec Serdes P07 04800110->000078cc
DX240 P08 Ctrl 04800200->14030211 Stat   P08 04800204->0007300d
DX240 P08 Auto 04800208->000033ec Serdes P08 04800210->000078cc
DX240 P09 Ctrl 04800300->14030213 Stat   P09 04800304->0007300d
DX240 P09 Auto 04800308->000033ec Serdes P09 04800310->000078cc
DX240 P10 Ctrl 04800400->14030215 Stat   P10 04800404->0007300d
DX240 P10 Auto 04800408->000033ec Serdes P10 04800410->000078cc
DX240 P11 Ctrl 04800500->14030217 Stat   P11 04800504->0007300d
DX240 P11 Auto 04800508->000033ec Serdes P11 04800510->000078cc
DX240 P12 Ctrl 05000000->14030219 Stat   P12 05000004->0007300d
DX240 P12 Auto 05000008->000033ec Serdes P12 05000010->000078cc
DX240 P13 Ctrl 05000100->14030221 Stat   P13 05000104->00071000
DX240 P13 Auto 05000108->000033ec Serdes P13 05000110->000078cc
DX240 P14 Ctrl 05000200->14030223 Stat   P14 05000204->00071000
DX240 P14 Auto 05000208->000033ec Serdes P14 05000210->000078cc
DX240 P15 Ctrl 05000300->14030225 Stat   P15 05000304->00071000
DX240 P15 Auto 05000308->000033ec Serdes P15 05000310->000078cc
DX240 P16 Ctrl 05000400->14030227 Stat   P16 05000404->00051c3e
DX240 P16 Auto 05000408->000033ec Serdes P16 05000410->000078cc
DX240 P17 Ctrl 05000500->14030229 Stat   P17 05000504->00051c3e
DX240 P17 Auto 05000508->000033ec Serdes P17 05000510->000078cc
DX240 P18 Ctrl 05800000->1403022b Stat   P18 05800004->00051c3e
DX240 P18 Auto 05800008->000033ec Serdes P18 05800010->000078cc
DX240 P19 Ctrl 05800100->1403022d Stat   P19 05800104->00051c3e
DX240 P19 Auto 05800108->000033ec Serdes P19 05800110->000078cc
DX240 P20 Ctrl 05800200->1403022f Stat   P20 05800204->0007300d
DX240 P20 Auto 05800208->000033ec Serdes P20 05800210->000078cc
DX240 P21 Ctrl 05800300->14030231 Stat   P21 05800304->0007300d
```
dump npu-stats

The `dump npu-stats` command loops through a series of NPU statistics twice and writes the results to the log.npu_debug file.

Internal Switch Statistics

The Net-Net system’s SPU contains a GigE switch which facilitates communication between every task on the Net-Net 9200 chassis. The `show switch` command usage is as follows:

```
ACMEPACKET# show switch <slot #> [portstate | portstats | linkstate | l2table] <port #>
```

The port # argument is optional and filters for the given port.

show switch portstate

The `show switch portstate` command displays the state of each port on the specified switch. You must include the slot number to indicate which switch to query. For example:

```
ACMEPACKET# show switch 0 portstate
BCM Switch Port 0 State is Active
BCM Switch Port 1 State is Active
BCM Switch Port 2 State is Active
BCM Switch Port 3 State is Active
BCM Switch Port 4 State is Active
BCM Switch Port 5 State is Active
BCM Switch Port 6 State is Active
BCM Switch Port 7 State is Active
BCM Switch Port 8 State is Active
BCM Switch Port 9 State is Active
BCM Switch Port 10 State is Active
BCM Switch Port 11 State is Active
BCM Switch Port 12 State is Active
BCM Switch Port 13 State is Active
BCM Switch Port 14 State is Active
ACMEPACKET#
```

show switch linkstate

The `show switch linkstate` command displays the link state for each port on the specified switch. You must include the slot number to indicate which switch to query. Specifying a port number filters for that port. For example:

```
ACMEPACKET# show switch 0 linkstate
BCM Switch Port 0 Link is Active
BCM Switch Port 1 Link is Active
BCM Switch Port 2 Link is Active
BCM Switch Port 3 Link is Active
BCM Switch Port 4 Link is Active
BCM Switch Port 5 Link is InActive
BCM Switch Port 6 Link is InActive
BCM Switch Port 7 Link is Active
BCM Switch Port 8 Link is InActive
```

Proprietary & Confidential
BCM Switch Port 9 Link is InActive
BCM Switch Port 10 Link is InActive
BCM Switch Port 11 Link is InActive
BCM Switch Port 12 Link is InActive
BCM Switch Port 13 Link is InActive
BCM Switch Port 14 Link is InActive
ACMEPACKET# show switch 0 linkstate 1
BCM Switch Port 1 Link is Active

**show switch portstats**

The `show switch portstats` command displays the statistics for each port on the specified switch. You must include the slot number to indicate which switch to query. Specifying a port number filters for that port. For example:

```
ACMEPACKET# show switch 0 portstats 1
Statistics for Unit 0 port ge1
 3529142237  snmpIfInOctets (stat 0)
 53518830  snmpIfInUcastPkts (stat 1)
    8  snmpIfInUCastPkts (stat 2)
   201  snmpIfInErrors (stat 4)
 3553834235  snmpIfOutOctets (stat 6)
 53515186  snmpIfOutUcastPkts (stat 7)
  4882  snmpIfOutUCastPkts (stat 8)
   6638  snmpDot1dBasePortMtuExceededDiscards (stat 17)
 3518838  snmpDot1dTpPortInFrames (stat 18)
 53520068  snmpDot1dTpPortOutFrames (stat 19)
   4890  snmpEtherStatsBroadcastPkts (stat 23)
   153  snmpEtherStatsFragments (stat 25)
 106499036  snmpEtherStatsPackets64Octets (stat 26)
 205155  snmpEtherStatsPackets65to127Octets (stat 27)
  30733  snmpEtherStatsPackets128to255Octets (stat 28)
  11158  snmpEtherStatsPackets256to511Octets (stat 29)
  136274  snmpEtherStatsPackets512to1023Octets (stat 30)
   49512  snmpEtherStatsPackets1024to1518Octets (stat 31)
   6638  snmpEtherStatsOversizePkts (stat 32)
 0x00000001a62da4d8  snmpEtherStatsOctets (stat 34)
 107038906  snmpEtherStatsPts (stat 35)
 53513478  snmpEtherStatsTXNoErrors (stat 38)
 53518790  snmpEtherStatsRXNoErrors (stat 39)
   48  snmpDot3StatsFrameTooLongs (stat 50)
 3529142237  snmpIfHCInOctets (stat 56)
 53518830  snmpIfHCInUcastPkts (stat 57)
    8  snmpIfHCInUCastPkts (stat 59)
 3553834235  snmpIfHCOutOctets (stat 60)
 53515186  snmpIfHCOutUcastPkts (stat 61)
  4882  snmpIfHCOutUCastPkts (stat 63)
   136  snmpBcmEtherStatsPackets1522to2047Octets (stat 69)
   350  snmpBcmEtherStatsPackets2048to4095Octets (stat 70)
   6152  snmpBcmEtherStatsPackets4095to9216Octets (stat 71)
```
**show switch l2table**

The `show switch l2table` command displays the Layer 2, Ethernet table on the specified switch. The Ethernet address and vlan ID are shown for the port they are bound to. For example:

```
ACMEPACKET# show switch 0 l2table
```

```
L2 Table for BCM 56304

[ iCm] mac=00:11:22:01:02:01 vlan=1 modid=0 port=6/ge6 [ iCm]
[ iCm] mac=00:11:22:00:21 vlan=1 modid=0 port=6/ge6 [ iCm]
[ iCm] mac=00:11:22:00:41 vlan=1 modid=0 port=4/ge4 [ iCm]
[ iCm] mac=00:11:22:01:06:01 vlan=1 modid=0 port=6/ge6 [ iCm]
[ iCm] mac=00:11:22:00:03:01 vlan=1 modid=0 port=8/ge8 [ iCm]
[ iCm] mac=00:11:22:01:05:11 vlan=1 modid=0 port=6/ge6 [ iCm]
[ iCm] mac=00:11:22:01:00:11 vlan=1 modid=0 port=1/ge1 [ iCm]
[ iCm] mac=00:11:22:00:00:41 vlan=1 modid=0 port=4/ge4 [ iCm]
[ iCm] mac=00:11:22:01:06:01 vlan=1 modid=0 port=6/ge6 [ iCm]
```

**TCU Statistics**

The Net-Net system’s TCU can be queried for contains a GigE switch which facilitates communication between every task on the Net-Net 9200 chassis. The `show tcu` command usage is as follows:

```
show TCU [flair | gbe | hm | ibx | tcm] <slot> [tcm-ID <port>]
```

The TCM ID and port arguments are only used with the gbe and ibx arguments.

**show tcu flair**

The `show tcu flair` command displays the FLAIR statistics and counters of an identified TCU. The command is entered as:

```
show tcu flair <tcu slot>
```

For example:

```
ACMEPACKET# show tcu flair 4
```

```
version : 0x6a0b0244
System Status : 0x00000065
Channel Select : 0x0000010c
Port 0 Link Error Counter : 0x00000000
Port 1 Link Error Counter : 0x00000000
Port 0 Data Error Counter : 0x00000000
Port 1 Data Error Counter : 0x00000000
```
show tcu gbe

The `show tcu gbe` command displays Ethernet statistics between the NPU and TCU. It requires a slot and TCM id argument where

- slot = TCU slot number
- tcm ID = TCM ID: 0, 1, 2, or 3

For example:

```
ACMEPACKET# show tcu gbe 4 0
========== Flair GbE unit: 0 Statistics ==========
rev                            : 0x00010003
mac_0                          : 0x00000000
mac_1                          : 0x00000000
frm_length                     : 0x00000600
pause_quant                    : 0x00000010
rx_section_empty               : 0x00000100
rx_section_full                : 0x00000000
tx_section_empty               : 0x000001e0
tx_section_full                : 0x00000000
rx_almost_empty                : 0x00000000
rx_almost_full                 : 0x00000000
tx_almost_empty                : 0x00000008
tx_almost_full                 : 0x00000020
mdio_addr0                     : 0x00000000
mdio_addr1                     : 0x00000001
phy_status                     : 0x0000001e
aFramesTransmittedOK           : 0x00000000
aFramesReceivedOK              : 0x00000000
aFramesCheckSequenceErrors     : 0x00000000
aAlignmentErrors               : 0x00000000
aOctetsTransmittedOK           : 0x00000000
aOctetsReceivedOK              : 0x00000000
aTxPAUSEMACCtrlFrames          : 0x00000000
aRxPAUSEMACCtrlFrames          : 0x00000000
ifInErrors                     : 0x00000000
ifOutErrors                    : 0x00000000
ifInUcastPkts                  : 0x00000000
ifInBroadcastPkts              : 0x00000000
ifInMulticastPkts              : 0x00000000
ifOutDiscards                  : 0x00000000
ifOutUcastPkts                 : 0x00000000
ifOutMulticastPkts             : 0x00000000
ifOutBroadcastPkts             : 0x00000000
DropEvent                      : 0x00000000
Octets                         : 0x00000000
Pkts                           : 0x00000000
UndersizePkts                  : 0x00000000
```
**show tcu hm**

The `show tcu hm` command displays health monitor statistics about a specified TCU on the screen. This command requires a slot argument which refers to the TCU in the slot you are querying. The command is entered as:

```
show tcu hm <tcu slot>
```

For example:

```
ACMEPACKET# show tcu hm 4
  Initialized           : TRUE
  Paused               : TRUE

  Packet matched VETH  : 0
  MAC Received packets : 0
  MAC RX packets to Q  : 0
  MAC RX packets to Q Error : 0

  Received NPU packets    : 0
  Received NPU pkt UNK ADDR  : 0

  Sent TCU packets       : 0
  Sent TCU packets ERROR : 0

  Link Down Count        : 0
```

**show tcu ibx**

The `show tcu ibx` command displays the IBX unit’s statistics and counters of an identified TCU. The command is entered as:

```
show tcu ibx <tcu slot> <TCM number> <TCM switch port>
```

- slot—TCU slot number, 4, 5, or 6
- tcm ID—TCM ID, 0, 1, 2, or 3
- port—DSP port 0 ~ 9, DBG port is 15, FLAIR port is 25, BCM1250 port is 26

**show tcu tcm**

The `show tcu tcm` command displays the TCM configuration of an identified TCU. The command is entered as:

```
show tcu tcm <tcu slot>
```

For example:

```
ACMEPACKET# show tcu tcm 4
  TCM 0 at CPU 0 core 0 is Present
  TCM 1 at CPU 1 core 0 is Present
  TCM 2 at CPU 0 core 1 is Present
  TCM 3 at CPU 1 core 1 is Present
```
Internal Switch Port Mirroring

To mirror traffic from ports to port on the SPU’s internal switch (BCM 56000), you use the `mirror` command. Mirroring is a way to sniff control traffic, that you can enable and disable as needed.

Enabling and disabling mirroring requires that you enter the SPU number, port number on the switch from which you want to mirror traffic (or you can mirror them all), the port number on the SPU to which you want that traffic mirrored, and either enabled or disabled. Traffic is ALWAYS mirrored to port 19. The `mirror` command usage is as follows:

```
mirror <SPU slot> <from-port> <to-port #> <enabled|disabled>
```

For example:

```
ACMEPACKET# mirror 0 10 19 enabled
```

Remember to disable mirroring when your debugging session ends.

BCM 56000 Ports

The following table lists the ports on the SPU’s BCM 56K switch.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Local SPU CPU 0</td>
</tr>
<tr>
<td>1</td>
<td>Local SPU CPU 1</td>
</tr>
<tr>
<td>2</td>
<td>Local SPU CPU 2</td>
</tr>
<tr>
<td>3</td>
<td>Local SPU CPU 3</td>
</tr>
<tr>
<td>4</td>
<td>Local SPU CPU 4</td>
</tr>
<tr>
<td>5</td>
<td>Other SPU CPU 0</td>
</tr>
<tr>
<td>6</td>
<td>Other SPU BCM56K</td>
</tr>
<tr>
<td>7</td>
<td>NPU’s CPU (slot 2)</td>
</tr>
<tr>
<td>8</td>
<td>NPU’s CPU (slot 3)</td>
</tr>
<tr>
<td>9</td>
<td>TCU CPU 0 (slot 4)</td>
</tr>
<tr>
<td>10</td>
<td>TCU CPU 1 (slot 4)</td>
</tr>
<tr>
<td>11</td>
<td>TCU CPU 0 (slot 5)</td>
</tr>
<tr>
<td>12</td>
<td>TCU CPU 1 (slot 5)</td>
</tr>
<tr>
<td>13</td>
<td>TCU CPU 0 (slot 6)</td>
</tr>
<tr>
<td>14</td>
<td>TCU CPU 1 (slot 6)</td>
</tr>
</tbody>
</table>

Switching Cores from the ACLI

When you open a connection to the Net-Net 9200 and are using the ACLI, you are connected by default to the master core on the SPU (0.0.0). However, you can connect to and use the ACLI on other cores. Using the ACLI on other cores gives you the same range of ACLI functionality that you have on the master core.

Connecting to other cores can be useful for debugging purposes, and also for viewing local logs within `/ramdrv/logs`. To switch cores from the ACLI:
1. In Superuser mode, enter the command `connect console` and then the slot, CPU, and core numbers to which you want to connect. You enter the slot, CPU, and core numbers in the spaced format.

   ACMEPACKET# connect console 0 0 1

2. The system prompts you to confirm. To proceed, type `y` and press <Enter>. To stay on the current core, type `n` to cancel the connection.

   Are You Sure [y/n]?: y

3. Once you have connected to another core, note the change in your command line prompt. The command line prompt indicates the location where you are running the ACLI.

   ACMEPACKET@0.0.1#

### System Card Communication Integrity

The Net-Net OS has mechanisms to verify internal connections between feature and interface cards. These processes are enabled within the appropriate configuration elements.

#### SPU to MIU Communication

A ping mechanism is used to test link integrity between an SPU and its dedicated MIU. The SPU sends a ping request out of the MIU’s wancom/management IP ports into the network. When a ping reply is received, the SPU-MIU link integrity is verified. If no reply is received, the SPU-MIU link integrity is considered failed.

In order to use this feature, you must configure a network device connected to the MIU’s Ethernet ports. This device must be capable of responding to ICMP ping request messages.

SPU to MIU communication verification is enabled with the `miu0-monitor-ip-address` or `miu1-monitor-ip-address` parameter located in the `system-config` configuration element.

- `miu0-monitor-ip-address`—Enter an IP address of a device that will return a ping, located in MIU0’s network.
- `miu1-monitor-ip-address`—Enter an IP address of a device that will return a ping, located in MIU1’s network.

#### NPU to TCU Communication

For transcoding applications, the NPU and TCU must communicate with each other. The Net-Net 9200 uses an internal process to verify the link between these two feature cards. NPU to TCU communication verification is enabled or disabled with the `xcode-path-monitor` parameter located in the `system-config` configuration element.

### Password Strength

**Password Policy**

You can configure the minimum acceptable length for a password if you have Superuser (administrative) privileges. The maximum password length is 64 characters.

To increase password strength, new passwords must include at least one character from three out of four of the following character sets:
Setting the Password Policy

In the security ACLI path, you will find the `password-policy` configuration. It contains the `min-secure-pwd-len` parameter where you set the length requirement—between 8 and 64 characters—to use for passwords when password secure mode is enabled. For example, if you set this value to 15, then your password must be a minimum of 15 characters in length.

To set the minimum password length to use for password secure mode:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   `ACMEPACKET# configure terminal`

   `ACMEPACKET(configure)#`

2. Type `security` and press <Enter>.
   
   `ACMEPACKET(configure)# security`

   `ACMEPACKET(security)#`

3. Type `password-policy` and press <Enter>.
   
   `ACMEPACKET(system-config)# password-policy`

   `ACMEPACKET(password-policy)#`

4. `min-secure-pwd-len`—Enter a value between 8 and 64 characters that defines the minimum password length to use when in password secure mode. This parameter defaults to 8.

5. Save your work using the ACLI `done` command.

6. Save and activate your configuration.

Setting a New Password

After setting a new minimum password length, you can change your password for either the User mode or the Superuser mode. The `set password` command is entered as follows:

```
set password [login | enable | reset]
```

Where

- `login`—Sets the User mode password
- `enable`—Sets the Superuser mode password
- `reset`—Resets all passwords

1. Type `set password login` in User mode.
   
   `ACMEPACKET# set password login`

2. Enter your new password at the Enter new password prompt. Your typing will not be echoed to the screen.
Enter new password:

3. If your password doesn’t conform to the requirements, the ACLI prints a summary of your password’s characteristics so you can see how to enter a valid password. For example:

    ACMEPACKET# set password login
    Enter new password:
    % Summary:
    %   password length: 9
    %   alpha character count: 9
    %   numeric character count: 0
    %   upper-case character count: 0
    %   lower-case character count: 9
    %   punctuation character count: 0
    %   invalid character count: 0
    
    % Only alphabetic (upper or lower case), numeric and punctuation characters are allowed in the password.
    % Password must be 10 - 64 characters, and have 3 of the 4 following character classes:
    %   - lower case alpha
    %   - upper case alpha
    %   - numerals
    %   - punctuation
    Enter new password:

4. Enter a new valid password, and then confirm the password.

Resetting Passwords

You can use the set password [login | enable] reset command to restore the associated password to the default.

Tech Support Show Command

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 show support-info usage is as follows:

    show support-info [standard | custom]

- standard—Displays information for all commands the show support-info command encompasses.
- custom—Uses the /code/supportinfo.cmds file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.
- media—Executes and writes out only the show media commands to the support-info.log file.
- signaling—Executes and writes all but the show media commands to the support-info.log file.

In all cases, the system displays the command’s output on the screen and writes the output to the support-log.info file (stored in /ramdrv/logs).

Each time the show support-info command is executed a new support-info.log file is created. The previous support-info.log file is renamed by appending a .1 to
the end of the file name. All additional support-info.log files are renamed to their previous number, plus 1. The Net-Net SBC maintains up to 6 support-info files: support-info.log and support-info.log.1 through support-info.log.5.

For example, when executing the show support-info command, a new support-info.log file is created. The existing support-info.log file is renamed to support-info.log.1. The existing support-info.log.1 file is renamed to support-info.log.2, and so on. If a support-info.log.5 exists prior to executing the show support-info command, it is deleted from the system when rotating the files.

The show support-info command combines the output of several ACLI commands into a single command. These include:

**General System Commands**

- show bootparams
- show version all
- show i2c
- show alarm current
- show clock
- show system
- show log level * all
- show task active
- show task standby
- show arp
- show sip sessions
- show features
- show health
- show status
- show status slot
- show user
- show space
- show ip connections
- show acl all
- show cpu summary

**Physical Interface Commands**

- show interfaces
- show media network
- show media frame-statistics
- show media phy-statistics <slot> <port>
- show media host-statistics <slot> <port>
- show media classify <slot> <port>
- show media gmac-statistics <slot> <port>

**SIP Commands**

- show sip realm
- show sip cache
- show sip all
- show sip agents
- show log level sip*@*all

**Call Media Commands**

- show mbcd all
- show mbcd realms
xserver Commands

```
show xserver <4.0.0,5.0.0,6.0.0> stats
show xserver <4.0.0,5.0.0,6.0.0> audit alloc
show xclient xlist
show xclient api-stats
show arp
show arp-statistics-all
show arp info
show arp standby
show nat statistics
show npu hm
```

Security Commands

```
show security certificates brief
show security ssh-pub-key
show ssm-accelerator
show tls session-cache
```

Display Information to the Screen

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 standard
   ```

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

System Configuration Listing

The `show support info` command can append the complete running config output (`show running-config`) to the end of the support output file by adding the “config” argument to the end of any `show support-info` command, except `show support-info custom`. For example:

```
ACMEPACKET# show support-info standard config
```

ACLI Management

ACLI Terminal Settings

The height and width of the ACLI display, in characters is customizable. You can also control the use of the `more` prompt.

```
show terminal
```

You can view a summary for all these settings using the ACLI `show terminal` command. For example:

```
ACMEPACKET# show terminal
Terminal settings:
  Height: 40
  Width: 80
  More: enabled
```
Using the `set terminal height` command, you can configure the number of rows to set the height of the display. The default is 40 rows, and valid values range from 5-1000. You can also set the terminal height to zero (0), which turns off the more prompt.

**To set the terminal height:**

1. Type the command `set terminal height` followed by the number of rows corresponding to the height. You can choose between 5-1000 rows, and setting the terminal height to 0 turns the more prompt feature off. Then press <Enter>. For example:

```
ACMEPACKET# set terminal height 50
```

Using the `set terminal width` command, you can configure the number of columns to set the width of the display. The default is 80 columns, and valid values range from 10-256.

**To set the terminal width:**

1. Type the command `set terminal width` followed by the number of columns corresponding to the width. Then press <Enter>. For example:

```
ACMEPACKET# set terminal width 100
```

When the output of a command is too large to fit your configured terminal size, the system displays the output in smaller sections. At the end of a section a message is displayed with your options:

- `<Space>`—Display the next section of output
- `<q>`—Quits and returns to the system prompt
- `<c>`—Displays the rest of the output in its entirety

**To turn the more prompt feature on:**

1. Type the command `set terminal more enabled`, and then press <Enter>.

```
ACMEPACKET# set terminal more enabled
```

**To turn the more prompt feature off:**

1. Type the command `set terminal more disabled`, and then press <Enter>.

```
ACMEPACKET# set terminal more disabled
```

The Net-Net 9200 can alert you when a configuration has been changed and you’ve applied the `done` command, but have not saved and activated yet. When you issue the `done` command and return to Superuser mode, the system prefixes the ACLI prompt with two asterisks (**). For example:

```
**ACMEPACKET#
```

When you have saved the configuration, but not yet activated it, the system prefixes the ACLI prompt with one asterisk (*). For example:

```
*ACMEPACKET#
```

When the saved configuration and the activated configuration are synchronized after activating the saved configuration, the ACLI prompt does not contain any asterisks. For example:
Although the **ACMEPACKET#** prompt is lost on reboot, logging out of an ACLI session will not affect the done configuration prompt. In such a case, the **ACMEPACKET#** prompt persists across ACLI sessions.

### Setting the Configuration Mismatch Warning

**To enable the configuration mismatch warning:**

1. At the Superuser prompt, type `set cfgchange-prompt enable`. For example:
   ```
   ACMEPACKET# set cfgchange-prompt enable
   ```

**To confirm the configuration version mismatch alert functionality:**

1. At the Superuser prompt, type `show cfgchange-prompt`. For example:
   ```
   ACMEPACKET# show cfgchange-prompt
   ```

### Save Configuration Warning

The ACLI alerts you if a configuration change has not been saved before you perform a reboot. For example:

```
**ACMEPACKET#** reboot

---------------------------------------------------
WARNING: configuration changes have not been saved!
Rebooting without performing a "save config" will result in all configuration changes being lost!
---------------------------------------------------

Are You Sure [y/n]?:
```

At this point, you should type `n <enter>`, and save and activate your configuration. If you only save the configuration, but do not activate it prior to reboot. The following message appears inline during the boot process:

```
Using last running configuration, issue "activate config" to load current configuration
```

### CLI Audit Trail

You can configure your Net-Net SBC to save 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 `/ramdrv/logs/cli.audit.log` file. This file is lost when the Net-Net 9200 reboots. 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`.

The `cli.audit.log` file is closed when it reaches 1,000,000 bytes. The Net-Net 9200 maintains 5 closed files at any time before the oldest file is overwritten.

The system records details like 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 resembles the following example:

```
Dec 23 19:44:06.479 OPENED 0.0.0 /ramdrv/logs/cli.audit.log
Dec 23 2009 19:48:12.330 Task: console@0,0,0 user@console : 'enable'
Dec 23 2009 19:51:53.918 Task: console@0,0,0 admin@console : 'configure terminal'
Dec 23 2009 19:51:54.951 Task: console@0,0,0 admin@console : 'system'
Dec 23 2009 19:51:57.398 Task: console@0,0,0 admin@console : 'system-config'
Dec 23 2009 19:52:06.132 Task: console@0,0,0 admin@console : 'select'
Dec 23 2009 19:52:06.750 Task: console@0,0,0 admin@console : 'done'
Dec 23 2009 19:52:18.151 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:19.158 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:21.389 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:23.038 Task: console@0,0,0 admin@console : 'show interfaces'
Dec 23 2009 19:58:30.794 Task: console@0,0,0 admin@console : 'show auditlog 0'
```

### Viewing the CLI Audit Trail

You can use the `show auditlog` command to view CLI Audit Trail files (cli.audit.log) directly at the ACLI. Without specifying any arguments, the system displays the file currently being written to.

You can specify the closed log to view by including an optional number argument at the end of the command. For example, typing `show auditlog 3` displays `cli.audit.log.3.gz` on the screen.

Note that rolled over files are large (1 Mb in uncompressed size) and content will take several seconds or minutes to be displayed on the screen.

### ACLI Instructions and Examples

To enable CLI audit trail:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ```
2. Type `system` and press <Enter> to access the system-level configuration elements.
   ```
   ACMEPACKET(configure)# system
   ```
3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   ```
   ACMEPACKET(system)# system-config
   ```
4. `cli-audit-trail`—Set this to enabled for the CLI audit trail feature to run.
5. Save and activate your configuration.

### Support for Last Modified By

The Last Modified By feature appends a new field to all configuration elements, which is displayed when viewing any configuration element instance on the ACLI. The new field indicates whether the last configuration element change was performed from the ACLI or from the Net-Net EMS, and identifies the user who performed the change.
**Note:** The last-modified-by field is blank after an upgrade from a Net-Net OS version that does not support this feature.

**EMS derived modification**

When a configuration element was last modified via EMS, the `last-modified-by` line appears as follows:

```
last-modified-by                EMS_admin_172.30.80.2_UTC
```

In the above example, the EMS identifier indicates that the modification was made by EMS. The admin identifier indicates that the modifications was made from the EMS admin account. Next, the IP address identifies the host machine of the system on which EMS was hosted. Finally, the UTC identifier indicates the time zone where the EMS user made the modifications, as configured.

**ACLI Derived Modification**

When a configuration element was last modified via the ACLI, the `last-modified-by` line of a configuration element output can take two forms, based on how the user accessed the Net-Net SBC.

**Console Access**

When configuring the Net-Net SBC via a console connection, the `last-modified-by` line appears as `admin` separated from the word `console` by an ampersand. For example:

```
last-modified-by                admin@console
```

**Telnet/SSH Access**

When configuring the Net-Net SBC via a Telnet or SSH connection, the `last-modified-by` line appears as `admin` separated from the remote access machine’s IP address by an ampersand. For example:

```
last-modified-by                admin@172.30.0.78
```

**RADIUS Authentication**

When a Telnet or SSH login has been authenticated via RADIUS, the `last-modified-by` user takes a slightly different format than that used for internally authenticated users.

**Console Access**

For a RADIUS authenticated console login, the `last-modified-by` line takes the same form as when the console connection was internally authenticated. For example:

```
last-modified-by                admin@console
```

**Telnet/SSH Access**

For a RADIUS authenticated Telnet or SSH login, the `last-modified-by` line appears as the RADIUS user-name separated from the remote access system’s IP address by an ampersand. For example:

```
last-modified-by                radius-username@172.30.0.78
```

**FTP/SFTP Session Management**

When listing the current user sessions on the Net-Net SBC, the ACLI now displays FTP and SFTP sessions.
### Viewing Sessions

The `show users` ACLI command includes console, Telnet, SSH, FTP and SFTP entry applications as listed in the `type` column. The `state` column shows either `login` or user name, where `login` signifies that the user has yet to login. Because SFTP sessions are initiated over an SSH session, the `type` column shows up as `ssh` before login. Once the SFTP session has been initiated, the `type` column changes to `sftp`. For example:

```
ACMEPACKET# show users
Index task-id remote-address IdNum duration type state
----- ---------- --------------------- ----- -------- ------- -----
0 0x193348a0                           0   6d:03h console user
1 0xf22c250 10.0.200.204:4065   100 00:01:56     ssh  priv *
11 0x195b7290 10.0.200.204:4068    11 00:00:07     ftp  user
21 0x196298c0 10.0.200.204:4065    21 00:01:59    sftp  user
```

### Terminating Sessions

The `kill` command now supports terminating FTP and SFTP sessions. The `kill` command is used in conjunction with the `IdNum` column output, corresponding to a user session, in the `show users` command. For example:

```
ACMEPACKET# kill 11
Killing ftp session at Index 11
```

The above example terminates the FTP session in the `show users` example above.

### Historical Data Recording

Historical data recording (HDR) refers to a group of management features that allow you to configure the Net-Net SBC to periodically collect statistics about system operation and function, and then periodically send those records to designated servers. System statistics, defined in detail below, are saved to a comma-separated value (CSV) files, which are then sent to the designated server(s).

Information types are grouped so that you can refer to a set of statistics by simply invoking their group name. Within each group, there are several metrics available.

### How It Works

In the system configuration, you can enable HDR by first turning on the system’s collection function, then choosing the groups you want to capture, and finally setting up server(s) to which you want records sent.

The main collect configuration (found in the main system configuration) allows you to create global settings that:

- Turn the HDR function on and off
- Set the sample rate in minutes, or the time between individual sample collections
- Set the time in minutes in between individual pushes to designated servers (configured in the push receiver configuration accessed via the collect configuration)
- Set the time you want the collect to start and stop; time is entered in year, month, day, hours, minutes, and seconds

You also configure settings for each group of data you want to collect, and the push receiver (server) to which you want data sent.
About the CSV File

When you enable HDR and configure one or more servers to which you want records sent, data is transmitted in a CSV file in standard format. There is one CSV file per record group type, and the first record for each file is a header containing the field name for each attribute in that file.

Collection Interval and Push

In your HDR configuration, you set parameters that govern:

- The groups for which the Net-Net SBC collects records
- How frequently the Net-Net SBC collects records
- How frequently the Net-Net SBC sends records off-box

Groups, collections, and records are determined as follows:

- Number of groups you configure corresponds to the number of push files sent.
- Number of collections per file is the push interval divided by the sample interval.
- Number of records per collection is dependent on the group you are collecting.

For example, for a collection group of ten records, with a push interval time of 5 minutes and a sample interval time of 1 minute, the Net-Net SBC would send 50 group records and 1 header record for each push.

Note that after each successful push, the Net-Net SBC clears (deletes) all records. The Net-Net SBC also clears files on system reboot, and after three consecutive push failures.

Group Record Types

In the group-name parameter for the group-settings configuration, you can enter any one of the groups record type defined in the following table. You specify the collection object, and then all metrics for that groups are sent.

<table>
<thead>
<tr>
<th>Collection Object—ACLI parameter</th>
<th>Metrics Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Group—card</td>
<td>• Slot Number</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Card state</td>
</tr>
<tr>
<td></td>
<td>• Health score</td>
</tr>
<tr>
<td></td>
<td>• Redundancy state</td>
</tr>
<tr>
<td>CPU Core Group—core</td>
<td>• Core number</td>
</tr>
<tr>
<td></td>
<td>• Core description</td>
</tr>
<tr>
<td></td>
<td>• Core state</td>
</tr>
<tr>
<td></td>
<td>• CPU utilization</td>
</tr>
<tr>
<td></td>
<td>• RAM description</td>
</tr>
<tr>
<td></td>
<td>• RAM utilization</td>
</tr>
<tr>
<td>Environmental fan statistics (fan)</td>
<td>• Fan location</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Speed</td>
</tr>
<tr>
<td>Collection Object—ACL parameter</td>
<td>Metrics Included</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Interface statistics—interface</td>
<td>• Interface index</td>
</tr>
<tr>
<td></td>
<td>• Name/description</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• MTU</td>
</tr>
<tr>
<td></td>
<td>• Speed</td>
</tr>
<tr>
<td></td>
<td>• Physical address</td>
</tr>
<tr>
<td></td>
<td>• Administrative status</td>
</tr>
<tr>
<td></td>
<td>• Operational state</td>
</tr>
<tr>
<td></td>
<td>• In last change</td>
</tr>
<tr>
<td></td>
<td>• In octets</td>
</tr>
<tr>
<td></td>
<td>• In unicast packets</td>
</tr>
<tr>
<td></td>
<td>• In non-unicast packets</td>
</tr>
<tr>
<td></td>
<td>• In discards</td>
</tr>
<tr>
<td></td>
<td>• Out errors</td>
</tr>
<tr>
<td></td>
<td>• Out octets</td>
</tr>
<tr>
<td></td>
<td>• Out unicast packets</td>
</tr>
<tr>
<td></td>
<td>• Out non-unicast packets</td>
</tr>
<tr>
<td></td>
<td>• Out discards</td>
</tr>
<tr>
<td></td>
<td>• Errors</td>
</tr>
<tr>
<td>Session realm statistics—session-realm</td>
<td>• Realm name</td>
</tr>
<tr>
<td></td>
<td>• Inbound active sessions</td>
</tr>
<tr>
<td></td>
<td>• Inbound session rate (CPS)</td>
</tr>
<tr>
<td></td>
<td>• Outbound active sessions</td>
</tr>
<tr>
<td></td>
<td>• Outbound session rate (CPS)</td>
</tr>
<tr>
<td></td>
<td>• Inbound sessions admitted</td>
</tr>
<tr>
<td></td>
<td>• Inbound sessions not admitted</td>
</tr>
<tr>
<td></td>
<td>• Inbound concurrent sessions high</td>
</tr>
<tr>
<td></td>
<td>• Inbound average session rate (CPS)</td>
</tr>
<tr>
<td></td>
<td>• Outbound sessions admitted</td>
</tr>
<tr>
<td></td>
<td>• Outbound sessions not admitted</td>
</tr>
<tr>
<td></td>
<td>• Outbound concurrent sessions high</td>
</tr>
<tr>
<td></td>
<td>• Outbound average session rate (CPS)</td>
</tr>
<tr>
<td></td>
<td>• Max burst rate (in and out) (CPS)</td>
</tr>
<tr>
<td></td>
<td>• Total seizures</td>
</tr>
<tr>
<td></td>
<td>• Total answered sessions</td>
</tr>
<tr>
<td></td>
<td>• Answer/seizure ratio</td>
</tr>
<tr>
<td></td>
<td>• Average one way signaling latency</td>
</tr>
<tr>
<td></td>
<td>• Maximum one way signaling latency</td>
</tr>
<tr>
<td>ACL Group—sip-ACL</td>
<td>• Total entries</td>
</tr>
<tr>
<td></td>
<td>• Trusted</td>
</tr>
<tr>
<td></td>
<td>• Blocked</td>
</tr>
<tr>
<td></td>
<td>• ACL requests</td>
</tr>
<tr>
<td></td>
<td>• Bad messages</td>
</tr>
<tr>
<td></td>
<td>• Promotions</td>
</tr>
<tr>
<td></td>
<td>• Demotions</td>
</tr>
<tr>
<td>Collection Object—ACL parameter</td>
<td>Metrics Included</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>SIP-b2bua</td>
<td>• INVITE sessions</td>
</tr>
<tr>
<td></td>
<td>• licensed sessions</td>
</tr>
<tr>
<td></td>
<td>• subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Dialogs</td>
</tr>
<tr>
<td></td>
<td>• CallID Map</td>
</tr>
<tr>
<td></td>
<td>• Exceeded License Capacity</td>
</tr>
<tr>
<td></td>
<td>• Missing Dialogs</td>
</tr>
<tr>
<td></td>
<td>• Expired Sessions</td>
</tr>
<tr>
<td></td>
<td>• Terminated Sessions</td>
</tr>
<tr>
<td></td>
<td>• Multiple OK Drops</td>
</tr>
<tr>
<td></td>
<td>• Mapped Dialogs</td>
</tr>
<tr>
<td></td>
<td>• Map dialog forwards</td>
</tr>
<tr>
<td></td>
<td>• Map dialog miss</td>
</tr>
<tr>
<td></td>
<td>• XML bodies parsed</td>
</tr>
<tr>
<td></td>
<td>• XML bodies updated</td>
</tr>
<tr>
<td></td>
<td>• XML Bodies NAted</td>
</tr>
<tr>
<td></td>
<td>• XML errors</td>
</tr>
<tr>
<td></td>
<td>• Transaction errors</td>
</tr>
<tr>
<td></td>
<td>• Application Errors</td>
</tr>
<tr>
<td></td>
<td>• Redundancy Errors</td>
</tr>
<tr>
<td></td>
<td>• INVITE Session Rate</td>
</tr>
<tr>
<td>SIP Client Group—sip-client</td>
<td>• Total</td>
</tr>
<tr>
<td></td>
<td>• Initial</td>
</tr>
<tr>
<td></td>
<td>• Trying</td>
</tr>
<tr>
<td></td>
<td>• Calling</td>
</tr>
<tr>
<td></td>
<td>• Proceeding</td>
</tr>
<tr>
<td></td>
<td>• Cancelling</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Established</td>
</tr>
<tr>
<td></td>
<td>• Confirmed</td>
</tr>
<tr>
<td></td>
<td>• Terminated</td>
</tr>
<tr>
<td>SIP-core</td>
<td>• Response Contexts</td>
</tr>
<tr>
<td></td>
<td>• Forwarded Requests</td>
</tr>
<tr>
<td></td>
<td>• Saved Contexts</td>
</tr>
<tr>
<td></td>
<td>• Challenge Found</td>
</tr>
<tr>
<td></td>
<td>• Challenge Not Found</td>
</tr>
<tr>
<td></td>
<td>• Challenge Dropped</td>
</tr>
<tr>
<td></td>
<td>• Overload Rejects</td>
</tr>
<tr>
<td></td>
<td>• DNS Errors</td>
</tr>
<tr>
<td></td>
<td>• No Target/Route</td>
</tr>
<tr>
<td></td>
<td>• Transaction Errors</td>
</tr>
<tr>
<td></td>
<td>• Application Errors</td>
</tr>
<tr>
<td>Collection Object—ACLI parameter</td>
<td>Metrics Included</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| SIP Errors—sip-errors            | • Transport Overload  
• Core Overload  
• LS Overload  
• Connections Rejected  
• Connection Errors  
• Pending Msg Dropped  
• Suppressed Retransmit  
• Response Retransmit  
• Req Dropped  
• Invalid Requests  
• Invalid Responses  
• Invalid Messages  
• ACL Demotions  
• Transaction Timeouts  
• Duplicate Transactions  
• Transport Errors  
• Transport App Errors  
• Trans Redundancy Errs  
• Challenge Not Found  
• Challenge Dropped  
• DNS Errors  
• No Target/Route  
• XML Errors  
• Core Trans Errors  
• Core App Errors  
• Exceeded License Cap  
• Missing Dialog  
• Expired Sessions  
• Terminated Sessions  
• Multiple OK Drops  
• B2BUA Trans Errors  
• B2BUA App Errors  
• B2BUA Redundancy Errs  
• Reg Rejects  
• Reg Cache Timeouts  
• Reg w/o Contacts  
• Forced UnRegister  
• Out of Map Ports  
• NMC Rejected  
• NMC Diverted  
• No Routes Found  
• Next Hop OOS  
• Anonymous Source  
• Invalid Trunk Group  
• Inb SA Constraints  
• Outb SA Constraints  
• Inb REG SA Constraint  
• Outb REG SA Constraint  
• LS Trans Errors  
• LS App Errors  
• LS Redundancy Errors  
• Media Overload  
• SDP Offer Errors  
• SDP Answer Errors  
• Drop Media Errors  
• Invalid SDP  
• Media Failure Drops  
• Media Exp Events  
• Early Media Exp  
• Exp Media Drops  
• Media Trans Errors  
• Media App Errors |
<table>
<thead>
<tr>
<th>Collection Object—ACLI parameter</th>
<th>Metrics Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Policy Group—sip-policy</td>
<td>• Local Policy Lookups</td>
</tr>
<tr>
<td></td>
<td>• Local Policy Hits</td>
</tr>
<tr>
<td></td>
<td>• Local Policy Misses</td>
</tr>
<tr>
<td></td>
<td>• Local Policy Drops</td>
</tr>
<tr>
<td></td>
<td>• Agent Group Hits</td>
</tr>
<tr>
<td></td>
<td>• Agent Group Misses</td>
</tr>
<tr>
<td></td>
<td>• NMC Calls</td>
</tr>
<tr>
<td></td>
<td>• NMC Priority Calls</td>
</tr>
<tr>
<td></td>
<td>• NMC Rejected</td>
</tr>
<tr>
<td></td>
<td>• NMC Diverted</td>
</tr>
<tr>
<td></td>
<td>• No Routes Found</td>
</tr>
<tr>
<td></td>
<td>• Next Hop OOS</td>
</tr>
<tr>
<td></td>
<td>• Anonymous Source</td>
</tr>
<tr>
<td></td>
<td>• Invalid Trunk Group</td>
</tr>
<tr>
<td></td>
<td>• Inb SA Constraints</td>
</tr>
<tr>
<td></td>
<td>• Outb SA Constraints</td>
</tr>
<tr>
<td></td>
<td>• Inb REG SA Constraint</td>
</tr>
<tr>
<td></td>
<td>• Outb REG SA Constraint</td>
</tr>
<tr>
<td></td>
<td>• Overload Rejects</td>
</tr>
<tr>
<td>SIP Server Group—sip-server</td>
<td>• Total</td>
</tr>
<tr>
<td></td>
<td>• Initial</td>
</tr>
<tr>
<td></td>
<td>• Trying</td>
</tr>
<tr>
<td></td>
<td>• Calling</td>
</tr>
<tr>
<td></td>
<td>• Proceeding</td>
</tr>
<tr>
<td></td>
<td>• Cancelled</td>
</tr>
<tr>
<td></td>
<td>• Established</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Confirmed</td>
</tr>
<tr>
<td></td>
<td>• Terminated</td>
</tr>
<tr>
<td>SIP Sessions Group—sip-sessions</td>
<td>• Invite Sessions</td>
</tr>
<tr>
<td></td>
<td>• Licensed Sessions</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions:</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions:Initial</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions:Early</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions:Established</td>
</tr>
<tr>
<td></td>
<td>• Total Sessions:Terminated</td>
</tr>
<tr>
<td></td>
<td>• Dialogs</td>
</tr>
<tr>
<td></td>
<td>• Dialogs:Initial</td>
</tr>
<tr>
<td></td>
<td>• Dialogs:Early</td>
</tr>
<tr>
<td></td>
<td>• Dialogs:Confirmed</td>
</tr>
<tr>
<td></td>
<td>• Dialogs:Terminated</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions:Initial</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions:Pending</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions:Active</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions:Terminated</td>
</tr>
<tr>
<td>Collection Object—ACLI parameter</td>
<td>Metrics Included</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| **SIP Transport Group—sip-transport** | - Server Trans  
- Client Trans  
- Context IDs  
- Sockets  
- Sockets:Inbound Connections  
- Sockets:Outbound Connections  
- Sockets:Connection Aliases  
- Sockets:Pending Messages  
- Sockets:Connections Rejected  
- Sockets:Connection Errors  
- Sockets:Pending Msg Dropped  
- Reg Cache Updates  
- Overload Rejects  
- Supressed Retransmit  
- Response Retransmit  
- Request Dropped  
- Response Dropped  
- Invalid Requests  
- Invalid Responses  
- Invalid Messages  
- Transaction Timeouts  
- Duplicate Transactions  
- Transaction Errors  
- Application Errors  
- Redundancy Errors  
- Rejected Messages |
| **SIP Media Group—sip-media** | - Media Sessions  
- Media Pending  
- Media Refreshed  
- Media Overload  
- SDP Offer Errors  
- SDP Answer Errors  
- Drop Media Errors  
- Invalid SDP  
- Media Failure Drops  
- Media Exp Events  
- Early Media Exps  
- Exp Media Drops  
- Transaction Errors  
- Application Errors |
<table>
<thead>
<tr>
<th>Collection Object—ACL parameter</th>
<th>Metrics Included</th>
</tr>
</thead>
</table>
| **SIP Registry Group—sip-register** | • User Entries  
• Local Contacts  
• HNT Contacts  
• Non-HNT Contacts  
• AURI Entries  
• Free Map Ports  
• Used Map Ports  
• Transactions  
• Forwards  
• Refreshes  
• Updates Sent  
• Challenges  
• ReJECTs  
• Timeouts  
• Fwd Postponed  
• Fwd Rejects  
• Refr Extension  
• Refresh Extended  
• Reg Cache Hits  
• Reg Cache Misses  
• Route to Registrar  
• Reg w/o Contacts  
• Forced UnRegister  
• Out of Map Ports  
• Transaction Errors  
• Application Errors  
• Redundancy Errors  
• Surrogate Regs  
• Surrogate Sent  
• Surrogate Reject  
• Surrogate Timeout |
| **System Group—system** | • Current signaling sessions  
• Current signaling session rate (CPS)  
• CAM utilization NAT  
• CAM utilization ARP  
• License capacity  
• Cached SIP Local Contact Registrations  
• Current H323 Number of Registrations |
| **SIP Invite Group—sip-invites** | • Timestamp  
• Message/Event  
• Server Totals  
• Client Totals |
| **H.323 Statistics (h323-stats)** | • Incoming Calls  
• Outgoing Calls  
• Connected Calls  
• Incoming Channels  
• Outgoing Channels  
• Contexts  
• Queued Messages  
• TPKT Channels  
• UDP Channels |
<table>
<thead>
<tr>
<th>Collection Object—ACL parameter</th>
<th>Metrics Included</th>
</tr>
</thead>
</table>
| Combined session agent statistics (session-agent) | • Hostname  
• System Type  
• Status  
• Inbound Active Sessions  
• Inbound Session Rate  
• Outbound Active Sessions  
• Outbound Session Rate  
• Inbound Sessions Admitted  
• Inbound Sessions Not Admitted  
• Inbound Concurrent Sessions High  
• Inbound Average Session Rate  
• Outbound Sessions Admitted  
• Outbound Sessions Not Admitted  
• Outbound Concurrent Sessions High  
• Outbound Average Sessions Rate  
• Max Burst Rate  
• Total Seizures  
• Total Answered Sessions  
• Answer/Seizure Ratio  
• Average One-Way Signaling Latency  
• Maximum One-Way Signaling Latency |
| Environmental temperature statistics—temperature | • Slot  
• Sensor Type  
• Description  
• Temperature (Celsius)  
• State |
| ENUM Group—enum-stats | • ENUM Agent  
• Transactions  
• Queries Sent  
• Queries Sent:Success  
• Queries Sent:NoResults  
• Queries Sent:Timeout  
• Queries Sent:Failure  
• Resolvers  
• Cached Results  
• Cached NoResult  
• Cache Hits (Results)  
• Cache Hits (NoResult)  
• Cache Drops |
ACL Instructions and Examples

This section shows you how to configure HDR. You need to set up:

- The collection configuration to govern default sample and push intervals, start and end times for collection
- The group settings configuration that tells the Net-Net SBC what groups of records to collect, when to start and stop collecting them, and how often to sample for that group
- Push receivers that take the records the Net-Net SBC sends

All HDR parameters are RTC-supported, so you can save and activate your configuration for them to take effect. Typing `reset collection` is required to actually execute a newly configured collection after a change.

Accessing the HDR Configuration Parameters

You access the parameters that enable and support HDR using the CLI system path.

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ACMEPACKET# configure terminal

2. Type `system` and press <Enter>.
   
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#

3. Type `collect` and press <Enter>.
   
   ACMEPACKET(system)# collect
   ACMEPACKET(collect)#

   From here, you can type a question mark (?) to see individual parameters for the configuration.
You access the collection configuration through the ACLI `system-configuration` menu. Once in the collection configuration, you can establish the global settings for HDR collection.

Note that the push receiver is configured in a sub-configuration; refer to the Push Receiver Settings (153) for details.

**To configure global settings for HDR support:**

1. **boot-state**—Set this parameter to `enabled` to start group collection, or to `disabled` (default) to prevent the Net-Net SBC from collecting HDR statistics. This parameter does not go into effect until the system is rebooted. You can also use the ACLI request `reset collect` command to start collection; using this command, you can reset collection for all groups, or for one specified group.
2. **sample-interval**—Enter the time in minutes for how often you want the Net-Net SBC to sample data records. The maximum value for this parameter is 120 minutes (2 hours).
3. **push-interval**—Enter the time in minutes for how often you want the Net-Net SBC to send collected records to push receiver(s). The default is 15.
4. **start-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to start HDR collection; this time is either `now` (default) or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second.
5. **end-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to finish HDR collection; this time is either `never` (default) or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.

You can configure multiple collection groups on your Net-Net SBC; the names of these groups appear in the Group Record Types (143) section above. Collection group settings are accessible through the collection configuration.

Note that the sample collection interval, start time, and end time you set here override the ones established in the global collection settings. The largest value you can enter for an group’s sample collection must be smaller than the global push interval value. Default group-settings are inherreted from the collection configuration element. If you do not configure any group-settings, all groups will be collected.

**To configure collection group settings:**

1. Access the collection group (`group-settings`) configuration by way of the collection configuration. Once
   ```
   ACMEPACKET(system-config)# collect
   ACMEPACKET(collect)# group-settings
   ```
2. **group-name**—Enter the group name corresponding to the records that you want to collect; there are 21 possible groups for which the Net-Net SBC can collect data. The system group name is the default for this parameter; the other possible names to which you can refer are listed in the Group Record Types (143) table above.
3. **boot-state**—To turn HDR for this collection group on, set this parameter to `enabled`. If the collect configuration element’s boot-state is set to disabled, this group-settings configuration element is ignored.

4. **sample-interval**—Enter the time in minutes for how often you want the Net-Net SBC to sample data records for the specified group. The maximum value for this parameter is 120 minutes (2 hours).

5. **start-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to start collecting records for this group; this time is either now or a time in the future. Your entry must be in the format `yyyy-mm-dd hh:mm:ss`, where `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.

6. **end-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to stop collecting records for this group; this time is either never or a time in the future. Your entry must be in the format `yyyy-mm-dd hh:mm:ss`, where `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.

---

### Push Receiver Settings

You can configure multiple servers to receive the records that the Net-Net SBC. Push receiver settings are accessible through the collection configuration. To provide added security, you can transfer the HDR record files using SFTP as well as FTP. Note that public key authentication is not available for this feature. Instead, the Net-Net SBC uses password authentication.

If you configure more than one server, then the Net-Net SBC sends data to all of the servers. If one server fails, the Net-Net SBC generates an SNMP trap. In terms of clearing data, this means that if there are four servers configure and the Net-Net SBC successfully pushes data to three of them, then it will clear the data.

**To configure servers to act as push receivers for HDR data:**

1. Access the collection group (**group-settings**) configuration by way of the collection configuration. Once
   ```
   ACMEPACKET(system-config)# collect
   ACMEPACKET(collect)# push-receiver
   ```

2. **address**—Enter the IP address of the push receiver (server) to which you want records sent. The default for this parameter is `0.0.0.0`.

3. **username**—Enter the username that the Net-Net SBC will use when it tries to send records to this push server using FTP. There is no default for this parameter.

4. **password**—Enter the password (corresponding to the username) that the Net-Net SBC will use when it tries to send records to this push server using FTP. There is no default for this parameter.

   **Note:** Passwords appear in clear text and are viewable by anyone logged into the Net-Net SBC.

5. **data-store**—Enter the directory on the push receiver where you want collected data placed. There is no default for this parameter.

6. **protocol**—Valid values for this parameter are `FTP` (default) and `SFTP`. You only need to set this parameter if you want to use SFTP to send HDR collection record files.
Controlling HDR from the Command Line

For added ease-of-use, you can stop and start record collection from the command line in Superuser Mode. You can stop and start record collection for the entire HDR process, or you can specify a group name for which you want to stop and start collection.

When you stop collection using this command, it will not restart it using this command.

**To start record collection from the command line:**

1. In Superuser mode, type the ACLI `start collection all` command. If you press <Enter> at this point, the Net-Net SBC will start all record collection. If you enter a specify a group-name instead of the `all` argument and press <Enter>, collection for that record group only will be started.

   ACMEPACKET# start collection voltage

**To stop record collection from the command line:**

1. In Superuser mode, type the ACLI `stop collection all` command. If you press <Enter> at this point, the Net-Net SBC will stop all record collection. If you enter a specify a group-name instead of the `all` argument and press <Enter>, collection for that record group only will be stopped.

   ACMEPACKET# stop collection voltage

**To restart record collection from the command line:**

1. In Superuser mode, type the ACLI `reset collection` command. If you press <Enter> at this point, the Net-Net SBC will restart all record collection.

   ACMEPACKET# reset collection

   Resetting a collection lets the current sample interval and push interval cycle complete, and then reads and uses the sample interval and push interval times from the collect configuration element.

**To delete all collection data files resident on the Net-Net SBC:**

1. In Superuser mode, type the ACLI `delete collection` command. If you press <Enter> at this point, the Net-Net SBC will delete all record collections.

   ACMEPACKET# delete collection

**To display the status of collection groups and push servers:**

1. In Superuser mode, type the ACLI `show collection` command to view groups currently collected, next push time and next push interval. Also, the configured collectors and their states are displayed. If you press <Enter> at this point, the Net-Net SBC will show record collection status.

   ACMEPACKET# show collection

   Collector is currently collecting on:
   Group   Boot-State   Start Time   End Time
   fan     disabled     now           never

   Next Push Scheduled for: 2008-01-11-11:12:06
   Subsequent Push Interval: 15 minutes

   Registered push receivers are:
### CPU Core Index Mapping

The following table lists CPU CoreID values seen in HDR and SNMP statistics.

<table>
<thead>
<tr>
<th>CPU and Core value</th>
<th>Core ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu 0 core 0</td>
<td>CoreID 0</td>
</tr>
<tr>
<td>cpu 0 core 1</td>
<td>CoreID 1</td>
</tr>
<tr>
<td>cpu 1 core 0</td>
<td>CoreID 256</td>
</tr>
<tr>
<td>cpu 1 core 1</td>
<td>CoreID 257</td>
</tr>
<tr>
<td>cpu 2 core 0</td>
<td>CoreID 512</td>
</tr>
<tr>
<td>cpu 2 core 1</td>
<td>CoreID 513</td>
</tr>
<tr>
<td>cpu 3 core 0</td>
<td>CoreID 768</td>
</tr>
<tr>
<td>cpu 3 core 1</td>
<td>CoreID 769</td>
</tr>
<tr>
<td>cpu 4 core 0</td>
<td>CoreID 1024</td>
</tr>
<tr>
<td>cpu 4 core 1</td>
<td>CoreID 1025</td>
</tr>
</tbody>
</table>

### NTP Features

NTP is a fully RTC-enabled service on the Net-Net 9200.

### NTP Application Debugging

The commands listed in this section are used to debug NTP-application level issues. They show operating status for the NTP daemons, one of which runs on each core of the Net-Net 9200.

#### show ntp status

The `show ntp status` command displays information about the synchronization and running status of the specified NTP daemon. If no argument is supplied, the command displays NTPD status for the master active core. This includes the state of the NTP daemon, and the server to which it’s synced. For example:

```
ACMEPACKET# show ntp status

NTPD 0.0.0                                     TUE NOV  19:18:08  2007
NTPD NTPD active server is running.
NTP synchronized to server at: 172.30.0.25
```

If you include a core argument, the ACLI displays NTPD status on that core. A core is specified by `<slot> <CPU> <core>`, separated by spaces. For example:

```
ACMEPACKET# show ntp status 0 1 0

NTPD 0.1.0                                     TUE NOV  19:18:58  2007
NTPD NTPD client is running.
NTP synchronization in progress...
```
**show ntp server**

The **show ntp server** displays the state of each NTP core daemon you query. If you type this command without any arguments, the ACLI displays information about the master active core’s NTP daemon. The ACLI displays the statistics listed in the following table for each NTP daemon.

<table>
<thead>
<tr>
<th>Display Column</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **server**     | Lists the NTP servers configured on the Net-Net 9200 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, 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. |

For example:

```
ACMEPACKET# show ntp server

NTPD 0.0.0                                      TUE NOV 19:23:57  2007
NTPD NTPD active server is running.
peer                  st  poll   reach     delay       offset       disp
----------------------- --  ----  ------    --------    --------    -----  
*172.30.0.25             2   512      37    0.015625    0.005153    0.046539
```

If you include a core argument, the ACLI displays NTPD status on that core. A core is specified by <slot> <CPU> <core>, separated by spaces. For example:

```
ACMEPACKET# show ntp server 0 1 1

NTPD 0.1.1                                      TUE NOV 19:24:08  2007
NTPD NTPD client is running.
peer                  st  poll   reach     delay       offset       disp
----------------------- --  ----  ------    --------    --------    -----  
=169.254.176.0           3   512      37    0.015625  -0.016335     0.52643
```
NTP System Level Debugging

The following commands display NTP system statistics and counters. This information reflects how NTP daemons interact with each other and the system processes that support the Net-Net 9200’s operation.

**show task ntp**

This command displays the statistics for each NTP daemon (NTPD) running on every core. For example:

```
ACMEPACKET# show task ntp
19:21:05-137 (ntpd@0.0.0) ID=e2560ec0
Task Status        Recent        LifeTime
Services           17            18            18
Messages           4             4             4
Alloc Buffers      50            52            52
Free Buffers       2             2             2
Transactions       0             0             0
Timed Objects      19            21            21
TOQ Entries        2             2             2
Operations         0             0             0
Messages Received  -             -             -
Messages Sent      -             -             -
Partial Message    -             -             -
Part Msg Expired   -             -             -
Part Msg Dropped   -             -             -
Timed Events       -             -             -
Alarms             -             -             -
System Logs        -             -             -
Process Logs       -             -             -
Remote Logs        -             -             -
Load Rate          0.0%          0.26%        0.1%
```

You can also use the `show task ntp 2.0.1` syntax, for example, to query a specific core.

**show amp ntpd**

This command shows AMP statistics for the NTP daemon (NTPD) running on each core. For example:

```
ACMEPACKET# show amp ntpd
19:22:09-100 (ntpd@0.0.0) ID=e2560ec0
Protocol       Recent  Total  PerMax  Recent  Total  PerMax
               ------  -------  ------  -------  -------  ------
Total          2       7       3       1       7       3
MAN            0       0       0       0       0       0
CLIP           2       7       3       1       6       3
```

You can also use the `show amp ntpd x.0.x` syntax to query a specific core.
Network Management

Commands discussed in this chapter primarily concern OSI model layers 2-4 information on the Net-Net 9200.

Network Connections

The commands listed in this section are used to view physical interfaces and logical network connections as currently in use on the Net-Net 9200.

**show interfaces**

The `show interfaces` command is used to list all configured Ethernet interfaces, their IP settings, and ethernet statistics. Configured media interfaces are displayed by their phy-interface configuration element name followed by the hardware location in parenthesis). The following is an abbreviated display of this show command:

```
ACMEPACKET# show interfaces
eth (unit number 2, MIU1):
  Flags: UP
  Type: ETHERNET_CSMACD
  inet: 172.30.92.92
Broadcast address: 172.30.255.255
Netmask: 0xFFFF0000 Subnetmask: 0xFFFF0000
Ethernet address is 00:08:25:02:65:b2
Metric is 0
Maximum Transfer Unit size is 1500
47046434 octets received
49199787 octets sent
52427 unicast packets received
977093 unicast packets sent
205814 non-unicast packets received
2 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
private(media slot 0 port 0):
  Flags: UP
  Type: ETHERNET_CSMACD (COPPER)
  Admin State: enabled
  Auto Negotiation: enabled
  Duplex Mode: HALF
  Force Speed Selection: 100 Mbps
  inet: 192.168.0.77 vlan: 0
Broadcast address: 192.168.255.255
Netmask: 0xFFFF0000
Gateway: 192.168.0.10
Ethernet address is 20:68:02:25:08:04
```
Virtual Ethernet address is 00:00:25:fe:1c:00
Metric is 0
Maximum Transfer Unit size is 1500
3552470 octets received
192 octets sent
54537 unicast packets received
3 unicast packets sent
54036 non-unicast packets received
3 non-unicast packets sent
1 incoming packets discarded
0 outgoing packets discarded
0 incoming errors
0 outgoing errors
0 unknown protos
0 collisions; 0 dropped

**show ip connections**

In order to quickly view all active network connections on the Net-Net 9200, the **show ip connections** command is used. This command first displays a list of the network connections on active cards. The command next lists all network connections on standby cards. For example:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>172.30.92.96:23</td>
<td>10.0.200.204:1749</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:21</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:22</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:23</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:41</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:111</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:6666</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>172.30.92.96:8080</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:111</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:123</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.30.92.96:161</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.30.92.96:1125</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.30.92.96:1812</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.16.0.77:5060</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.0.77:5060</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
</tbody>
</table>

**Internet Connections on Standby (including servers)**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:21</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:22</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:23</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:41</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:111</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:6666</td>
<td>0.0.0.0:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:111</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:123</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.30.92.94:161</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>172.30.92.94:1051</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
</tbody>
</table>
show ip statistics

The `show ip statistics` command allows you to display a list of IP statistics including the number of ACL denials and the last IP address denied. For example:

```
ACMEPACKET# show ip statistics
system-acl statistics
  acl-denials          0
  last-srcip-denied         0.0.0.0
```

ARP Statistics

The commands listed in this section are used to view ARP table statistics and related information.

**show arp commands**

The `show arp` commands are used to display ARP tables, ARP table statistics for media interfaces, and management routes. The `show arp` command usage is as follows:

```
ACMEPACKET# show arp [statistics-all | statistics-by-interface | table-all | table-by-interface | info] <slot> <port>
```

**show arp statistics-by-interface**

This `show` command displays the counts and statistics for a specified media interface’s ARP table. Information displayed includes receive, transmit, and CAM statistics. This command is entered as:

```
ACMEPACKET# show arp statistics <slot> <port>
<slot>: 0,1
<port>: 0,1,2,3
```

For example:

```
Manifestoo# show arp statistics-by-interface 0 0
```

```
Interface: 0/0

-- Receive --
  Add intf:          1, Error:           0
  Delete intf:          0, Error:           0
  Flush intf:          0, Error:           0
  Arp enable:          0, Error:           0
  Arp disable:          0, Error:           0
  Add dynamic:          0, Error:           0
  Add static:          0, Error:           0
  Delete dynamic:          0, Error:           0
  Delete static:          0, Error:           0
  Info Req:          0, Error:           0
  Pendl:          0, Error:           0, Drop:          0
  Request:      57288, Update:          0, Drop:      57288
  Reply:      2, Update:          1, Drop:          0
  Network:      57289, Error:          0
  ARP:           0
  Subnet:           0
  Intf:           0
  IP:           0
```
show arp statistics-all

This `show` command works similarly to the `show arp statistics-by-interface` command except that it does not take any arguments, and it displays statistics for all configured media interfaces.

```
ACMEPACKET# show arp statistics-all

ARPM STATUS: ACTIVE

Interface: ALL

-- Receive --

Add intf: 2, Error: 0
Delete intf: 0, Error: 0
Flush intf: 0, Error: 0
Arp enable: 0, Error: 0
Arp disable: 0, Error: 0
Add dynamic: 0, Error: 0
Add static: 0, Error: 0
Delete dynamic: 0, Error: 0
Delete static: 0, Error: 0
Info Req: 1, Error: 0
Pend: 0, Error: 0, Drop: 0
Request: 114541, Update: 0, Drop: 114541
Reply: 2, Update: 2, Drop: 0
Network: 120033, Error: 5490
ARP: 0
Subnet: 5490
Intf: 0
IP: 0
Operation: 0

-- Transmit --

Request: 10, Error: 0
Reply: 0, Error: 0
Pend: 0, Error: 0
```
show arp table-all

This `show` command displays the complete arp table for management and media interfaces, including ARP table entry type, MAC address, IP address, interface (slot/port) and VLAN, time added to the table for each entry, and Secondary gateways. For example:

```
Manifestoo# show arp table-all
--- Management ARP Table ---

destination      gateway            flags  Refcnt  Use           Interface
---------------------------------------------------------------------
172.30.0.1       00:0f:23:4a:d8:80  33686533  2       0             eth2
172.30.0.25      00:11:2f:74:88:5f  33686533  1       852551        eth2
---------------------------------------------------------------------
--- Media and Signaling ARP Table ---

Total ARP Entries = 6
-----------------------
Intf  VLAN     IP-Address             MAC          time-stamp   type
active-count
0/3    0   172.016.000.010     00:15:F2:4C:FC:F7  1193227957  dynamic
1
0/0    0   192.168.000.010     00:0E:0C:9B:FE:B5  1193227957  dynamic
1

Special Entries:

0/3    0   000.000.000.000     00:15:F2:4C:FC:F7  1193170829  gateway
0/3    0   172.016.000.000     00:00:00:00:00:00  1193170829  network
0/0    0   000.000.000.000     00:0E:0C:9B:FE:B5  1193170829  gateway
0/0    0   192.168.000.000     00:00:00:00:00:00  1193170829  network

Gateway Status:

Intf  VLAN     IP-Address             MAC          time-stamp hb status
0/3    0   172.016.000.010     00:15:F2:4C:FC:F7  1193227957  reachable
0/0    0   192.168.000.010     00:0E:0C:9B:FE:B5  1193227957  reachable

Secondary Gateway Status:
**show arp table-by-interface**

By adding a slot and port argument to the `show arp table` command, the ACLI displays the arp table for a given media interface. This table lists ARP table entry type, MAC address, IP address, interface (slot/port) and VLAN, and time added to the table for each entry. This command is entered as:

```
ACMEPACKET# show arp table-by-interface <slot> <port>
```

For example:

```
ACMEPACKET# show arp table 0 0
```

```
Total ARP Entries = 9
```

```
<table>
<thead>
<tr>
<th>Intf</th>
<th>VLAN</th>
<th>IP-Address</th>
<th>MAC</th>
<th>time-stamp</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0</td>
<td>0</td>
<td>172.016.000.199</td>
<td>00:0B:82:08:1E:A9</td>
<td>1152879227</td>
<td>dynamic</td>
</tr>
<tr>
<td>0/0</td>
<td>0</td>
<td>172.016.000.099</td>
<td>00:14:BF:B3:41:4E</td>
<td>1152878833</td>
<td>dynamic</td>
</tr>
<tr>
<td>0/0</td>
<td>0</td>
<td>172.016.000.010</td>
<td>00:0E:0C:37:B4:7A</td>
<td>1152878941</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

**Special Entries:**

```
0/0  0  000.000.000.000  00:0E:0C:37:B4:7A  1152837989  gateway
0/0  0  172.016.000.000  00:00:00:00:00:00  1152837989  network
```

**Gateway Status:**

```
<table>
<thead>
<tr>
<th>Intf</th>
<th>VLAN</th>
<th>IP-Address</th>
<th>MAC</th>
<th>time-stamp</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0</td>
<td>0</td>
<td>172.016.000.010</td>
<td>00:0E:0C:37:B4:7A</td>
<td>1152878941</td>
<td>reachable</td>
</tr>
</tbody>
</table>
```

**show arp info**

This `show` command displays the ARP table statistics. This command does not take a slot and port argument. For Example:

```
ACMEPACKET# show arp info
```

```
-- ARP table info --
Maximum number of entries : 4096
Number of used entries    : 9
Length of search key      : 1 (x 64 bits)
First search entry address: 0x1f000
Length of data entry      : 2 (x 64 bits)
First data entry address  : 0x3e000
Enable aging              : 0
Enable policing            : 0
```

**show arp standby**

This `show` command displays ARP table statistics for the task you identify that exists on the standby card. For example:

```
ACMEPACKET# show arp standby info
```

```
Retrieving info from standby NPU [3.0.0]
```

```
-- ARP table info --
```

164 Net-Net 9000 Maintenance and Troubleshooting Guide  Version S-D7.1.0

Proprietary & Confidential
Maximum number of entries : 4096
Number of used entries     : 4
Length of search key       : 1 (x 64 bits)
First search entry address : 0x1f000
Length of data entry       : 2 (x 64 bits)
First data entry address   : 0x3e000
Enable aging               : 0
Enable policing            : 0

Manual ARP Table
Changes

You can manually modify entries in the ARP table with the add, delete, and check commands. If your deployment does not use VLANs, set all VLAN arguments to 0.

check arp

The check arp command sends a test message to the indicated physical interface. The check arp command usage is as follows:

ACMEPACKET# check arp <slot> <port> <vlan> <ip>
<slot>: 0, 1
<port>: 0, 1, 2, 3
<vlan>: 0, 1, 2, etc
<ip>: IP address in the form x.x.x.x

For example:

ACMEPACKET# check arp 1 0 0 172.16.0.123
Invalid arp request

add arp

The add arp command adds an ARP entry to 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 add arp command usage is as follows:

ACMEPACKET# add arp <slot> <port> <vlan> <ip> <mac>
<slot>: 0, 1
<port>: 0, 1, 2, 3
<vlan>: 0, 1, 2, etc
<ip>: IP address in the form x.x.x.x
<mac>: MAC address in the form x:x:x:x:x:x

For example:

ACMEPACKET# add arp 0 0 0 172.16.0.102 ab:cd:ef:01:23:45

delete arp

The delete arp command removes ARP entries from the ARP table. You only need to identify the IP address, VLAN tag, and slot and port pair to be removed. The delete arp command usage is as follows:

ACMEPACKET# delete arp <slot> <port> <vlan> <ip>
<slot>: 0, 1
<port>: 0, 1, 2, 3
<vlan>: 0, 1, 2, etc
<ip>: IP address in the form x.x.x.x

For example:

ACMEPACKET# delete arp 0 0 0 172.16.0.102
Other ARP Commands
You can reset the accumulated ARP statistics with the `reset arp statistics` command. For example:

```
ACMEPACKET# reset arp statistics
Clearing arp stats
```

ACL Statistics
The commands listed in this section are used to view ACL table statistics and related information.

Show ACL commands
The `show acl` commands are used to display ACL entries in the ACL table for media interfaces. The `show acl` command usage is as follows:

```
ACMEPACKET# show acl [all | denied | info | ip | trusted | untrusted]
```

`show acl denied`
The `show acl denied` command displays the list of denied ACL entries. Once an endpoint is added to the denied list, it appears in this show command’s output. Information for each entry includes:
- Connecting media port, slot, and VLAN tag
- Source IP Address, bit mask, port, and port mask
- Destination IP address, bit mask, port, and port mask
- Protocol
- ACL entry as static or dynamic
- ACL entry index

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
```

`show acl info`
The `show acl info` command displays ACL table statistics. For each type of ACL entry, denied, trusted, media, or untrusted, statistics are given for the number of active entries, % utilization of total entries, and max entries. In addition the count and percentage of CAM space used is displayed. Finally, counts are displayed for allocation failures to do ACL constraints. The following show acl info command is for a Net-Net 9200 with a 64K CAM installed:

```
ACMEPACKET# show acl info
Access Control List Statistics:
<table>
<thead>
<tr>
<th># of entries</th>
<th>% utilization</th>
<th>Max Entries</th>
</tr>
</thead>
</table>
Denied     | 0             | 0.000%      | 14000       |
Trusted    | 5             | 0.031%      | 16000       |
Media      | 33479         | *           | *           |
Untrusted  | 1             | 99.976%     | 33488       |
---------------------------------------------------------------
Total CAM space used = 33485 of 63488 (47.258% free)
* = Media and Untrusted are shared
```
The following show acl info command is for a Net-Net 9200 with a 256K CAM installed:

```
ACMEPACKET# show acl info
```

```
May 13 13:57:20.643

Access Control List Statistics:
<table>
<thead>
<tr>
<th># of entries</th>
<th>% utilization</th>
<th>Max Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denied</td>
<td>2</td>
<td>0.006%</td>
</tr>
<tr>
<td>Trusted</td>
<td>8</td>
<td>0.007%</td>
</tr>
<tr>
<td>Media</td>
<td>0</td>
<td>*</td>
</tr>
<tr>
<td>Untrusted</td>
<td>4</td>
<td>0.004%</td>
</tr>
</tbody>
</table>

Total CAM space used = 14 of 253952 (99.994% free)
* = Media and Untrusted are shared

```

```
show acl ip

You can filter the output of show acl all based on IP address. This command is useful if you want to check the ACL properties of a specific IP address. For example:

```
ACMEPACKET# show acl ip 192.168.0.123
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
1/0:0 0.0.0.0 192.168.0.123:5060 UDP static 2 0 0
1/0:0 192.168.0.10:53 192.168.0.123 UDP static 4 0 0

Total number of untrusted entries = 3
```
**show acl trusted**

The `show acl trusted` command displays the list of trusted ACL entries. Once an endpoint is added to the trusted list, it appears in this show command's output. Information for each entry includes:

- Connecting media port, slot, and VLAN tag
- Source IP Address, bit mask, port, and port mask
- Destination IP address, bit mask, port, and port mask
- Protocol
- ACL entry as static or dynamic
- ACL entry index
- Packets received
- Packets dropped

For example:

```
Manifestoo# show acl trusted
trusted entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index  recv
0/0:0   0.0.0.0                     192.168.0.77             ICMP static  1    0
0/3:0   0.0.0.0                     172.16.0.77              ICMP static  2    0
```

Total number of trusted entries = 2

**show acl untrusted**

The `show acl untrusted` command displays the list of untrusted ACL entries. Once an endpoint is added to the untrusted list, it appears in this show command’s output. Information for each entry includes:

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

For example:

```
Manifestoo# show acl untrusted
untrusted entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
0/0:0   0.0.0.0                     192.168.0.77:5060        UDP  static  3
0/3:0   0.0.0.0                     172.16.0.77:5060         UDP  static  4
```

Total number of untrusted entries = 2

**show acl all**

The `show acl all` command displays the concatenation of all other `show acl` commands and a final summary.
NAT Statistics

The commands listed in this section are used to view NAT statistics for media interfaces.

Show NAT commands

The show nat commands are used to display the NAT table for the Net-Net system. You can query a NAT table entry by its address, NAT table index, or display a shortened tabular form of the NAT table. The show nat command usage is as follows:

```
show nat [by-addr | by-index | in-tabular | info | statistics]
```

**show nat by-addr**

The show nat by-addr command displays a tabular output of the NAT table for a given IP address. The IP address that you supply is used to match for the source IP, destination IP, translated source IP, or translated destination IP addresses. Information for each entry includes:

- NAT table index number
- Protocol of this NAT flow
- Slot / Port : Vlan ID on source side of the flow
- Source IP address and port
- Destination IP address and port

The show nat by-addr command usage is as follows:

```
ACMEPACKET# show nat by-addr <IP Address>
```

For example:

```
ACMEPACKET# show nat by-addr 172.16.0.123
```

```
Index Proto Intf:Vlan Src IP:Port            Dst IP:Port
----------------- ----------------- --------------- ---------------
  1       6     I=0/0:0  172.16.0.10:23           172.16.0.123:0
       O=1/0:0  192.168.0.123:23         192.168.0.10:0
  2       6     I=1/0:0  192.168.0.0:0            192.168.0.123:23
       O=0/0:0  172.16.0.123:0           172.16.0.10:23
  6       6     I=0/0:0  0.0.0.0:0                172.16.0.123:0
  7       6     I=0/0:0  0.0.0.0:0                172.16.0.123:1
       O=0/0:0  0.0.0.0:0                172.16.0.123:1
  8      17     I=0/0:0  0.0.0.0:0                172.16.0.123:5060
```

**show nat by-index**

The show nat by-index command displays full statistics for the NAT table entries specified in a supplied entry index 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. Information for each entry includes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA_flow_key</td>
<td>Source IP address key used for matching in the look-up process.</td>
</tr>
<tr>
<td>DA_flow_key</td>
<td>Destination IP address key used for matching in the look-up process.</td>
</tr>
<tr>
<td>SP_flow_key</td>
<td>Source port used for matching in the look-up process.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DP_flow_key</td>
<td>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>
<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 = TCP/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=HIP</td>
</tr>
<tr>
<td></td>
<td>• bit 11 - 1=TCU (transcoding)</td>
</tr>
<tr>
<td></td>
<td>• bit 12 - 1 Diagnostics (testing only)</td>
</tr>
<tr>
<td></td>
<td>• bit 13 - 1 NAT ALG packets</td>
</tr>
<tr>
<td>optional_data</td>
<td>This value specifies DSP device ID or session ID of transcoded traffic.</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>
</tbody>
</table>
The show nat by-index command usage is as follows:

```
ACMEPACKET# show nat by-index <index range start> <index range finish>
```

For example:

```
ACMEPACKET# show nat by-index 4 4
```

```
NAT table search address 4, xsmAddr 62558 :
Flow type: Fully qualified flow
SA_flow_key : 192.168.000.010       SA_prefix : 32
DA_flow_key : 192.168.000.123       DA_prefix : 32
SP_flow_key : 53                    SP_prefix : 16
DP_flow_key : 0                     DP_prefix : 0
VLAN_flow_key : 0
Protocol_flow_key : 17
Ingress_flow_key : 1
Ingress Slot : 1
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 : 1
Egress Slot : 1
Egress Port : 0
flow_action : 0X81
optional_data : 6000
FPGA_handle : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry : 0
host_table_index : 4
Switch ID : 0x00000416
average_rate : 0
weight : 0x1b
init_flow_guard : 4294967295
inact_flow_guard : 4294967295
max_flow_guard : 4294967295
```

**show nat in-tabular**

The `show nat in-tabular` command displays a tabular output of the NAT table for a supplied entry index range. Information for each entry includes:

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

```
init_flow_guard : 4294967295
inact_flow_guard : 4294967295
max_flow_guard : 4294967295
```
• NAT table index number
• Protocol of this NAT flow
• Slot / Port : Vlan ID on source side of the flow
• Source IP address and port
• Destination IP address and port

The show nat by-addr command usage is as follows:

```
ACMEPACKET# show nat in-tabular <index-start> <index-end>
```

For example:

```
ACMEPACKET# show nat in-tabular 1 5
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Proto</th>
<th>Intf:Vlan</th>
<th>Src IP:Port</th>
<th>Dst IP:Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>I=1/0:0</td>
<td>0.0.0.0:0</td>
<td>192.168.0.123:0</td>
</tr>
<tr>
<td>2</td>
<td>17</td>
<td>I=1/0:0</td>
<td>0.0.0.0:0</td>
<td>192.168.0.123:5060</td>
</tr>
<tr>
<td>3</td>
<td>17</td>
<td>I=0/0:0</td>
<td>0.0.0.0:0</td>
<td>172.16.0.123:5060</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>I=1/0:0</td>
<td>192.168.0.10:53</td>
<td>192.168.0.123:0</td>
</tr>
</tbody>
</table>

**show nat info**

The `show nat info` command displays NAT table information. For example:

```
ACMEPACKET# show nat info
```

```
-- NAT table info --
Maximum number of entries : 63488
Number of used entries     : 3
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

-- TM info --
Flow ID list size     : 98303
Number of used flows  : 100
Number of free flows  : 98203
```

**show nat standby**

The `show nat standby` command displays standby NAT statistics for the specified NAT task stored on the Net-Net SBC. For example:

```
ACMEPACKET# show nat standby info
```

```
Mar 25 13:02:52.946
Retrieving info from standby NPU [3.0.0]

-- NAT table info --
Maximum number of entries : 63488
Number of used entries     : 16
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

-- TM info --
Flow ID list size           : 98303
Number of used flows        : 98
Number of free flows        : 98205

**show nat statistics**

The **show nat statistics** command displays NAT table transaction statistics. For example:

```
ACMEPACKET# show nat statistics
```

**NATM Status:** ACTIVE

**API Stats --**

<table>
<thead>
<tr>
<th>Command</th>
<th>RX-Total</th>
<th>RX-OK</th>
<th>Rx-Error</th>
<th>TX-OK</th>
<th>TX-Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nat Add</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Nat Delete</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nat Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nat Update-Add</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nat Update-Delete</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nat Latch</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Flow Gd Notify</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nat Info</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stats Get</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Stats Clear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Diag Enable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Diag Disable</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Arp Add</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Arp Delete</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**CAM Stats --**

<table>
<thead>
<tr>
<th>Errors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add errors</td>
<td>0</td>
</tr>
<tr>
<td>Delete errors</td>
<td>0</td>
</tr>
<tr>
<td>Update errors</td>
<td>0</td>
</tr>
<tr>
<td>Convert errors</td>
<td>0</td>
</tr>
<tr>
<td>Record errors</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate errors</td>
<td>0</td>
</tr>
<tr>
<td>Number of shuffles</td>
<td>0</td>
</tr>
</tbody>
</table>

**Flowguard Stats --**

<table>
<thead>
<tr>
<th>Errors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add errors</td>
<td>0</td>
</tr>
<tr>
<td>Delete errors</td>
<td>0</td>
</tr>
<tr>
<td>Reserve errors</td>
<td>0</td>
</tr>
<tr>
<td>Invalid NAT IDs</td>
<td>0</td>
</tr>
<tr>
<td>Find CAM errors</td>
<td>0</td>
</tr>
</tbody>
</table>

**show nat table**

The **show nat table** command expands on the **show nat in-tabular** command by displaying the written-out protocol and weight of each NAT entry. In addition, you can search for entries in the nat table by specifying source address (xxx.xxx.xxx.xxx), source port (xxxxx), destination address(xxx.xxx.xxx.xxx), or destination port (xxxxx).
The show nat table command usage is as follows:

\texttt{show nat table [tabular | by-src-addr | by-src-port | by-dest-addr | by-dest-port]}

For example:

\texttt{ACMEPACKET# show nat table tabular}

\begin{verbatim}
Oct 14 11:49:19.661
Index Proto Weight Intf:Vlan Src IP:Port Dst IP:Port
------------------------------------------------------------------
  1   TCP   0     l =0/0:0  0.0.0.0:0  172.16.0.200:41
  2   ICMP  0     l =0/0:0  0.0.0.0:0  172.16.0.200:0
  3   TCP   0     l =0/0:0  0.0.0.0:0  172.16.0.200:23
  4   UDP   0     l =1/0:0  0.0.0.0:0  192.168.0.200:506
\end{verbatim}

\textbf{Other NAT Commands}

You can reset the accumulated NAT statistics with the \texttt{reset nat statistics} command. For example:

\texttt{ACMEPACKET# reset nat statistics}

\textbf{Media Interface Statistics}

This commands listed in this section are used to view statistics about the media interface hardware.

\textbf{Show media commands}

The \texttt{show media} command displays information about the Net-Net system’s media interfaces. This \texttt{show media} command usage is as follows:

\texttt{ACMEPACKET# show media [classify | frame-statistics | gmac-statistics | host-statistics | network | phy-statistics] [<slot> <port>]}

\textbf{show media classify}

The \texttt{show media classify} command displays network processor statistics for a specified media interface.

The \texttt{show media classify} command usage is as follows:

\texttt{ACMEPACKET# show media classify <slot> <port>}

For example:

\texttt{ACMEPACKET# show media classify 0 0}

\begin{verbatim}
Slot 0 Port 0 Microcode Statistics
-------------------------------------
  DIX/IP     0x00:  [0x002de87b.00000000]
  SNAP/IP    0x01:  [0x00000000.00000000]
  VLAN-DIX/IP 0x02:  [0x00000000.00000000]
  VLAN-SNAP/IP 0x03:  [0x00000000.00000000]
  DIX/ARP    0x04:  [0x00000038b.00000000]
  SNAP/ARP   0x05:  [0x00000000.00000000]
\end{verbatim}
The `show media frame-stats` command displays statistics about the traffic manager’s CPU port. No arguments are used with this command.

For example:

```
ACMEPACKET# show media frame-statistics
FRAME Total RX 5700 = 4
FRAME Total RX END-L2 = 0
FRAME Total RX END-L3 = 0

FRAME Total TX END = 0
FRAME Total TX 5700 = 2

FRAME_RX_APP_Q_WRITE_ERR = 0
FRAME_RX_APP_Q_READ_ERR = 0
FRAME_RX_APP_ERR = 0
FRAME_RX_APP_NPM = 4

FRAME_RX_5700DFT_INIT_COUNT = 0
FRAME_RX_MBLK_ERR = 0
FRAME_RX_CRC_ERR_COUNT = 0
FRAME_RX_BAD_LEN_ERR_COUNT = 0
FRAME_RX_IDMA5700_HCOUNT = 0
FRAME_RX_5700DFT_STATUS_ERR = 0
FRAME_RX_END_STANDBY_ERR = 0
FRAME_RX_ALG_PATH_ERR = 0
FRAME_RX_TASK_ERR = 0
```
show media gmac-statistics

The `show media gmac-statistics` command displays GMAC statistics for a supplied GMAC device and interface.

The `show media gmac-statistics` command usage is as follows:

```
ACMEPACKET# show media gmac-statistics <GMAC Slot#> <GMAC Port#>
```

For Example:

```
ACMEPACKET# show media gmac-statistics 0 0
Device 0 Port 0 IXF1104 Ethernet Statistics

          Tx Stats         Rx Stats
                   ---------         ---------
     Octets OK    1428825567  1369464813
  Octets BAD          0          0
   Ucast Pkts       3004034     3003886
   Mcast Pkts            0          0
   Bcast Pkts            0       5652
     Pkts 64 Octets          0       907
     Pkts 65-127 Octets      907     4064
   Pkts 128-255 Octets      0     1016
   Pkts 256-511 Octets    2000161   2003551
   Pkts 512-1023 Octets    1002966     1000000
   Pkts 1024-1518 Octets      0          0
  Pkts 1519-Max Octets      0          0
   Rx FCS Errors          0          0
   Rx Tagged              0          0
   Rx Data Errors         0          0
   Rx Align Errors        3004034     2003551
   Rx Long Errors         1002966     1000000
   Rx Jabber Errors       0          0
   Rx Unkn MAC Ctrl      0          0
   Rx Runt Errors         0          0

```
show media host-statistics

The `show media host-statistics` command displays statistics about traffic received on media interfaces destined for the system host. The `show media host-statistics` command usage is as follows:

```
ACMEPACKET# show media host-statistics <slot> <port>
<slot>: 0,1
<port>: 0,1,2,3
```

For Example:

```
ACMEPACKET# show media host-statistics 0 0

Host Receive Packet Stats for Slot: 0 and Port: 0
Latch Flow Packets: 0
Packet Capture Packets: 0
SFE Packets: 0
IP Fragments: 0
Arp Packets: 55692
IP Stack Packets: 0
 Phy stats Packets: 0
Diag Packets: 0
Nat Alg Packets: 0
IPsec Packets: 0
Total END Packets: 111389
Total END Error Packets: 0
Total SFE Error Packets: 0
Invalid Acme Hdr: 0
Invalid Port: 0
Invalid Forward Code: 0

Host Transmit Packet Stats for Slot: 0 Port: 0
Layer 2 Packets: 3
Layer 3 Packets: 0
Pend Packets: 0
IPsec Packets: 0
TM Packets: 17
Failed Packets: 0
Failed Mblk: 0
```

show media network

The `show media network` command displays network configuration details for all configured media interfaces (NIUs). Information for each entry includes:
• NIU interface slot / port
• VLAN ID
• IP Address configured for that slot / port / VLAN ID
• Netmask
• Configured gateway
• Secondary gateway
• Status

For example:

ACMEPACKET# show media phy-statistics

The `show media phy-statistics` command displays statistics about the phy side of the dx240. This command outputs the same data as the `show npu phy-stats` command. This command takes a media slot and port argument.

For example:

ACMEPACKET# show media phy-statistics 1 0

ACMEPACKET# show media network

show media phy-statistics

Other Media Commands

You can reset the accumulated media card hardware statistics with the `reset media` commands.

The `reset media` command usage is as follows:

```
ACMEPACKET# reset media [gmac-statistics | host-statistics]
```
HIP Statistics

The commands listed in this section are used to view information about the host-in-path (HIP) traffic statistics. HIP functionality lets you direct a specific class of traffic through a media interface to the host application.

**show hip commands**

The `show hip` command displays information about the Net-Net system’s HIP statistics. The `show hip` command usage is as follows:

```
ACMEPACKET# show hip [interfaces | statistics-all | statistics-by-interface <slot> <port>]
```

**show hip interfaces**

The `show hip interfaces` command lists the physical interface and network interface where a HIP entry is configured on the Net-Net 9200. For example:

```
ACMEPACKET# show hip interfaces

HIP (unit number 1)
  Hip Intf     1
  Media Slot   0
  Media Port   3
  Media Intf   6
  Sub Port     0
  IP Address   172.16.0.77
  Netmask      255.255.0.0
  MAC Address  00:08:25:fe:1c:03
```

**show hip statistics-all**

The `show hip statistics-all` command displays receive and transmit statistics for all services that reach the host, from all media interfaces. In addition, overall HIP statistics are displayed on the the screen.

For example:

```
ACMEPACKET# show hip statistics-all

Intfs cfg:          0
Intfs added:        0
Intfs add fails:    0
Intfs deleted:      0
Invalid rtp fd:     FALSE
Invalid kern fd:    FALSE

Interface: ALL

<table>
<thead>
<tr>
<th></th>
<th>Rx Stats</th>
<th>Tx Stats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FTP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TELNET</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SNMP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show hip statistics-by-interface

The show hip command with supplied slot and port arguments displays receive and transmit statistics for each service you can allow to reach the host on the specified interface.

The show hip command usage is as follows:

```
ACMEPACKET# show hip statistics-by-interface <slot> <port>
```

For Example:

```
ACMEPACKET# show hip statistics-by-interface 0 1
```

```
Interface: 0/1

<table>
<thead>
<tr>
<th>Rx Stats</th>
<th>Tx Stats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total:</td>
<td>0</td>
</tr>
<tr>
<td>ARP:</td>
<td>0</td>
</tr>
<tr>
<td>IP:</td>
<td>0</td>
</tr>
<tr>
<td>UDP:</td>
<td>0</td>
</tr>
<tr>
<td>ICMP:</td>
<td>0</td>
</tr>
<tr>
<td>TCP:</td>
<td>0</td>
</tr>
<tr>
<td>FTP:</td>
<td>0</td>
</tr>
<tr>
<td>TELNET:</td>
<td>0</td>
</tr>
<tr>
<td>SNMP:</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Other HIP Commands

You can reset the accumulated HIP statistics with the reset hip statistics command. For example:

```
ACMEPACKET# reset hip statistics
Clearing hip stats
```

Route Statistics

This commands listed in this section are used to learn about host routes configured in the routing table, and their statistics.

**show routes**

The show routes command displays the current system routing table. Information includes the destination, gateway to use, flags, RefCnt, Use, protocol, ToS bit, and respective physical interface for that destination. For example:

```
ACMEPACKET# show routes
```

```
<table>
<thead>
<tr>
<th>Destination/Pfx</th>
<th>Gateway</th>
<th>Flags</th>
<th>RefCnt Use</th>
<th>Proto</th>
<th>Tos</th>
<th>I/f</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>172.30.0.1</td>
<td>2010003</td>
<td>1 0</td>
<td>1 0</td>
<td>eth2</td>
<td></td>
</tr>
<tr>
<td>10.0.200.204</td>
<td>172.30.0.1</td>
<td>2020007</td>
<td>1 868</td>
<td>2 0</td>
<td>eth2</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>2200005</td>
<td>0 0</td>
<td>2 0</td>
<td>lo0</td>
<td></td>
</tr>
<tr>
<td>169.254.0.0/16</td>
<td>169.254.33.0</td>
<td>200001</td>
<td>2 0</td>
<td>0 0</td>
<td>eth1</td>
<td></td>
</tr>
<tr>
<td>169.254.64.0/18</td>
<td>169.254.97.0</td>
<td>200001</td>
<td>1 0</td>
<td>0 0</td>
<td>eth0</td>
<td></td>
</tr>
<tr>
<td>169.254.128.0/18</td>
<td>169.254.161.0</td>
<td>200001</td>
<td>0 0</td>
<td>0 0</td>
<td>veth0</td>
<td></td>
</tr>
<tr>
<td>169.254.128.0/18</td>
<td>169.254.176.0</td>
<td>101</td>
<td>0 0</td>
<td>0 0</td>
<td>veth0</td>
<td></td>
</tr>
<tr>
<td>172.16.0.0/16</td>
<td>172.16.0.77</td>
<td>200001</td>
<td>0 0</td>
<td>2 0</td>
<td>hip1</td>
<td></td>
</tr>
<tr>
<td>172.30.0.0/16</td>
<td>172.30.92.92</td>
<td>200001</td>
<td>3 0</td>
<td>2 0</td>
<td>eth2</td>
<td></td>
</tr>
<tr>
<td>172.30.92.96</td>
<td>172.30.92.96</td>
<td>200001</td>
<td>0 0</td>
<td>2 0</td>
<td>veeth2</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>192.168.0.77</td>
<td>200001</td>
<td>0 0</td>
<td>2 0</td>
<td>hip0</td>
<td></td>
</tr>
</tbody>
</table>
show route-stats

The **show route-stats** command shows routing statistics including bad routing redirects, dynamically created routes, new gateway due to redirects, destinations found unreachable, and use of a wildcard route. For example:

```
ACMEPACKET# show route-stats

routing:
  0 bad routing redirect
  0 dynamically created route
  0 new gateway due to redirects
  4294952170 destination found unreachable
  0 use of a wildcard route
```

### Pinging an IP Address

This section explains how to determine the existence of an IP address, whether it is up and accepting requests. The ACLI lets you ping external interfaces from the management ethernet ports. The output of the **ping** command includes:

- 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.

For example:

```
ACMEPACKET# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=255 time=1.9 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=1.8 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=1.9 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=1.8 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.8/1.8/1.9 ms
```

### Specifying a Source Address for ICMP Pings

The Net-Net 9200 supports sending ICMP Pings out of a user-specified network-interface and VLAN by using optional arguments with the ping command. If a source network interface and IP address are not specified, the Net-Net 9200 will send the ping out of its active MIU’s Ethernet port.

The ping command is entered as follows:

```
ping <host-address> [<network-interface-name:vlan>] <source-address>
```

For Example:

```
ACMEPACKET# ping 192.168.0.96 private:0 192.168.0.80
```

### Configuring a Network Interface for pinging

Before sending pings from a Net-Net 9200 network interface, you must enable the `icmp` parameter on the network interface you plan to ping from. In addition, you must add the source-address you plan to ping from to the network-interface’s `hip-ip-list` parameter.

**To configure a network interface for pinging network hosts:**
1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ```
   ACMEPACKET# configure terminal
   ```

2. Type `system` and press <Enter> to access the system-level configuration elements.
   
   ```
   configure# system
   ```

3. Type `network-interface` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   
   ```
   system# network-interface
   network-interface#
   ```

4. `icmp`—Set this parameter to enabled to support ICMP traffic.

5. `hip-ip-list`—Enter one or more IP addresses you wish to ping from. You must type `add` immediately before the IP addresses you are configuring in the HIP list.

6. Save and activate the configuration.

## DNS and ENUM Management

**DNS Statistics**

The Net-Net 9200 includes several commands used to debug, validate, and monitor DNS transactions and the status of the DNS configuration.

**show dns cache**

The `show DNS cache` command displays contents of DNS cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The `show DNS cache` command can be entered as follows:

```
show dns cache all
show dns cache <realm> all
show dns cache <realm> <type> <name>
```

**show dns lookup**

The `show DNS lookup` command display results of DNS lookup for a number within the DNS cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The `show DNS lookup` command can be entered as follows:

```
show dns lookup <realm> <type> <name>
```

**show dns query**

The `show DNS query` command performs an DNS lookup directly to the DNS server, without looking in the local cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The `show DNS query` command can be entered as follows:

```
show dns query <realm> <type> <name>
```

**show dns realm**

The `show DNS realm` command display a DNS statistics for a supplied realm. The `show DNS server` command is entered as follows:

```
show dns realm <realm>
```
**show dns server**  The *show DNS server* command displays information about the local DNS resolution server. The *show DNS server* command is entered as follows:

```
show dns server
```

**show dns sip**  The *show DNS sip* command displays information about the Net-Net 9200’s SIP applications’ interactions with the DNS application. The *show dns SIP* command is entered as follows:

```
show dns sip
```

**show dns sockets**  The *show DNS sockets* command displays information about the system’s DNS sockets. The *show dns sockets* command is entered as follows:

```
show dns sockets
```

**clear dns**  The *clear DNS* command is used to remove one or more entries from the DNS cache. Supplying only a realm argument clears the cache for that realm, while supplying type and name arguments clear that name from the cache. Use the *all* argument to remove all entries. The *clear DNS* command is entered as follows:

```
clear dns all
clear dns <realm> all
clear dns <realm> <type> <name>
```

**ENUM Statistics**  The Net-Net 9200 includes several commands used to debug, validate, and monitor ENUM transactions and the status of the ENUM configuration.

**show enum cache**  The *show enum cache* command displays contents of ENUM cache. This command can take an enum-server argument and a phone number argument. The enum-server argument is used to choose the cache statistics for the given ENUM server. The phone number argument is used to display cache statistics for that phone number on the entered enum server. The *show enum cache* command can be entered as follows:

```
show enum cache all
show enum cache <enum-server> all
show enum cache <enum-server> <number>
```

**show enum lookup**  The *show enum lookup* command display results of ENUM lookup for a number within the cache. This command can take an enum-server argument and a phone number argument. The enum-server argument is used to choose the lookup statistics for the given ENUM server. The phone number argument is used to display lookup statistics for that phone number on the entered enum server. The *show enum lookup* command is entered as follows:

```
show enum lookup <enum-server> <number>
```

**show enum query**  The *show enum query* command performs an ENUM lookup directly to the ENUM server. This command takes an enum-server argument and a phone number argument. The enum-server argument determines the server to query, and the phone number argument is the actual queried number. The *show enum query* command is entered as follows:
show enum server

The **show enum server** command displays a specific ENUM server’s statistics. The **show enum server** command is entered as follows:

```
show enum server <enum-server>
```

clear enum

The **clear enum** command is used to remove one or more entries from the ENUM cache. Supplying only an enum-server argument clears the cache for that server, while supplying a number argument clears that number from the cache. Use the all argument to remove all entries. The **clear enum** command is entered as follows:

```
clear enum all
clear enum <enum-server> all
clear enum <enum-server> <number>
```

Clearing ENUM and DNS Statistics

To clear statistics for ENUM and 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 command—by typing, for example, **show enum stats**.

The **reset** command takes the ENUM and 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.

ACLI Instructions and Examples

This section shows you how to clear ENUM and DNS statistics. The ENUM example confirms successful completion of the command; the second shows the error message that appears if the command fails.

**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
   ```

**To clear DNS statistics:**

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

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

Packet Trace

The packet trace feature lets the Net-Net SBC mirror any communication between two endpoints running through the Net-Net SBC, or between itself and a specific endpoint. To accomplish this, the Net-Net SBC replicates the packets sent and received, and then sends them to a configured trace server. Using a protocol analyzer running on the trace server, you can then analyze the mirrored packets. Currently, the Packet Trace feature supports:

- One configurable trace server (on which you have installed your software protocol analyzer)
How It Works

To use this feature, create a trace server configuration on the Net-Net SBC so that it knows where to send the mirrored packets. Once the trace server is configured, the Net-Net SBC uses one of its internally configured IP addresses (such as one for a SIP interface) on which to source the trace.

You start a packet trace using the ACLI Superuser command `start packet-trace`, entered with these pieces of information:

- **Network interface**—The name of the network interface on the Net-Net SBC from which you want to trace packets; this value can be entered either as a name alone or as a name and subport identifier value (name:subportid)
  
  This feature is supported for NIU (media) interfaces; it is not supported for MIU (management) interfaces.

- **IP address**—IP address of the endpoint to and from which the Net-Net SBC will mirror calls

- **Local port number**—Optional parameter; Layer 4 port number on which the Net-Net SBC receives and from which it sends; if no port is specified or if it is set to 0, then all ports will be traced

- **Remote port number**—Optional parameter; Layer 4 port number to which the Net-Net SBC sends and from which it receives; if no port is specified or if it is set to 0, then all ports will be traced

The usage is as follows:

```
start packet-trace <network-interface:subport ID> <IP address> 
[<local-port>] [<remote-port>]
```

See the Starting a Packet Trace (189) section for an example.

Once the trace is initiated, the Net-Net SBC duplicates all packets sent to and from the endpoint identified by the IP address that are sent or received on the specified Net-Net SBC network interface.

The Net-Net SBC then encapsulates the original packets in accordance with RFC 2003 (IP Encapsulation within IP); it adds the requisite headers, and the payload contains the original packet trace with the Layer 2 header removed. Since software protocol analyzers understand RFC 2003, they can easily parse the original traced packets. In order to see only packet traces information in your software protocol analyzer, you can use a capture filter; for example, the Ethereal/Wireshark syntax is “ip proto 4.”
It is possible that—for large frames—when the Net-Net SBC performs the steps to comply with RFC 2003 by adding the requisite header, the resulting packet might exceed Ethernet maximum transmission unit (MTU). This could result in packets being dropped by external network devices, but widespread support for jumbo frames should mitigate this possibility.

If the Net-Net SBC either receives or transmits IP fragments during a packet trace, then it will only trace the first fragment. The first fragment is likely to be a maximum-sized Ethernet frame.

The Net-Net SBC continues to conduct the packet trace and send the replicated information to the trace server until you instruct it to stop. You stop a packet trace with the ACLI `stop packet-trace` command. With this command, you can stop either an individual packet trace or all packet traces that the Net-Net SBC is currently conducting. The usage is as follows:

```
stop packet-trace <network-interface:subport ID> <IP address> [<local-port>] [<remote-port>]
```

### Packet Trace Scenarios

This section describes three possible ways that you might use the packet trace feature. You can examine communications sent to and from one endpoint, sent between two endpoints, or sent between ingress and/or egress Net-Net SBC interfaces to endpoints.

### Packet Trace for One Endpoint

When you use the `start packet-trace` command, the Net-Net SBC sets up packet tracing for the traffic between itself and one endpoint. The Net-Net SBC collects and replicates the packets to and from one endpoint. All traffic on all ports is replicated to the trace server. To enable this kind of trace, you set up one packet trace using the `start packet-trace` command. For example:

```
ACMEPACKET# start packet-trace <Network Interface> <IP address of Endpoint A>
```
Packet Trace for Both Call Legs

If you want to trace both sides (both call legs) of a call that runs through the Net-Net SBC, then you must set up individual traces for each endpoint—meaning that you would initiate two packet traces. This trace gives you the communications for both call legs between the endpoints you specify. All traffic on all ports for both call legs is replicated to the trace server.

The commands you carry out would take the following form:

```
ACMEPACKET# start packet-trace <Destination Network Interface of Endpoint A> <IP address of Endpoint A>
ACMEPACKET# pstart acket-trace <Destination Network Interface of Endpoint B> <IP address of Endpoint B>
```
Packet Trace for a Net-Net SBC Signaling Address

You can perform a packet trace for addresses internal to the Net-Net SBC. Using signaling interface addresses puts the emphasis on the Net-Net SBC rather than on the endpoints by allowing you to view all traffic that traverses specified interfaces.

The commands you carry out would take the following form:

```
ACMEPACKET# start packet-trace <Network Interface where Endpoint A connects> <SIP Interface 1 IP address> 5060
ACMEPACKET# start packet-trace <Network Interface where Endpoint B connects> <SIP Interface 2 IP address> 5060
```

ACLI Instructions and Examples

There are three steps you can take when you use the packet trace feature:

- Configuring the Net-Net SBC with the trace server information so that the Net-Net SBC knows where to send replicated data
- Setting up the capture filter “ip proto 4” in your software protocol analyzer if you only want to see the results of the Net-Net SBC packet trace(s)
- Starting & Stopping a packet trace

This section provides information about how to perform all three tasks.

Configuring a Trace Server

You must configure a trace server on the Net-Net SBC; this is the device to which the Net-Net SBC sends replicated traffic. The Net-Net SBC supports one trace server.

**To configure a trace server on your Net-Net SBC:**

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ```
   ACMEPACKET# configure terminal
   ```
2. Type `system` and press <Enter>.
   
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(configure)#
   ```
3. Enter `capture-receiver` and press <Enter>.
   
   ```
   ACMEPACKET(system)# capture-receiver
   ACMEPACKET(capture receiver)#
   ```

4. **state**—Type `enabled` so that you can use the trace server to which you want to send the mirrored packets for calls you are packet tracing. This parameter defaults to `disabled`.

5. **address**—Enter the IP address of the trace server; there is no default.

6. **network-interface**—Enter the name and subport of the Net-Net SBC network interface from which the Net-Net SBC is to send mirrored packets. Your entry needs to take the form `name:subport`. The default for this parameter is `:0`.

7. Save your work using the ACLI `done` command.

8. Save and activate your configuration.

---

**Starting a Packet Trace**

Start a packet trace by entering the appropriate ACLI command with these pieces of information:

- Network interface (`name:subport ID` combination)
- IP address to be traced; if you do not enter local and/or remote ports when you start the trace, the Net-Net SBC will trace all ports
- (Optional) Local UDP/TCP port on which the Net-Net SBC sends and receives traffic to be traced
- (Optional) Remote UDP/TCP port to which the Net-Net SBC sends traffic, and from which it receives traffic to be traced; you cannot enter the remote port without specifying a local port

**To start a packet trace with local and remote ports specified:**

1. Type `start packet-trace` followed by a <Space>. After another <Space>, type in the name and subport ID for the network interface followed by a <Space>, the IP address to be traced followed by a <Space>, the local port number followed by a <Space>, and then optionally the remote port number. Then press <Enter>.
   
   ```
   ACMEPACKET# start packet-trace core:0 192.168.10.99 5060 5060
   Trace started for 192.168.10.99
   ```

**Stopping a Packet Trace**

You use the stop a packet trace by entering the appropriate ACLI command with these pieces of information:

- Network interface (`name:subport ID` combination)
- IP address to be traced
- (Optional) Local UDP/TCP port on which the Net-Net SBC sends and receives traffic to be traced
- (Optional) Remote UDP/TCP port to which the Net-Net SBC sends traffic, and from which it receives traffic to be traced

If the packet trace you want to stop has no entries for local and/or remote ports, then you do not have to specify them.

**To stop a packet trace with local and remote ports specified:**

1. Type `stop packet-trace` followed by a <Space>. After another <Space>, type in the name and subport ID for the network interface followed by a <Space>, the
IP address to be traced followed by a <Space>, the local port number followed by a <Space>, and then optionally the remote port number. Then press <Enter>.

ACMEPACKET# stop packet-trace core:0 192.168.10.99 5060 5060

To stop all packet traces on the Net-Net SBC:

1. Type stop packet-trace followed by a <Space>and the word all and press <Enter>.
   
ACMEPACKET# stop packet-trace all

Viewing Active Packet Traces

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Local-Port</th>
<th>Remote-Port</th>
<th>Slot</th>
<th>Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>192.168.10.99</td>
<td>5060</td>
<td>5060</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>23</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Commands discussed in this chapter are used for Net-Net OS application management. This class of commands refers to statistics and counters dealing with media and signaling traffic.

SIP Management

The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its SIP implementation.

SIP Tasks Show Commands

SIP processing spans several tasks on the Net-Net 9200. The following SIP show commands display various details of SIP system functionality.

show sip transport

The `show sip transport` command displays statistics related to the SIP transport application (sipt). This application implements the Transport Layer and the Transaction Layer of the SIP Signaling Protocol. It is the entry and exit point for all SIP messages. It parses and validates all received SIP message requests and responses. It formats and transmits all outgoing SIP message requests and responses. It also performs all SIP-NAT encoding and decoding on SIP messages. For example:

```
ACMEPACKET# show sip transport
12:37:53 106 sipt
SIP Transport        Recent        Lifetime
Active    High   Total      Total   PerMax   High
Server Trans             0       0       0      32574    6009    1982
Client Trans             0       0       0      32574    6010    1981
Context IDs              0       0       0      32574    6009    1982
Sockets                  2       2       0          3       3       3
Req Rejected             -       -       0          0       0
Req Dropped              -       -       0          0       0
DNS Trans                0       0       0          0       0       0
DNS Sockets              0       0       0          0       0       0
DNS Results              0       0       0          0       0       0
Invalid Requests         -       -       0          0       0
Invalid Responses        -       -       0          0       0
Invalid Messages         -       -       0          0       0
Transaction Errors       -       -       0          0       0
Application Errors       -       -       0          0       0
```

show sip server

The `show sip server` command displays statistics related to the server. For example:

```
ACMEPACKET# show sip server
08:07:38 106 sip@0.3.0
SIP Server Trans        Recent        Lifetime
Active    High   Total      Total   PerMax   High
```

Proprietary & Confidential
show sip client

The **show sip client** command displays statistics related to the client. For example:

```
ACMEPACKET# show sip client
08:07:12-121 sipls@0.3.0
SIP Client Trans        ---- Recent ---- -------- Lifetime --------
Active  High  Total      Total  PerMax  High
Total                      0       0       0          0       0       0
<Initial>                  0       0       0          0       0       0
<Trying>                   0       0       0          0       0       0
<Calling>                  0       0       0          0       0       0
<Proceeding>               0       0       0          0       0       0
<Cancelling>               0       0       0          0       0       0
<Completed>                0       0       0          0       0       0
<Established>              0       0       0          0       0       0
<Confirmed>                0       0       0          0       0       0
<Terminated>               0       0       0          0       0       0
```

show sip codecs

The **show sip codecs** command displays realm codec statistics. For example:

```
ACMEPACKET# show sip codecs public
18:56:31-46 Realm public
Codec Statistics        ---- Recent ---- -------- Lifetime --------
Active  High  Total      Total  PerMax  High
Transcoded               0       0       0          0       0       0
Transrated               0       0       0          0       0       0
Transparent              0       0       0          0       0       0
PCMU Count               -       -       0          0       0       0
PCMA Count               -       -       0          0       0       0
G722 Count               -       -       0          0       0       0
G723 Count               -       -       0          0       0       0
G726-16 Count            -       -       0          0       0       0
G726-24 Count            -       -       0          0       0       0
G726-32 Count            -       -       0          0       0       0
G726-40 Count            -       -       0          0       0       0
G728 Count               -       -       0          0       0       0
G729 Count               -       -       0          0       0       0
GSM Count                -       -       0          0       0       0
iLBC Count               -       -       0          0       0       0
H261 Count               -       -       0          0       0       0
H263 Count               -       -       0          0       0       0
T38 Count                -       -       0          0       0       0
Other Count              -       -       0          0       0       0
```
**show sip core**

The `show sip core` command displays statistics related to the SIP core task (sipc). This is where the SIP proxy function is carried out and where requests are forwarded to one or more next hop target destinations. For example:

```
ACMEPACKET# show sip core
08:01:32-180 sipl@0.3.0
SIP Core ---- Recent -------- Lifetime --------
Active     High   Total      Total  PerMax    High
Response Contexts 0       0       0          0       0       0
Forwarded Requests 0       0       0          0       0       0
Saved Contexts    0       0       0          0       0       0
Challenge Found   -       -       0          0       0       0
Challenge Not Found -       -       0          0       0       0
Challenge Dropped -       -       0          0       0       0
Overload Rejects  -       -       0          0       0       0
DNS Errors       -       -       0          0       0       0
No Target/Route  -       -       0          0       0       0
Transaction Errors -       -       0          0       0       0
Application Errors -       -       0          0       0       0
```

**show sip b2bua**

The `show sip b2bua` command displays statistics related to the SIP Back To Back UA task (sipbb). The SIP B2B UA manages all SIP sessions and dialogs in addition to implementing the Back-to-Back User Agent functionality for SIP. For example:

```
ACMEPACKET# show sip b2bua
08:05:13-101 sipl@0.3.0
SIP B2BUA ---- Recent -------- Lifetime --------
Active     High   Total      Total  PerMax    High
Dialogs    0       0       0          0       0       0
Sessions   0       0       0          0       0       0
CallID Map 0       0       0          0       0       0
Pending Requests 0       0       0          0       0       0
Missing Dialog 0       0       0          0       0       0
Expired Sessions 0       0       0          0       0       0
Multiple OK Drops 0       0       0          0       0       0
Multiple OK Terms 0       0       0          0       0       0
Media Failure Drops 0       0       0          0       0       0
Non-ACK 2xx Drops 0       0       0          0       0       0
Transaction Errors 0       0       0          0       0       0
Application Errors 0       0       0          0       0       0
```

**show sip sessions**

The `show sip sessions` command displays statistics related to the states of SIP sessions and dialogs. For example:

```
ACMEPACKET# show sip sessions
12:38:29-142 sipbb
SIP Session ---- Recent -------- Lifetime --------
Active     High   Total      Total  PerMax    High
Sessions   0       0       0      10000    1837     154
Initial    0       0       0      10000    1837      3
Early      0       0       0      10000    1837      5
Established 0       0       0      10000    1837    149
Terminated 0       0       0      10000    1837     75
Dialogs    0       0       0      20000    3674    452
None       0       0       0      20000    3674      2
```
show sip cache

The **show sip cache** command displays statistics for the SIP Registration Cache (location service). For example:

```
ACMEPACKET# show sip cache
12:38:38-149 sipls
SIP Loc Server .... Recent .... ........ Lifetime ........
                      Active  High  Total  Total  PerMax  High
Cached Entries       0     0     0      0     0     0
Local Entries        0     0     0      0     0     0
Free Map Ports       0     0     0      0     0     0
Used Map Ports       0     0     0      0     0     0
Transactions         0     0     0      0     0     0
Forwards             -     -     0      0     0
Rejects              -     -     0      0     0
Timeouts             -     -     0      0     0
Fwd Postponed        -     -     0      0     0
Fwd Rejects          -     -     0      0     0
Refr Extension       0     0     0          0     0     0
Refresh Extended     -     -     0      0     0
Reg Cache Hits       -     -     0      0     0
Reg Cache Misses     -     -     0      10000 1837
Route to Registrar  -     -     0      0     0
Reg w/o Contacts    -     -     0      0     0
Transaction Errors  -     -     0      0     0
Application Errors  -     -     0      0     0
```

show sip policy

The **show sip policy** command displays statistics related to local policy lookups. This functionality is part of the SIP location service. For example:

```
ACMEPACKET# show sip policy
12:38:42-154 sipls
SIP Policy/Routing .... Lifetime ....
                      Recent  Total  PerMax
Local Policy Lookups 0   10000 1837
Local Policy Hits    0   10000 1837
Local Policy Misses  0     0  0
Local Policy Drops   0     0  0
Agent Group Hits     0     0  0
Agent Group Misses   0     0  0
No Routes Found      0     0  0
Inb SA Constraints   0     0  0
Outb SA Constraints  0     0  0
```

show sip media

The **show sip media** command displays statistics related to SIP media sessions. For example:

```
ACMEPACKET# show sip media
12:39:05-180 sipm
SIP Media .... Recent .... ........ Lifetime ........
```

Proprietary & Confidential
show sip load

The `show sip load` command displays the SIP transport task’s current load. For example:

```
ACMEPACKET# show sip load
SIP Transport Load is 0.0; Limit is 80
```

SIP Messages Show Commands

The following show commands display statistics related to SIP messages of the type indicated. The Server columns display counts of the SIP message type received by the Net-Net 9200, and the Client columns display counts of the SIP message type sent by the Net-Net 9200.

show sip invite

```
ACMEPACKET# show sip invite
18:52:12-198 sipls@0.4.1
--------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  -----
INVITE Requests            1          1       1        1          1       1
Retransmissions            0          0       0        0          0       0
100 Trying                 1          1       1        1          1       1
180 Ringing                1          1       1        1          1       1
200 OK                      1          1       1        1          1       1
Response Retrans           0          0       0        0          0       0
Transaction Timeouts       0          0       0        0          0       0
Locally Throttled          0          0       0
Avg Latency=0.009 for 1
Max Latency=0.009
```

show sip ack

```
ACMEPACKET# show sip ack
12:39:13-187
--------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  -----
ACK Requests           0 10000    1837        0 10000    1837
Retransmissions       0          0       0        0          0       0
Duplicate Response    0          0       0        0          0       0
Transaction Timeouts  0          0       0        0          0       0
Avg Latency=0.000 for 0
Max Latency=0.000
```
show sip bye

ACMEPACKET# show sip bye
12:39:19-192

<table>
<thead>
<tr>
<th>Message/Event</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYE Requests</td>
<td>0</td>
<td>12574</td>
<td>2338</td>
<td>0</td>
<td>12574</td>
<td>2338</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200 OK</td>
<td>0</td>
<td>12574</td>
<td>2339</td>
<td>0</td>
<td>12574</td>
<td>2339</td>
</tr>
<tr>
<td>Duplicate Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Avg Latency=0.000 for 0
Max Latency=0.000

show sip register

ACMEPACKET# show sip register
13:59:17-135

<table>
<thead>
<tr>
<th>Message/Event</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTER Requests</td>
<td>6</td>
<td>13343</td>
<td>5</td>
<td>1</td>
<td>287</td>
<td>2</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200 OK</td>
<td>6</td>
<td>13343</td>
<td>5</td>
<td>1</td>
<td>287</td>
<td>2</td>
</tr>
<tr>
<td>Duplicate Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Avg Latency=0.002 for 7
Max Latency=0.016

show sip cancel

ACMEPACKET# show sip cancel
14:13:56-114

<table>
<thead>
<tr>
<th>Message/Event</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>CANCEL Requests</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200 OK</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Duplicate Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Avg Latency=0.000 for 0
Max Latency=0.000

show sip prack

ACMEPACKET# show sip prack
---< NO DATA AVAILABLE >---

show sip options

ACMEPACKET# show sip options
---< NO DATA AVAILABLE >---

show sip info

ACMEPACKET# show sip info
---< NO DATA AVAILABLE >---
show sip sub

ACMEPACKET# show sip sub
--- < NO DATA AVAILABLE > ---

show sip subscribe

ACMEPACKET# show sip subscribe
--- < NO DATA AVAILABLE > ---

show sip notify

ACMEPACKET# show sip notify
--- < NO DATA AVAILABLE > ---

show sip refer

ACMEPACKET# show sip refer
--- < NO DATA AVAILABLE > ---

show sip update

ACMEPACKET# show sip update
--- < NO DATA AVAILABLE > ---

show sip message

ACMEPACKET# show sip message
--- < NO DATA AVAILABLE > ---

show sip publish

ACMEPACKET# show sip publish
--- < NO DATA AVAILABLE > ---

show sip other

ACMEPACKET# show sip other
--- < NO DATA AVAILABLE > ---

show sip forked

Using the ACLI show sip forked command, you can display the total number of forked sessions the Net-Net SBC received and the total number it rejected. The Net-Net SBC counts forked sessions when it receives a dialog-creating INVITE and is enabled to shared bandwidth. Further, it counts as forked all session with the P-Multiring-Correlator header.

ACMEPACKET# show sip forked
16:57:46-131 sipls@0.4.1
Forked Session Stats               ---- Recent ---- ---- Lifetime -----
Active    High   Total      Total  PerMax    High
Total Sessions                    -       -       0          0       0
Total Sessions Rej                -       -       0          0       0

SIP Networking

Show Commands

The following show commands display statistics about logical SIP entities in the network and their connections to the Net-Net system.

show sip agents

The show sip agents command displays statistics related to defined SIP session agents. Entering this command without any arguments lists all SIP session agents. Adding the IP address or hostname of a session agent at the end of the command displays statistics for that session agent. For example:

ACMEPACKET# show sip agents
No Session Agents found
show sip sockets

The `show sip sockets` command displays connections and message counts on the Net-Net system. For example:

```
ACMEPACKET# show sip sockets
Handle | Socket | MsgRcvd | MsgSent | Errors
------ | ------ | ------- | ------- | --------
2      | UDP[0:0]172.16.0.170:5060 | 32574   | 42574   | 0
3      | UDP[2:0]192.168.24.170:5060 | 42574   | 32574   | 0
------ | ------ | ------- | ------- | --------
Total Open Sockets: 2
```

show sip endpoint

The `show sip endpoint` command displays registration information for a supplied endpoint. For example:

```
ACMEPACKET# show sip endpoint 801
User sip:801@172.16.0.123 ID=2
Contact: ID=2 exp-UA=1497 exp-SD=1493
UA=<sip:801@172.16.0.199>
real=public local=172.16.0.123:5060 remote=172.16.0.199:5060
SD=<sip:801@192.168.0.123:5060> real=private
Call-ID=8829479ed7557833@172.16.0.199
```

show sip realm

The `show sip realm` command displays current statistics for all configured realms used for SIP services. For example:

```
ACMEPACKET# show sip realm
07:39:21
----- Inbound -----  ---- Outbound ----  -- Latency --  Max
Realms            Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
private                 0   0.0      0       0   0.0      0  0.000  0.000     0
public                  0   0.0      0       0   0.0      0  0.000  0.000     0
```

Entering a specific realm as the final argument returns statistics for the identified realm. For example:

```
ACMEPACKET# show sip realm public
15:01:38-38
Realm net200 ID=06 [In Service]
----- Recent -----  ------ Lifetime ------
Inbound Sessions 0 0 0 0 0 0 0 0
Sustained Rate - - 0.0 - -
Rate Exceeded - - 0 0
Num Exceeded - - 0 0
Burst Rate(10s) 0 0 0 0 0 0
RegRate Exceeded - - 0 0
Outbound Sessions 0 0 0 0 0 0 0 0
Sustained Rate - - 0.0 - -
Rate Exceeded - - 0 0
Num Exceeded - - 0 0
Burst Rate(10s) 0 0 0 0 0 0
RegRate Exceeded - - 0 0
```
| Burst (10s) | 0 | 0 | 0 | 0 | 0 | 0 |
| Trans Timeouts | 0 | 0 | 0 | 0 | 0 | 0 |
| Requests Sent | - | - | 0 | 1 | 1 |
| Requests Complete | - | - | 0 | 1 | 1 |
| Requests Received | - | - | 0 | 0 | 0 |
| Seizure | - | - | 0 | 0 | 0 |
| Answer | - | - | 0 | 0 | 0 |
| ASR Exceeded | - | - | 0 | 0 | 0 |
| Minutes Exceed Rej | - | - | 0 | 0 | 0 |
| Short Session (10s) | 0 | 0 | 0 | 0 | 0 | 0 |

Avg Latency=0.000 for 1
Max Latency=0.000

**SIP CPU Load Limiting**

See [SIP Load Limiting](#) for a description on how to enable SIP CPU load limiting.

**Call Protocol (SIP) Tracing**

For debugging needs, you can capture and save a log of all VoIP application messages that reach and are sourced from the Net-Net 9200 as a signalling protocol log. This log file can be stored locally (RAM drive), remotely (process log server), or simultaneously locally and remotely.

This feature works similarly to the [Process Log Files](#) feature.

**SIP Protocol Trace Output**

The SIPT process is the SIP task that generates a protocol trace. When writing a protocol trace locally, the sipmsg.log file is located on the file system local to the CPU/core where the SIPT runs, in the `/ramdrv/logs/` directory. You can use the `show manifest` command to find the location of SIPT.

When you set SIPT’s task logging configuration to a specific level, all messages of that level and higher are written to the task log. By default, if you set the task’s logging level to TRACE or DEBUG, it also outputs a protocol trace. Alternatively, you can use the call trace parameter to enable a protocol message trace, regardless of the task’s logging level.

**Configuration**

Call protocol tracing is enabled in the system configuration. You must also set the call trace mode parameter, which determines the location of the call trace log files. You may choose one of four selectable call trace modes to specify what the Net-Net 9200 does with the call trace log.
APPLICATION MANAGEMENT

- local—Writes the protocol trace file locally.
- remote—Sends protocol trace message to the configured Acme Process Log Server.
- both—Writes the protocol trace file to both the configured Acme Process Log Server and locally.
- none—Task does not write to local or remote location.

To enable SIP call tracing:

1. In Superuser mode, type `configure terminal` and press <Enter>.
   
   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type `system` and press <Enter> to access the system path.
   
   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type `system-config` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   
   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. `call-tracing`—Set this parameter to enabled for the Net-Net 9200 to generate a call trace log.

5. `call-trace-mode`—Set the call trace log mode that you want to use from these available choices:
   - remote—Send call trace logs to the Process log server only
   - local—Send call trace logs to the local file system only (default)
   - both—Send call trace logs to the Process log server and to the local file system
   - none—No call trace logging

6. Save your work using the ACLI `done` command.

7. Save and activate the configuration.

Displaying and Clearing Registration Cache Entries

The Net-Net SBC’s registration cache management offers detailed information (beyond basic registration cache displays) and flexible ways to view the registration cache. You can query, clear, and audit entries.

Querying the SIP Registration Cache

You can view SIP registration cache information `by-user`, `by-realm`, `by-route`, and `by-registrar`. For each of these search criteria, you can specify the whole term, part of the search term, or a wildcard “*”. If you only use part of a user name without adding the wildcard character, the Net-Net SBC only returns exact matches.

The SIP registration cache statistics include counters for free and allocated signaling ports. You can issue a show registration command to display the statistics:

```
17:36:55-190
SIP Registrations          -- Period -- Lifetime --------
Active  High  Total  Total  PerMax  High
```
User Entries          4       4       0          7       4       4
Local Contacts        4       4       0          7       4       4
Free Map Ports    12284   12284       0      12291   12288   12288
Used Map Ports        4       4       0          7       4       4
Forwards              -       -       1         22       4
Refreshes             -       -       3        43       3
Rejects               -       -       0          0       0
Timeouts              -       -       0          1       1
Fwd Postponed         -       -       0          0       0
Fwd Rejected          -       -       0          0       0
Refr Extension        0       0       0          0       0       0
Refresh Extended      -       -       0          0       0

The labels for the first two items reflect the restructured registration cache:

- User Entries—Counts the number of unique SIP addresses of record in the cache. Each unique address of record represents a SIP user (or subscriber). The address of record is taken from the To header in the REGISTER request. There might be one or more registered contacts for each SIP user. The contacts come from the Contact header of the REGISTER request.

- Local Contacts—Counts the number of contact entries in the cache. Because the same user can register from multiple endpoints (user agents); the number of Local Contacts might be higher than the number of User Entries.

- Free Map Ports—Counts the number of ports available in the free signaling port pool.

- Used Map Ports—Counts the number of signaling ports allocated for registration cache entries. The value of Used Map Ports will equal the number of Local Contacts when the port mapping feature is used for all registrar/softswitch realms in the Net-Net 9200.

by-user

The registration cache can be searched by a specific username, phone number, or portion of a username or phone number. All of these user types are equivalent. This command is entered as:

```
show registration sip by-user <endpoint> [brief | extended | detail]
```

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 with 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*). For example:

```
ACMEPACKET> show registration sip by-user user*
```

<table>
<thead>
<tr>
<th>User</th>
<th>Contacts</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip:<a href="mailto:user@acme.com">user@acme.com</a></td>
<td>1</td>
<td>2007-07-26 11:29:50</td>
</tr>
<tr>
<td>sip:<a href="mailto:username@acme.com">username@acme.com</a></td>
<td>1</td>
<td>2007-07-26 11:29:51</td>
</tr>
<tr>
<td>sip:<a href="mailto:username2@acme.com">username2@acme.com</a></td>
<td>1</td>
<td>2007-07-26 11:29:51</td>
</tr>
</tbody>
</table>

ACMEPACKET>
You can add the **detailed** argument only to the by-user query to view complete registration cache contents:

```
ACMEPACKET> show registration sip by-user user detailed
```

```
Registration Cache (Detailed View) TUE JUL 2 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-m2vm2n09kb@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
```

**by-realm**

The registration cache can be searched for calls that have registered through a specified ingress realm. Wild cards will be supported as well. This command is entered as:

```
show registration sip by-realm <realm> [brief | extended]
```

The output will also be sorted alphabetically by the realm name which will be shown first in the output. For example:

```
ACMEPACKET# show registration sip by-realm *
```

```
Registration Cache THU OCT 2 15:02:12 2007

<table>
<thead>
<tr>
<th>Realm</th>
<th>User</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>sip:420000002@172.16.34.10</td>
<td>2007-10-11-15:01:51</td>
</tr>
<tr>
<td>backbone</td>
<td>sip:<a href="mailto:17815552020@acmepacket.com">17815552020@acmepacket.com</a></td>
<td>2007-10-11-14:10:26</td>
</tr>
</tbody>
</table>

Total 2 entries
```

You can add the **extended** argument to view this command’s output with detailed information as shown in the Extended Registration Cache Output section.

**by-route**

The registration cache can be searched for calls by their Internet-routable IP address with the search type "by-route". This is useful for viewing the endpoints associated with public addresses. Wild cards are supported as well. Search values are checked
to be a valid IPv4 IP address, except in the case of use with the wild cards where only the first part of the address is checked. This command is entered as:

```
show registration sip by-route <IP-address> [brief | extended]
```

The output is sorted by the IP address. For example:

```
ACMEPACKET# show registration sip by-route *
```

Registration Cache

<table>
<thead>
<tr>
<th>Routable IP Address</th>
<th>User</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.34.10</td>
<td>sip:4200000002@172.16.34.10</td>
<td>2007-10-11-15:01:51</td>
</tr>
<tr>
<td>192.168.34.10</td>
<td>sip:<a href="mailto:17815552020@acmepacket.com">17815552020@acmepacket.com</a></td>
<td>2007-10-11-14:10:26</td>
</tr>
</tbody>
</table>

**Total 2 entries**

You can add the `extended` argument to view this command’s output with detailed information as shown in the Extended Registration Cache Output section.

**by-registrar**

The registration cache can be searched for calls that use a specific registrar. The search will support wild cards so either complete name of the realm, partial name ending with the "*" or "**" by itself could be used. This command is entered as:

```
show registration sip by-registrar <IP-address> [brief | extended]
```

The output is sorted alphabetically by the registrar address. A delay before printing the output of the by-registrar command to the screen is likely. Before the number of entries there will be a note: "Searching entries…total n". The maximum supported number of entries is 999,999.

```
ACMEPACKET# show registration sip by-registrar *
```

Registration Cache

<table>
<thead>
<tr>
<th>Registrar IP Address</th>
<th>User</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.34.10</td>
<td>sip:4200000002@172.16.34.10</td>
<td>2007-10-11-15:01:51</td>
</tr>
<tr>
<td>192.168.34.10</td>
<td>sip:<a href="mailto:17815552020@acmepacket.com">17815552020@acmepacket.com</a></td>
<td>2007-10-11-14:10:26</td>
</tr>
</tbody>
</table>

**Total 2 entries**

You can add the `extended` argument to view this command’s output with detailed information as shown in the Extended Registration Cache Output section.

**Extended Registration Cache Output**

You can add the `extended` argument to the show registration sip command’s output. The output includes User, Registration Time, registration realm, registrar’s
Writing Registration Queries to a File

You can write all output from the `show registration sip` commands to a file located on the local flash file system instead of to the ACLI. You use the `to-file` switch, followed by the output filename. The file is written to the `/ramdrv/` location, or any subdirectory as indicated in the filename. For example:

```
ACMEPACKET# show registration sip by-user * to-file /ramdrv/output.txt
```

If the file already exists, the old file is renamed to `file_name.bak`. Subdirectories are supported and will be created by the system if they do not exist.

**Note:** The contents of the `/ramdrv/` is cleared on reboot. Therefore, you must FTP them off the Net-Net SBC if they require preservation.

Displaying H.323 Registration Cache Entries

The Net-Net SBC’s registration cache management offers detailed information (beyond basic registration cache displays) and flexible ways to view the registration cache. You can query, clear, and audit entries.

**by-alias**

The H.323 registration cache can be searched by a specific endpoint. This command is entered as:

```
show registration h323 by-alias <endpoint> [brief | detail]
```

The `<endpoint>` portion of the command can be a single phone number or one of the terminal aliases. Use of the wildcard character `*` is supported as the last character of the endpoint string.

For example, an endpoint might be registered as `4278_endp`.

The phone number can be a single number (such as `7815551234`) or a single number wildcarded with 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*`). For example:

```
ACMEPACKET> show registration h323 by-alias 4278_endp
```

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Expiration</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>4278_endp</td>
<td>27</td>
<td>2007-08-03-19:58:34</td>
</tr>
</tbody>
</table>
You can add the **detailed** argument to view complete registration cache contents:

```
ACMEPACKET> show registration h323 by-alias 4224_endp detail
```

**Registration Cache (Detailed View)**

- **Endpoint:** 4224_endp, state: Registered
- **Registered at:** 2007-04-24-14:50:05
- **Expiration:** 204
- **Gatekeeper:** open-gk1

- **Endpoint NAT Address:** 192.168.200.56:1372
- **SD Call Signaling Address:** 150.150.150.10:2048
- **SD RAS Address:** 150.150.150.10:8200

**Terminal Alias(s):**
- **Alias:** e164: 17815552222, **Registered:** true

**Call Signaling Address(s):**
- **Address:** 192.168.200.56:1720

**RAS Address(s):**
- **Address:** 192.168.200.56:1372

---

**Clearing the SIP Registration Cache**

You can clear a single user entry from the SIP registration cache, or you can clear the full registration cache with the **clear registration sip** command.

**clear registration sip**

You can clear the entire registration cache by using the **all** switch, or remove the registration cache entry for a single specified user or phone number. The phone number can be a single number (7815554400). You can also enter a user name for this value. This command takes the form:

```
clear registration sip [all | by-user <user> ]
```

After you use this command, all affected endpoints will have to register through the Net-Net SBC once again.

**Note:** You can wildcard user values with the clear registration sip command.

**Entries Registered by a Surrogate Agent**

Endpoints registered by a surrogate are uniquely displayed on the ACLI. These same endpoints can not be removed from the registration cache by regular means. You can disable the surrogate agent in the configuration to remove these entries from the cache.

**Displaying Registrations**

Entries created by the surrogate agents will have a "**" before the user name when running a show registration command. There will be also a separate count for those
entries. If no endpoints were registered by a surrogate agent, no extra line with the surrogate counter will be shown. For example:

\[\text{ACMEPACKET}\gt \text{show registration sip by-user mike}\]

<table>
<thead>
<tr>
<th>User</th>
<th>Contacts</th>
<th>Registered at</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip:<a href="mailto:mike@acme.com">mike@acme.com</a></td>
<td>1</td>
<td>2007-03-06-11:29:50</td>
</tr>
<tr>
<td>* sip:mi <a href="mailto:kesmith@acme.com">kesmith@acme.com</a></td>
<td>1</td>
<td>2007-03-06-11:29:51</td>
</tr>
<tr>
<td>sip:<a href="mailto:mikester@acme.com">mikester@acme.com</a></td>
<td>1</td>
<td>2007-03-06-11:29:51</td>
</tr>
</tbody>
</table>

Total 3 entries
1 entry created by the surrogate agent(s)

Clearing Registrations

When using the clear-cache command, entries created by the surrogate agent will be skipped and will not be cleared if exist in the registry. The extra counter for the surrogate entries will point out how many of those are skipped. The original counter will print out the number of entries that where cleared.

If the clear-cache command is successful there are several possible outputs displayed to the screen. If there were no entries created by the surrogate agents then the output looks like this:

Successfully cleared 658 Registration Cache entries

When the registration cache contains mixed elements, both created normally and by the surrogate agents, the output looks like this:

Successfully cleared 658 Registration Cache entries
65 entries skipped (created by the surrogate agent(s))

If all of the entries in the registry were created by the surrogate agents, then the output looks like this:

No entries cleared!
65 entries skipped (created by the surrogate agent(s))

If requested search finds no matching entries, the output looks like this:

No matching entries found!

Clearing the H.323 Registration Cache

You can clear a single user entry from the H.323 registration cache, or you can clear the full registration cache with the clear registration h323 command.

clear registration sip

You can clear the entire registration cache by using the all switch, or remove the registration cache entry for a single specified endpoint. This command takes the form:

\[\text{clear registration h323 [all | by-alias <endpoint> ]}\]

After you use this command, all affected endpoints will have to register through the Net-Net SBC once again.

You can wildcard user values with the clear-cache registration h323 command.
Session Agent Management

**Manual Registration**

Session agents represent statically defined logical next-hops and previous-hops, for the purpose of providing hostname-to-IP Address resolution. You can provision admission control, constraints, and identification or provisioning properties for each session-agent.

After an endpoint registers to a registrar through the Net-Net SBC, its registration is cached to memory on the system. This cached registration exists for the time indicated by the expiration of the REGISTER response sent from the registrar. If an endpoint sends another REGISTER before the cached registration expires, the Net-Net SBC responds directly to the endpoint, rather than forwarding it to the real registrar. Additionally, if the registrar is configured as a session agent, this association is stored in the contact line within the registration-cache.

The Net-Net SBC includes provisions to explicitly invalidate current registrations in certain instances with the `reset session-agent` command. If the registrar, configured as a session agent, goes out of service, the SBC can invalidate the current endpoint registrations to that session agent. Thus, after resetting the session agent, the Net-Net SBC acts as if the registrations have expired, and forces the endpoints to re-register with the registrar. The command is entered as follows:

```
reset session-agent <session-agent-name>
```

To help identify when session agents have been marked as invalid, the associated session agent for a contact can now be displayed by the `show sip endpoint` ACLI command:

An asterisk '*' is displayed next to the session agent when it is in service and an 'X' is displayed when a session agent failover has occurred or if the session agent has been marked as invalid. For example:

```
ACMEPACKET# show sip endpoint-ip 9
User <sip:9580000001@192.168.201.86>
  Contact ID=1008 exp=597
    UA-Contact: <sip: sipp@192.168.200.254:9004> UDP
    SA=172.16.0.66 *
    SD-Contact: <sip:9580000001-hchse0jm171u2@172.16.10.86:5060>
    real msi:p172
    Call-ID: 1-20622@192.168.200.254'
    Service-Route= <sip:172.16.0.66:5060;lr>'

ACMEPACKET# reset session-agent 172.16.0.66

ACMEPACKET# show sip endpoint-ip 9
User <sip:9580000001@192.168.201.86>
  Contact ID=1008 exp=597
    UA-Contact: <sip: sipp@192.168.200.254:9004> UDP
    SA=172.16.0.66 X
    SD-Contact: <sip:9580000001-hchse0jm171u2@172.16.10.86:5060>
    real msi:p172
    Call-ID: 1-20622@192.168.200.254'
    Service-Route= <sip:172.16.0.66:5060;lr>'
```
**MBCD Management**

MBCD communicates with the networking control portions of the Net-Net OS to coordinate between signaling and media functions. MBCD is generally used to set up and manage media flows.

**MBCD Show Command**

The following `show` commands are used to query MBCD and display real time statistics. The `show mbcd` command usage is as follows:

```
ACMEPACKET# show mbcd [client | server | nat | acl | errors | add | modify | subtract | notify | flows | cams | realms | rules-natalg | sessions-natalg | forked-sessions]
```

**show mbcd client**

The `show mbcd client` command displays statistics related to MBCD transactions when MBCD acts as a client communicating with signaling tasks, acting as servers. For example:

```
ACMEPACKET# show mbcd client
12:08:15-130
MBCD Client                 ---- Recent ---- -------- Lifetime --------
                      Active High Total      Total  PerMax   High
Client Trans              0       0       0      30000    5511      3
Server Trans              0       0       0          0       0       0
Trans Timeouts            -       -       0          0       0       0
Client Sessions           0       0       0      10000    1837     154
Client Errors             -       -       0          0       0       0
Open Streams Failed       -       -       0          0       0       0
Drop Streams Failed       -       -       0          0       0       0
Exp Flow Events           -       -       0          0       0       0
Exp Flow Not Found        -       -       0          0       0       0
```

**show mbcd server**

The `show mbcd server` command displays statistics related to MBCD transactions when MBCD acts as the server communicating with signaling tasks, acting as clients. These counts primarily reflect asynchronous transactions, such as the action to take after a flow guard expiration. For example:

```
ACMEPACKET# show mbcd server
12:08:21-133
MBC Server                 ---- Recent ---- -------- Lifetime --------
                      Active High Total      Total  PerMax   High
Client Trans              0       0       0          0       0       0
Server Trans              0       0       0      30000    5510    1767
Trans Timeouts            -       -       0          0       0       0
Contexts                  1       1       0      10001    1837     155
Flows                     2       2       0      20005    3674     313
Flow-Port                 0       0       0      20000    3674     308
Flow-NAT                  2       2       0       60010   11021     309
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               2       2       0      30005    5511     308
Free Ports                3000    3000       0      43000    7624    3000
Used Ports                0       0       0      40000    7348     616
```
show mbcd nat

The `show mbcd nat` command displays statistics on MBCD’s NAT table transactions. For example:

```
ACMEPACKET# show mbcd nat
12:08:24-136
NAT Entries      ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
NAT Entries    2       2       0      30005    5511     308
Transactions   0       0       0      60008    11020     7
Trans Queued   0       0       0          0       0       0
Trans Timeouts -       -       0          0       0       0
Trans Errors   -       -       0          0       0       0
Adds           -       -       0      30005    5511
Deletes        -       -       0      30003    5510
Updates        -       -       0          0       0       0
Non-Starts     -       -       0          0       0       0
Stops          -       -       0          0       0       0
Expired        -       -       0          0       0       0
ARP Timeouts   -       -       0          0       0       0
```

```
show mbcd acl
```

The `show mbcd acl` command displays statistics on MBCD’s entries in the ACL list. For example:

```
ACMEPACKET# show mbcd acl
12:08:29-142
ACL Entries      ---- Recent ---- -------- Lifetime --------
Active    High   Total      Total  PerMax    High
Static Trusted 0       0       0          0       0       0
Static Blocked 0       0       0          0       0       0
Dynamic Trusted 0       0       0          0       0       0
Dynamic Blocked 0       0       0          0       0       0
App Requests   -       -       0          0       0       0
Added           -       -       0          0       0       0
Removed        -       -       0          3       3       0
Dropped        -       -       0          0       0       0
```

```
show mbcd errors
```

The `show mbcd errors` command displays statistics related to MBCD task errors. The following fields are explained:

- 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.
• 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.

• Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications.

• Stale Ports Reclaimed—Number of ports that were reclaimed when the standby card had a stale flow that the active card replaced; when the flow is replaced, the steering ports are also reallocated properly (i.e., according to the active system).

• Stale Flows Replaced—Number of times that the standby card had entries in its flow tables that did not match those on the active card; the active card replaced the standby’s stale flows with valid ones.

• Pipe Alloc Errors—Number of times that buffer allocation failed for communication between application tasks and middlebox control protocol tasks.

• Pipe Write Errors—Number of times that messages were not sent between the application tasks and middlebox control protocol tasks, possibly because of a pipe/buffer allocation error.

• XCode Alloc Errors—Number of times opening a transcoding session was denied because of no remaining sessions.

ACMEPACKET# show mbcd errors
16:25:20-145
MBC Errors

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Recent</th>
<th>Total</th>
<th>PerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Flow Add Failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Flow Delete Failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Flow Update Failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Flow Latch Failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pending Flow Expired</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Exp CAM Not Found</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Unknown Exp Flow</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop/Exp Flow Missing</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Exp Notify Failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Proprietary & Confidential
show mbcd add

The `show mbcd add` command displays statistics on MBCD's add transactions. Add transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd add
12:08:40-151
--------- Server --------   --------- Client --------
Message/Event    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------
Add Commands          0      10000    1837        0          0       0
Retransmissions       0          0       0        0          0       0
Success               0      10000    1837        0          0       0
Errors                0          0       0        0          0       0

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

show mbcd modify

The `show mbcd modify` command displays statistics on MBCD's modify transactions. Modify transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd modify
12:08:41-154
--------- Server --------   --------- Client --------
Message/Event    Recent      Total  PerMax   Recent      Total  PerMax
------  ---------  ------   ------  ---------  ------
Modify Commands       0      10000    1837        0          0       0
Retransmissions       0          0       0        0          0       0
Success               0      10000    1837        0          0       0
Errors                0          0       0        0          0       0

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

show mbcd subtract

The `show mbcd subtract` command displays statistics on MBCD's subtract transactions. Subtract transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd subtract
```

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
Natm Send Errors      0  0  0
Natm Timeout Errors   0  0  0
Natm Errors           0  0  0
XCode Internal Errors 0  0  0
XCode Alloc Errors    0  0  0
XCode Update Errors   0  0  0
XCode Delete Errors   0  0  0
show mbcd notify

The `show mbcd notify` command displays statistics on MBCD’s notify transactions. Notify transactions only occur when MBCD acts in a client role.

show mbcd flows

The `show mbcd flows` command displays statistics on the contexts and flows MBCD has established. For example:

```
ACMEPACKET# show mbcd flows
Contexts & Flows:
CX=1 ID=1 <1way=1> UDP noQoS
  I=<private=s1/p0:0>0.0.0.0:0,192.168.0.123:5060
  O=<private=s1/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
  14 00:45:50.566

CX=1 ID=2 <1way=2> UDP noQoS
  I=<public=s0/p0:0>0.0.0.0:0,172.16.0.123:5060
  O=<public=s0/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
  14 00:45:50.583

CX=1 ID=3 <1way=3> UDP noQoS
  I=<private=s1/p0:0>192.168.0.10:53,192.168.0.123:0
  O=<private=s1/p0:0>0.0.0.0:0,192.168.0.123:0 SP=6000
  14 00:45:50.583

1 contexts: 3 flows

Note: Do not execute the `show mbcd flows` command on a loaded production system. The output’s load on the Net-Net 9200 could interrupt call processing.
The following explains the **show mbcd flows** output in detail:

![Diagram of application management](image)

**forked calls**

The **show mbcd flows** command displays the "forkedCallId" if the flows belong to a forked session. For example:

```
ACMEPACKET# show mbcd flows
CX=65537.1E | ID=65537-A <1way=a12> UDP/2c noQoS brq=200(f) med=audio <1g>
I=<net200=s0/p3:0>0.0.0.0,192.168.200.85:10000
O=<net1=s0/p2:0>192.168.1.85:10000,192.168.1.139:9200
23 21:04:56.318 last=23 21:04:56.455 other=65538; 4 ports:
192.168.200.85:10000+10001
192.168.1.85:10000+10001
XCode=no:off xE= xW=
2833ACT=NONE 2833InPL=101 2833OutPL=101 2833CLKFRQ=8000 2833INDEX=0
DTIn=0 DTOut=0
DigTypeIn=NONE DigTypeOut=NONE
ForkedCallId:pmultiringcorrelator@192.168.200.139
```

**Note:** Do not execute the **show mbcd flows** command on a loaded production system. The output’s load on the Net-Net 9200 could interrupt call processing.

**show mbcd cams**

The **show mbcd cams** command displays statistics on the flows entries MBCD has entered in the CAM. For example:

```
ACMEPACKET# show mbcd cams
Nat Flows:
UNTRUSTED NAT-ID=1 xop=80:1770 noQoS MP=
 I=1 <private=s1/p0:0>0.0.0.0,192.168.0.123:5060
O=1 <private=s1/p0:0>0.0.0.0,192.168.0.123:5060
UNTRUSTED NAT-ID=2 xop=80:1770 noQoS MP=
 I=2 <public=s0/p0:0>0.0.0.0,172.16.0.123:5060
O=2 <public=s0/p0:0>0.0.0.0,172.16.0.123:5060
UNTRUSTED NAT-ID=3 xop=80:1770 noQoS MP=
```

```
Proprietary & Confidential
```
The following explains the show mbcd flows output in detail:

The information displayed includes the following:

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

You can also add a configured realm name which to display specific information about by using the `show mbcd realms <realm-name>` command. This information is given for period and lifetime durations.

For example:

```
ACMEPACKET# show mbcd realms sip172
18:47:31-2881 Realm=sip172
-- Period -- -------- Lifetime --------
Active  High Total Total PerMax High
Ports Used 2 2 18 18 18 2
```
Free Ports  29999  30001  30017  30017  30017  30001
No Ports Avail  -   -  0   0   0   -
Ingress Band  OK  OK  0   0   0   OK
Egress Band   OK  OK   0   0   0   OK
BW Allocations  0   0   0   0   0   0
Band Not Avail  -  -  0   0   0   -
Total Bandwidth=0K

Steering Ports: 100% Success

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

**show mbcd rules-natalg**

The `show mbcd rules-natalg` command displays the number of configured static flows. Because internally to the Net-Net 9200 a static flow is configured as an ALG NAT entry, they show up here. For example:

```
ACMEPACKET# show mbcd rules-natalg
NatAlg Rules: 0
```

**show mbcd sessions-natalg**

The `show mbcd sessions-natalg` command displays the number of static flow sessions, created as NAT ALG s, listed by protocol.

```
ACMEPACKET# show mbcd sessions-natalg
NatAlg UDP Sessions: 0
NatAlg TCP Sessions: 0
```

**show mbcd forked-session**

The `show mbcd forked-session` command takes a forked call ID argument. This command displays the forkedSession table with the ingress and egress resource table entries. For example:

```
ACMEPACKET# show mbcd forked-session
pmultiringcorrelator@192.168.200.139
ForkedSessionEntry: pmultiringcorrelator@192.168.200.139
InResourceTable:
ForkedSessionResourceEntry: net2001
maxbwallocated = 200
Flows:
Flow id = 65537 bw = 200 bwi = 200 bwe = 200
Flow id = 65539 bw = 200 bwi = 0 bwe = 0

ForkedSessionResourceEntry: net11
maxbwallocated = 200
Flows:
```

Proprietary & Confidential
Flow id = 65538 bw = 200 bwi = 200 bwe = 200
Flow id = 65540 bw = 200 bwi = 0 bwe = 0

OutResourceTable:
ForkedSessionResourceEntry: net11
maxbwallocated = 200
Flows:
Flow id = 65537 bw = 200 bwi = 200 bwe = 200
Flow id = 65539 bw = 200 bwi = 0 bwe = 0

ForkedSessionResourceEntry: net2001
maxbwallocated = 200
Flows:
Flow id = 65538 bw = 200 bwi = 200 bwe = 200
Flow id = 65540 bw = 200 bwi = 0 bwe = 0

**Note:** Do not execute the `show mbcd forked-session` command on a loaded production system. The output’s load on the Net-Net 9200 could interrupt call processing.

### MBCD CPU Load Limiting
See [MBCD Load Limiting](#) for a description on how to enable MBCD CPU load limiting.

### SIP Session Management
You can query and view information about currently established SIP sessions. Because there can be a large number of sessions active at one time, the commands explained in this section may take several seconds to complete. This delay accommodates no net impact on active call processing. If the command requires many seconds to find a match, the system will display status messages to show progress.

All search terms in the following commands are implemented as substring filters. This means sessions matching any part of the string entered will be displayed (i.e., specifying the substring "168" will match sessions with "192.168.1.1" or "1.1.1.1:1680").

**Note:** The `show sip sessions <argument>` command described in this section should not be confused with the `show sip sessions` command, entered without any arguments, which displays cumulative counts of all SIP sessions active on the Net-Net 9200.

**show sip sessions**
The following commands must all begin with `show sip sessions`. All variations of the `show sip sessions` command display one or more SIP sessions entries. The
following is an example of such an output. After specifying the argument, enter a
search term. The following is an sample output of a matching session.

```
Session ID=0-000004 <ESTABLISHED=86398.474>
ingress=private egress=public media=65537 lic (1 dialog)
Call ID=1-6818@192.168.1.211
From=sipp <sip:sipp@192.168.1.211:5060>;tag=1
To=sut <sip:service@192.168.1.85:5060>;tag=1
Client Dialog ID=0-000007 <CONFIRMED>
other=0-000006 ses=0-000004 media=65537 trans=UDP
Call ID=1-6818@192.168.1.211;realm=public
Local=sipp <sip:sipp@192.168.1.211:5060>;tag=1;seq=1
Remote=sut <sip:service@192.168.1.85:5060>;tag=1;seq=0
RemoteTgt=<sip:192.168.200.211:5060;transport=UDP>;UDP
LocalTgt=sip:sipp@192.168.200.85:5060
branch=1elksi45136g35o8r7gs35by0
Server Dialog ID=0-000006 <CONFIRMED>
other=0-000007 ses=0-000004 media=65537 trans=UDP
Call ID=1-6818@192.168.1.211;realm=private
Local=sut <sip:service@192.168.1.85:5060>;tag=1;seq=0
Remote=sipp <sip:sipp@192.168.1.211:5060>;tag=1;seq=1
RemoteTgt=sip:sipp@192.168.1.211:5060;UDP
LocalTgt=<sip:192.168.1.85:5060;transport=UDP>
branch=1elk7h46rr4ckuvh7d0ta9961
Media ID=65537 <Talking|NONE>

Forward codec audio/PCMU p='0' bw='0' fpp='0' param='ptime=10'
peakr='0' avgr='0' mbs='0' sdp-rl='0' sdp-bw='disabled' pref='65536'
Reverse codec audio/PCMU p='0' bw='0' fpp='0' param='ptime=10'
peakr='0' avgr='0' mbs='0' sdp-rl='0' sdp-bw='disabled' pref='65536'
Call Duration (in seconds): 1
```

---

**all**

The **show sip sessions all** command displays all active sessions.

**by-to**

The **show sip sessions by-to** command requires a `<username>` argument and matches this username as a substring to anything found in the “To=” line, after the “=”. For example:

```
show sip sessions by-to <username>
```

**by-from**

The **show sip sessions by-from** command requires a `<username>` argument and matches this username as a substring to anything found in the “From=” line, after the “=”. For example:

```
show sip sessions by-from <username>
```

**by-ip**

The **show sip sessions by-ip** command requires an `<IP>` argument and matches this IP as a substring to anything found in the “RemoteTgt=” line, after the “=”. There can be multiple RemoteTgt lines for a session. For example:

```
show sip sessions by-ip <IP>
```
APPLICATION MANAGEMENT

by-media

The `show sip sessions by-media` command requires a `<media>` argument and matches this text as a substring to anything found in the “MediaID=” section, after the “=” sign. There are multiple pieces of information in this section of a session's description, including transcoding information. For example:

```
show sip sessions by-media <media>
```

by-call-id

The `show sip sessions by-call-id` command requires a `<call-id>` argument and matches this call ID as a substring to anything found in the “CallID=” line, after the “=” sign. There can be multiple CallID lines for a session. For example:

```
show sip sessions by-call-id <call-id>
```

by-agent

The `show sip sessions by-agent` command requires an `<agent>` argument and matches this agent as a substring to anything found in the “From=” or “To=” lines, after the “=” signs. For example:

```
show sip sessions by-agent <agent>
```

Session Agent Registration Management

The Net-Net SBC includes provisions to explicitly invalidate current registrations in certain instances with the `reset session-agent` command. If the registrar, configured as a session agent, goes out of service, the SBC can invalidate the current endpoint registrations to that session agent. Thus, after resetting the session agent, the Net-Net SBC acts as if the registrations have expired, and forces the endpoints to re-register with the registrar. The command is entered as follows:

```
reset session-agent <session-agent-name>
```

Short Duration Session Monitoring

A short duration session is defined as an answered session that has lasts only a short duration. If the number of short duration sessions received exceeds the configurable threshold within the configurable burst window, then an SNMP trap will be sent.

Short session statistics shows up in the `show sip realm` display.

Short Duration Session Trap

You can configure a number of short sessions that fall within a specific window of time that will set the apSysMgmtShortSessionExceedTrap.

ACLI Instructions and Examples

**To configure short duration session monitoring:**

1. In Superuser mode, type `configure terminal` and press <Enter>.
   ```
   ACMEPACKET# configure terminal
   ```
2. Type `session-router` and press <Enter>.
   ```
   ACMEPACKET(configure)# session-router
   ```
3. Type `session-router` and press <Enter>. You can now begin configuring the short duration session monitoring feature.
   ```
   ACMEPACKET(session-router)# session-router
   ACMEPACKET(session-router-config)#
   ```
4. **short-session-duration**—Enter the maximum length of time in seconds that defines a session as short duration. A value of 0 disables this feature.

5. **short-session-threshold**—Enter the number of active sessions, within the short duration window, that must occur to trigger the short session warning trap. A value of 0 disables this feature.

6. **short-session-window**—Enter the length of time in seconds that defines the burst window used to determine if a short session warning trap should be sent.

7. Save your work using the ACLI **done** command.

### Clear SIP and H.323 Sessions

The Clear Sessions function gracefully terminates a group of SIP or H.323 sessions from the ACLI. IWF sessions are considered both SIP and H.323 and can be cleared from either SIP or H.323.

#### Clearing SIP Sessions

The Net-Net 9200 clears SIP sessions by sending BYE messages to the originator and terminator. SIP initial and early sessions are cleared by sending a CANCEL message to the terminator and an error response to the originator.

Only sessions created by INVITE messages may be cleared by this feature, thus subscriptions would not be affected. Sessions in TERMINATED state are not cleared.

#### Clearing H.323 Sessions

The Net-Net 9200 clears H.323 sessions by sending release messages with cmReasonTypeUndefinedReason, reason code 8 (Preemption) to endpoints when clearing them. The CDR terminate-cause for this action is "Admin-Reset".

#### Rate Limiting

As a single clear sessions command could potentially tear down thousands of sessions, the Net-Net SBC's provides a mechanism to moderate the tear down rate as the CPU load grows to high levels. At 0% CPU usage, clear session requests are sequentially performed every 1 ms. At 100% CPU usage, requests are sequentially performed every 500 ms. Clear request intervals are scaled upward as CPU load increases.

#### System State

In order to prevent the Net-Net SBC from creating new sessions as it clears existing sessions, you must set the application protocol of the calls you are canceling in an off-line state. While a protocol is offline, it will not accept new sessions, although administrative tasks may still be performed. When the system state is set to offline, sessions and new registrations are rejected with 503 (SIP) or cmReasonTypeNoBandwidth (H.323) reasons. Established sessions and registrations will be allowed to operate as normal while system state is offline. Omitting the protocol argument ([sip | h323]) puts both protocols in the specified mode. The syntax is as follows:

```
set system-state <online | offline> [h323 | sip]
```

For example:

```
set system-state offline sip
```

### ACLI Instructions and Examples

The clear sessions command is used to gracefully terminate existing sessions. The syntax is as follows:
clear sessions <h323 | sip> <all | by-agent <SA-name> | by-call-id <call-id> | by-ip <ip-addr> | by-user <username>>

- <h323 | sip> - Protocol of sessions to clear. For IWF session, choose one leg of the call to terminate first and use that leg’s protocol.
- all - Clear all sessions for the protocol
- by-agent <SA-name> - Clear sessions originating or terminating from session-agent: <SA-name>
- by-call-id <call-id> - Clear session with call id: <call-id>
- by-ip <ip-addr> - Clear sessions originating or terminating from a client or server dialog URI IP address: <ip-addr> (found in the To:, From” or Contact: headers)
- by-user <username> - Clear sessions originating or terminating from client or server dialog URI username: <username> (found in the To:, From: or Contact: headers)

For example:
ACMEPACKET# clear sessions sip by-ip 192.168.44.55

Show sessions and show virtual-interfaces

The show sessions command allows you to determine the total sessions on the Net-Net 9200 over Period and Lifetime monitoring spans.

The show virtual-interfaces command shows the virtual interfaces for the Net-Net 9200 signaling services; for example, SIP-NAT external address, H.323 interface (stack) IP interface, and MGCP IP interface.

These two commands are useful for determining:
- Total sessions on the Net-Net 9200
- IP addresses in use by protocol

ACLI Instructions and Examples

Show sessions

To display sessions over a period or lifetime:

1. In either User or Superuser mode, type show sessions at the prompt.

ACMEPACKET# show sessions

Session Statistics

<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>0 0 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

IWF Statistics

<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>0 0 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Show virtual-interfaces

To display virtual interfaces for signaling serves:

1. In either User or Superuser mode, type `show virtual-interfaces` at the prompt.

```
ACMEPACKET# show virtual-interfaces
ACMEPACKET > show virtual-interfaces

intf phy-name vlan ip-addr     realm     type
0/0  access   0     172.16.34.131   Realm172  sip-port
1/0  backbone 0     192.168.34.131  Realm192  sip-port
```

SIP Media and Transcoding Statistics

Media-processing statistics per SIP traffic is viewable with the `show sip codecs` command. This command displays statistics per realm and requires a realm argument.

Session Based Statistics

Three statistics are session based. They are the transcoded, transrated, and transparent counts.

- **transcoded**—counts of sessions that use the Net-Net 9200’s TCUs to transcode between two or more codes.
- **transrated**—counts of sessions that use the Net-Net 9200’s TCUs change the packetization interval among dialogs in the session.
- **transparent**—counts of sessions that require no TCU hardware intervention (all end-to-end media uses the same codec)

A value of "none" which is not counted in the statistics is set when there is no media at all or media is not yet negotiated. Sessions within the same realm are counted only once.

These are meter type counters, and thus have an "active" count as well as total lifetime values. The media-processing state of the session only can increase in precedence (highest=transcoded, transrated, transparent, lowest=none). Thus, if a session begins as transcoded, and then is re-negotiated to transparent later by a re-INVITE, it is still considered transcoded. However, if a session begins as transparent, it can go to transcoded by a re-INVITE. In such a case, the total counts for both transparent and transcoded would be incremented. If there are several media lines, the highest precedence is used for the session.

Flow Based Statistics

The remaining 16 lines of the `show sip codecs` command track the number of codecs in established sessions. Only the Recent-Total and other lifetime columns are populated; the Active and Recent High are not applicable. Theses counts represent each SDP m= line emanating in the queried realm. Refer to the following examples:
Example 1

The following diagram shows an intra-realm session with one audio stream using the PCMU codec. Once the session is established, the PCMU count in the `show sip codecs` output is 2.

```
Offer:
m=audio 7000 RTP/AVP 0
```

![Diagram of a session with one audio stream using PCMU codec.]

```
Answer:
m=audio 7000 RTP/AVP 0
```

If the session originator and terminator in the previous diagram exist in two different realms, you must execute the `show sip codecs` command twice, once for each realm. A single PCMU count will be reflected in each respective query because only one m= line emanates from each realm.

Example 2

The following diagram shows an intra-realm session with two audio streams. Each stream uses a different codec. Once the session is established, the PCMU count in the `show sip codecs` output is 2, and the PCMA count is 2.

```
Offer:
m=audio 7000 RTP/AVP 0
m=audio 7001 RTP/AVP 8
```

![Diagram of a session with two audio streams using PCMU and PCMA codecs.]

```
Answer:
m=audio 7000 RTP/AVP 0
m=audio 7001 RTP/AVP 8
```

If the session originator and terminator in the previous diagram exist in two different realms, you must execute the `show sip codecs` command twice, once for each realm. A single PCMU count and a single PCMA count will be reflected in each respective query because two m= lines emanate from each realm.

Example 3

The following diagram shows an intra-realm transcoding scenario where the originator and terminator are using different audio codecs. The Net-Net 9200 is performing transcoding functions, which are invisible to the endpoints. Once the session is established, the PCMU count in the `show sip codecs` output is 1, and the PCMA count is 1.

```
Offer:
m=audio 7000 RTP/AVP 0
```

![Diagram of a transcoding scenario.]

```
Answer:
m=audio 7000 RTP/AVP 8
```

If the session originator and terminator in the previous diagram exist in two different realms, you must execute the `show sip codecs` command twice, once for each realm.
A single PCMU count appears in one query and a single PCMA count appears in the other query because only one m= line emanate from each realm.

An example show sip codecs command follows:

```
ACMEPACKET# show sip codecs public
13:37:29-59 Codec statistics

<table>
<thead>
<tr>
<th>Codec</th>
<th>Recent</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transcoded</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transrated</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transparent</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCMU Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>PCMA Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G722 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G723 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G726-16 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G726-24 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G726-32 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G726-40 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G728 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>G729 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>GSM Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>iLBC Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>H261 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>H263 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>T38 Count</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Other Count</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

QOS Management

QoS Commands

The Net-Net 9200 includes several commands used to debug, validate, and monitor QoS statistic gathering.

show qos errors

The show qos errors command displays debug-level QoS exception statistics. For example:

```
ACMEPACKET# show qos errors

QOS Exception Statistics:

qos delete failed               0
qos_gimp0_err:                 0
qos_gimp1_err:                 0
qos bad control struct:        0
qos update bad handle:         0
qos get handle fail:           0
cross connect failure:         0
qos update - invalid handle:   0
qos add no handle avail:       0
qos free already err:          0
qos update pend err:           0
qos del handle release err:    0
```
show qos statistics

The `show qos statistics` command displays QoS processing statistics. For example:

```
ACMEPACKET# show qos statistics

QoS Processing Statistics:
qos adds received:             0
qos adds completed:            0
qos deletes received:          0
qos deletes completed:         0
```

show qos flow

The `show qos flow` command is used to view live QoS statistics about currently active calls. This command requires a flow ID argument in order to show the flow statistic for a specified call. The flow ID is a hexadecimal value given by the FPGA_handle field as displayed in the `show nat by-index` command.

Reset QoS Statistics

You can reset the accumulated QoS statistics with the `reset qos` command. For example:

```
ACMEPACKET# reset qos
```

Application Load Limiting

SIP Load Limiting

You can set load limiting for all SIP tasks using the `set sip limit` command. The SIP load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of requests that are outside of a dialog. For example:

```
ACMEPACKET# set sip limit 75
```

SIP load limiting can also be configured upon boot within the sip-config. In the options parameter, add `load-limit=<x>`, where x = the load limit percentage.

MBCD Load Limiting

You can set load limiting for the MBCD task using the `set mbcd limit` command. The MBCD load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of flow ADDs. For example:

```
ACMEPACKET# set mbcd limit 75
```

Media load limiting can also be configured upon boot within the media-manager. In the options parameter, add `media-load-limit=<x>`, where x = the load limit percentage.
NATM Load Limiting

You can set load limiting for the NATM task using the `set nat limit` command. When load-limiting is triggered, the Net-Net 9200 drops signaling packets. A value of 0 disables the load limiting function; the default is 80%.

Once NATM task limiting is enabled because of an overload condition, the Net-Net 9200's drop rate scales linearly from 0 to the nat drop rate value at 100% CPU. The NAT drop rate default is 20%. You can optionally set the NAT drop rate using the `set nat limit` command.

NAT load limiting is entered as:

```
ACMEPACKET# set nat limit <limit> [ <nat drop rate> ]
```

NAT load limiting can also be configured upon boot within the media-manager. In the options parameter, add `nat-load-limit=<x>`, where x = the load limit percentage. Add `nat-load-drop=<x>`, where x = the nat load drop rate.

**Note:** natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

SFE Load Limiting

You can set load limiting for the SFE task using the `set sfe limit` command. When load-limiting is triggered, the Net-Net 9200 drops signaling packets. A value of 0 disables the load limiting function; the default is 95%.

Once SFE task limiting is enabled because of an overload condition, the Net-Net 9200's drop rate scales linearly from 0 to the sfe drop rate value at 100% CPU. The SFE drop rate default is 20%. You can optionally set the SFE drop rate using the `set sfe limit` command.

SFE load limiting is entered as:

```
ACMEPACKET# set sfe limit <limit> [ <drop rate> ]
```

SFE load limiting can also be configured upon boot within the media-manager. In the options parameter, add `sfe-load-limit=<x>`, where x = the load limit percentage. Add `sfe-load-drop=<x>`, where x = the SFE load drop rate.

H.323 Load Limiting

You can set load limiting for all H.323 tasks using the `set h323 limit` command. The H.323 load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of requests. For example:

```
ACMEPACKET# set h323 limit 75
```

H.323 load limiting can also be configured upon boot within the h323-config. In the options parameter, add `load-limit=<x>`, where x = the load limit percentage.

Transcoding Management

The Net-Net 9200 includes several commands used to debug, validate, and monitor transcoding sessions.

Xcode Server Commands

One xcode server runs on each the TCU's four cores and is responsible for controlling sessions and resources on each TCM. The following show commands are used to query the xserver and display real time statistics. The `show xserv` command usage is as follows:
show xserv <xserv identified by core> [api-stats | sessstats <session> | stats | sysinfo | dbginfo | devinfo <session> | dsp-events | dsp-channel <device ID> <channel ID> | dsp-device <device ID> | dsp-status <device ID>]

The location argument for the show xserv command works exclusively for: slots 4, 5, and 6; CPUs 0 and 1; cores 0 and 1.

**show xserv stats**

The **show xserv stats** command displays the 10 DSPs’ loads on a TCM. The location argument you supply corresponds with an xserv that control a TCM. It also shows total sessions, created, located, free, allocated, and lost. For example:

```
ACMEPACKET# show xserv 4.0.0 stats
```

```
################# RESOURCE STATS #################
Total Sessions Created = 1000
Total Sessions Located = 1000
Total Sessions FREE    = 0992
Total Sessions ALLOC'd = 0008
Total Sessions Lost    = 0000
Current Device Loading:
  Device00: 00.00%
  Device01: 00.00%
  Device02: 01.00%
  Device03: 01.00%
  Device04: 01.00%
  Device05: 01.00%
  Device06: 01.00%
  Device07: 01.00%
  Device08: 01.00%
  Device09: 01.00%
Max Device Loading:
  Device00: 00.00%
  Device01: 00.00%
  Device02: 01.00%
  Device03: 01.00%
  Device04: 01.00%
  Device05: 01.00%
  Device06: 01.00%
  Device07: 01.00%
  Device08: 01.00%
  Device09: 01.00%
```

**show xserv api_stats**

The **show xserv api_stats** command displays communication statistics about communication between xserver and xclient. For example:

```
ACMEPACKET# show xserv 4.0.0 api_stats
```

```
Xserv Msg/API Stats
++++++++++++++++++++
Total     Alloc's   Update's  Free's    Queries   Register  Heartbeat Dropped
=====     =======   ========  ======    =======   ========= ========= ========
104       8         0         0         3         0         92         0
```
The `show xserv audit-alloc` displays session allocation information about the selected xserver’s sessions. For example:

```
ACMEPACKET# show xserv 4.0.0 audit-alloc

############################ RESOURCE AUDIT ALLOC ########################

Device: 0
Device: 1
Device: 2
Session idx: 0x0000          Session ID: 0x30000000 ALLOCATED
Device: 3
Session idx: 0x0000          Session ID: 0x40000000 ALLOCATED
Device: 4
Session idx: 0x0000          Session ID: 0x50000000 ALLOCATED
Device: 5
Session idx: 0x0000          Session ID: 0x60000000 ALLOCATED
Device: 6
Session idx: 0x0000          Session ID: 0x70000000 ALLOCATED
Device: 7
Session idx: 0x0000          Session ID: 0x80000000 ALLOCATED
Device: 8
Session idx: 0x0000          Session ID: 0x90000000 ALLOCATED
Device: 9
Session idx: 0x0000          Session ID: 0xa0000000 ALLOCATED

Total Sessions Located = 1000
Total Sessions ALLOCATED = 8000
```

The `show xserv audit-free` displays session information about the selected xserver’s free sessions.

The `show xserv audit-lost` displays information about lost sessions, those neither free nor allocated for a selected xserver’s sessions. For example:

```
ACMEPACKET# show xserv 4.0.0 audit-lost

############################ RESOURCE AUDIT LOST ########################

Device: 0
Device: 1
Device: 2
Device: 3
Device: 4
Device: 5
Device: 6
Device: 7
Device: 8
Device: 9
Session idx: 0x0000          Session ID: 0x00000000 ALLOCATED

Total Sessions Located = 1000
Total Sessions LOST = 0000
```
**show xserv audit-full**
The `show xserv audit-full` command displays information about all session on a xserver. Use care in executing this command because the output of this command for a highly loaded xserver can span many screens.

**show xserv api-stats**
The `show xserv api-stats` command shows software/API information for an xserver application. For example:

```
ACMEPACKET# show xserv 4.0.0 api_stats

Xserv Msg/API Stats
====================
Total Alloc's Update's Free's Queries Register Heartbeat Dropped
======= ======= ======== ====== ======= ========= ========= =======
26344 5360 5041 4941 2 0 10994 0
```

**show xserv dbginfo**
The `show xserv dbginfo` displays debug information for various transcoding process counters.

```
ACMEPACKET# show xserv 4.0.0 dbginfo
GetDebugInfo
csmQStats:
  QgetCnt=00000000
  QputCnt=17560000
gtlQStats:
  QgetCnt=17560000
  QputCnt=00000000
TX pktStats:
  csmCnt_t_x_csmwrite =17540000
  csmCnt_t_x_queueblock =17540000
  csmCnt_t_x_addblock =17540000
  csmCnt_t_x_sendblock =17540000
  csmCnt_t_x_Cmddosend =17540000
  csmCnt_t_x_Ackdosend =75300000
  csmCnt_t_x_Sendto =25080000
RX pktStats:
  csmCnt_r_x_readPacket =25080000
  csmCnt_r_x_HandlEPacket =25080000
  csmCnt_r_x_ccontrolPacket =25070000
  csmCnt_r_x_datapacket =00000000
  csmCnt_r_x_noopPacket =10000000
  csmCnt_r_x_csmcallback =17560000
  csmCnt_r_x_MsgQSend =17560000
  csmCnt_r_x_MsgQReceive =17560000
  csmCnt_r_gtlreadcb =17560000
  csmCnt_r_response =17550000
  csmCnt_r_event =10000000
GTL ethStats:
  mSentCount =17540000
  mResentCount =00000000
  mAckableSentCount =17540000
  mAckCount =17540000
```
show xserv session

The `show xserv session` command displays the source and destination IP address and port associated with a transcoded call’s NAT flow. This command requires a session ID argument and is entered in the form:

```
show xserv <slot.CPU.core> session <transcoding_sessionID>
```

For example:

```
ACMEPACKET# show xserv 4.0.0 session 0xa0000

GetSessionInfo() for session: a0000

################# SESSION a0000000 ##################

Channel 0:
Conf ID = 0xa0000000
MSP device = 9
MSP chan = 10
MSP conf = 0
Src IP = 0.0.0.0
Dst IP = 0.0.0.0

Channel 1:
Conf ID = 0xa0000000
MSP device = 9
MSP chan = 11
MSP conf = 0
Src IP = 0.0.0.0
Dst IP = 0.0.0.0
```

show xserv sessstats

The `show xserv sessstats` command displays session Ethernet statistics associated with a given session. It also displays transcoding information about the session. This command requires a session ID argument and is entered in the form:

```
show xserv <slot.CPU.core> sessstats <transcoding_sessionID>
```

For example:

```
ACMEPACKET# show xserv 4.0.0 sessstats 0xa0000

GetSessionStats() for session: a0000

################# SESSION 0xa00000000 ##################

Channel 0:
MSP device = 9
MSP chan = 10
Src IP:Port = 0.0.0.0:0
```
show xserv sysinfo

The `show xserv sysinfo` command displays a high level overview for the given xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 sysinfo

---------------------
XSERVER System Info
---------------------
core ID : 0
cpu ID : 0
slot ID : 0
tile ID : 0
numDevices : 10
numTiles : 1
sessions per DSP: 100
FAX per DSP: 5
Initialized : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax count: 50
Free Sess count: 992
Free Fax count: 50
VAPI Initialized: 1
```

show xserv red-peers

The `show xserv red-peers` command displays redundancy information about this xserver’s redundant peer on a separate TCU. For example:
show xserv devinfo

The `show xserv dev-info` command shows device information for a supplied session running on a defined xserver application. You must supply a session ID for this show command. For example:

```
ACMEPACKET# show xserv 4.0.0 devinfo 0x10000

GetDeviceInfo() for session: 10000
GetDeviceInfo() stub

################# Device Stats  10000000 ##################

Device ID: 0:
    MSP device   = 0

**************************  EMAC Stats  **********************
    RxDroppedPkts     0x00000000
    RxFragPkts        0x00000000

**************************  ETH Stats  **********************
    TxFrames     0x7d76b500
    RxFrames     0x687b2f00
    TxVLANFrames  0x7ae83900
    RxVLANFrames  0x65ebac00
    RxBcastPkts   0x10700000
    RxERIFFrames  0x00000000
    UnknownBcstPkts 0x00000000
    UnknownPktType 0x00000000

**************************  IP Stats  **********************
    TxFrames     0x7ae83900
    RxFrames     0x65eca000
    FragPkts     0x00000000
    BadIPChecksum 0x00000000
    BadUDPChecksum 0x00000000
    UnknownProt  0x9de30000
    UnknownIPAddr 0x99e30000
    UnknownPort  0x00000000
```

show xserv dsp-events

The `show xserv dsp-events` command views the DSP events trace per xserver’s DSPs.

show xserv dsp-channel

The `show xserv dsp-channel` command shows information about a DSP devices selected channel on a given xserver. A DSP device ID and channel ID are required, in addition to specifying an Xserver. The command is entered as:

```
show xserver <core> dsp-channel <device ID> <channel ID>
```

For example:
show xserv dsp-device

The `show xserv dsp-device` command shows information about a DSP device on a given xserver. A DSP device ID is required, in addition to specifying an Xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 dsp-device 0
Supervisor Channel Info for active DSP devices

DSP Device ID: 0
CHANNEL SUPV

channel address      : 0xc20b56bc
device address       : 0xc20b56bc
callback function    : 0x0
request list         : 0xd5d3d0b0
connection ID        : 0x0
connection Type      : 0
connection State     : 0
connection Mode      : 0
MSP Channel ID       : 65535
TDM timeslot         : 0
channel param pointer: 0x0
channel param[0]     : 0xd5daef80
channel param[1]     : 0xd5daf150
Message Index        : 173
Payload Type         : 0
Codec                : 0
```

show xserv dsp-status

The `show xserv dsp-status` command shows information about the TCM’s DSPs which a given xserver controls. A DSP device ID is required, in addition to specifying an Xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 dsp-status 0

DSP Hardware Device Status
```
Xcode Client Commands

The xcode client communicates with the xcode server to request and set up transcoding sessions. The following show commands are used to query the xclient and display real time statistics. The `show xclient` command usage is as follows:

```plaintext
show xclient [api-stats | session-bitinfo | session-byid | session-byipp | session-cache | sessions | status | xlist | xserv-lock]
```

**show xclient status**

The `show xclient status` command displays an overview of the xclient. Information displayed includes the xclient state, number of xservers the xclient connects to, and whether the xclient to xserver communication is synchronous (non-blocking) or asynchronous (blocking). For example:

```
ACMEPACKET# show xclient status
xclient state: Created
xserver count: 8
XClient->XServ msg state: ASYNC
```

**show xclient sessions**

The `show xclient sessions` command displays the number and session ID of cached transcoding sessions. For example:

```
ACMEPACKET# show xclient sessions
Requesting xclient sessions table
Total Active Sessions: 8
Session Id: 0x30000 * cached *
Session Id: 0x40000 * cached *
Session Id: 0x50000 * cached *
Session Id: 0x60000 * cached *
Session Id: 0x70000 * cached *
Session Id: 0x80000 * cached *
Session Id: 0x90000 * cached *
Session Id: 0xa0000 * cached *
```

**show xclient xlist**

The `show xclient xlist` displays the xservers connected to the xclient, and the xservers’ internal IP address and status. For example:

```
ACMEPACKET# show xclient xlist
Requesting XClient's list of XServers:

State  VA_addr                  VC_addr                  Slot    Id   Devices
======  ==================     =================     ====    ==   ======--
Xserv_1: - Not Active/Lost HB.
```

---

### Table

```
<table>
<thead>
<tr>
<th>ID</th>
<th>State</th>
<th>Mode</th>
<th>EthHdrSet</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show xclient session-bitinfo

The show xclient bit-info command displays the session header for a given session. You must supply a session ID for this show command. It is entered as follows:

```
show xclient session-bitinfo <session-ID>
```

show xclient session-byid

The show xclient session-byid command shows session statistics for a supplied session. It is entered as follows:

```
show xclient session-byid <session-ID>
```

show xclient session-byipp

The show xclient session-byipp command shows session statistics for an endpoint’s supplied IP address and port. It is entered as follows:

```
show xclient session-byipp <endpoint IP address> <port>
```

show xclient session-cache

The show xclient session-cache command displays the cached transcoding sessions. It is entered as follows:

```
show xclient session-cache
```

show xclient xserv-lock

The show xclient xserv-lock command shows if the xclient is forced to allocated resources to one xserver. For example:

```
ACMEPACKET# show xclient xserv-lock
xserv lock is not set
```

Realm Management

The following features are used for realm management.

Monthly Minutes-Based CAC Data

The Net-Net SBC’s Call Admission Control (CAC) feature lets you configure the system to put time constraints on incoming networking calls. You can view current monthly minutes CAC data for a specified realm with the show monthly-minutes command. The usage is as follows:

```
show monthly-minutes <realm>
```

By not specifying a realm, data for all realms is displayed. The ACLI show monthly-minutes command displays the following information:

- How many minutes are configured for a realm
- How many of those are still available
- How many calls have been rejected due to exceeding the limit

For example:
### Realm Specifics

You can display configuration information for configuration elements associated with a specific realm with the `show realm-specifics` command. The command’s usage is as follows:

```
show realm-specifics <realm ID>
```

The information displayed includes the following configuration elements associated with the supplied realm:

- Realm configuration
- Steering pool
- Session agent
- Session translation
- Class policy
- Local policy (if the source realm or destination realm is defined)
H.323 Management

The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its H.323 implementation.

H.323 Show Commands

H.323 processing spans several tasks on the Net-Net 9200. The following H.323 show commands display various details of SIP system functionality.

show h323 agentstats

The show h323 agentstats command displays H.323 session agent statistics. For example:

```
ACMEPACKET# show h323 agentstats

H323RasGk@1.4.1
15:22:06-33

<table>
<thead>
<tr>
<th>Session Agent Max Burst</th>
<th>Active</th>
<th>Rate</th>
<th>ConEx</th>
<th>Active</th>
<th>Rate</th>
<th>ConEx</th>
<th>Avg</th>
<th>Max Burst</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.29</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>220</td>
<td>2.8</td>
<td>0.093</td>
<td>0.229</td>
</tr>
<tr>
<td>172.16.0.37</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>172.16.0.38</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>172.16.0.39</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>192.168.200.29</td>
<td>I</td>
<td>220</td>
<td>2.8</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>192.168.200.37</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>192.168.200.38</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>192.168.200.39</td>
<td>I</td>
<td>0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
</tbody>
</table>
```

show h323 all

The show h323 all command displays all H.323 statistics stored on the Net-Net SBC. For example:

```
ACMEPACKET# show h323 all
14:27:42-349168 h323RasGk@0.4.1

H323 SESSIONS        ---- Recent ---- -------- Lifetime -------
Active    High    Total      Total  PerMax    High
Total Sessions                   0       0       0          0       0       0
Total Incoming Sessions         0       0       0          0       0       0
Total Outgoing Sessions         0       0       0          0       0       0
Total Connected Sessions        0       0       0          0       0       0
Total Incoming Channels         0       0       0          0       0       0
Total Outgoing Channels         0       0       0          0       0       0
Incoming IWF Sessions            0       0       0          0       0       0
Outgoing IWF Sessions            0       0       0          0       0       0
IWF Server Transactions         0       0       0          0       0       0
IWF Client Transactions         0       0       0          0       0       0

H323D Status       Current    Lifetime
Queued Messages     0          0
```
show h323 groupstats

The show h323 groupstats command displays H.323 session group statistics. For example:

```
ACMEPACKET# show h323 groupstats

H323RasGk@0.4.1
17:00:10-10

---- Inbound -----  ---- Outbound ----- -- Latency --  Max
SAG          Active  Rate  ConEx  Active  Rate  ConEx    Avg    Max Burst
H323Group     D     0   0.0      0     222  11.7      0  0.112  0.582     8
```

show h323 h323stats

The show h323 h323stats command displays H.323 message statistics. For example:

```
ACMEPACKET# show h323 h323stats

H323RasGk@1.4.1
STACK : h323172
H.225 : Sent 4       Recd 8       maxCPU 0
H245 : Msg 0       Ack 0       Rej 0       Rel 0
RAS   : Req 11      Ack 11      Rej 0       maxCPU 4

STACK : h323192
H.225 : Sent 0       Recd 0       maxCPU 0
H245 : Msg 0       Ack 0       Rej 0       Rel 0
RAS   : Req 0       Ack 0       Rej 0       maxCPU 0
```

show h323 load

The show h323 load command displays H.323 load limiting information. For example:

```
ACMEPACKET# show h323 load
H323RasGk@0.0.0
H323RasGk Load Limit is disabled
```

show h323 registrations

The show h323 registrations command displays H.323 endpoint registrations.
**show h323 stackCallstats**

The `show h323 stackCallstats` command displays H.323 stack call statistics. For example:

```
ACMEPACKET# show h323 stackCallstats

H323RasGk@0.4.1

STACK                Max        Active     Exceeded   InitFail   InFail
OutFail
h323172              0          0          0          0          0          0
h323192              1          0          0          0          1          0
```

**show h323 stackDisconnectInstats**

The `show h323 stackDisconnectInstats` command displays H.323 stack disconnect incall statistics. For example:

```
ACMEPACKET# show h323 stackDisconnectInstats

H323RasGk@0.4.1

STACK          Busy       Normal     Reject     Unreachable  Unknown    Local
h323172        0          0          0          0            0          0
h323192        0          0          0          0            0          1
```

**show h323 stackDisconnectOutstats**

The `show h323 stackDisconnectOutstats` command displays H.323 stack disconnect outcall statistics. For example:

```
ACMEPACKET# show h323 stackDisconnectOutstats

H323RasGk@0.4.1

STACK          Busy      Normal      Reject   Unreachable  Unknown    Local
h323172        0          0          0          0            0          0
h323192        0          0          0          0            0          1
```

**show h323 stackPvtstats**

The `show h323 stackPvtstats` command displays H.323 stack PVT statistics. For example:

```
ACMEPACKET# show h323 stackPvtstats

H323RasGk@1.4.1

STACK                Max        Current    maxUsed
h323172              115470     873        873
h323192              115470     873        873
```

**show h323 status**

The `show h323 status` command displays H.323 server statistics. For example:

```
ACMEPACKET# show h323 status

14:29:47-349292 h323RasGk@0.4.1

H323 SESSIONS                     ---- Recent ---- -------- Lifetime -----
--------------------------------- ----------- -------- ------------- -------
Active    High   Total      Total  PerMax    High
Total Sessions                   0       0       0          0       0       0
Total Incoming Sessions          0       0       0          0       0       0
Total Outgoing Sessions          0       0       0          0       0       0
Total Connected Sessions         0       0       0          0       0       0
Total Incoming Channels          0       0       0          0       0       0
Total Outgoing Channels          0       0       0          0       0       0
Incoming IWF Sessions            0       0       0          0       0       0
```
**Outgoing IWF Sessions**
0 0 0 0 0 0

**IWF Server Transactions**
0 0 0 0 0 0

**IWF Client Transactions**
0 0 0 0 0 0

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

### Resetting H.323 Statistics
You can reset the H.323 statistics counters on the Net-Net SBC by using the `reset h323` command.

```
ACMEPACKET# reset h323
```

### H.323 CPU Load Limiting
See [H.323 Load Limiting](#) for a description on how to enable H.323 CPU load limiting.

### H.323 Stack Monitoring
The H.323 stack/interface configuration provides a way to set one of three alarm thresholds on a per-stack basis, based on the max-calls value. Upon a threshold being crossed the Net-Net SBC will trigger an alarm and an SNMP trap.

To prevent the alarm from firing continuously as call volume through the stack varies, each severity level has an has a reset value below the TCA you set. In addition, each threshold value resets when:

- An alarm with a higher severity is triggered, or
- The built-in reset value for the threshold level is 1% less than the parameter value

### ACLI Instructions and Examples
This section shows you how to configure H.323 stack monitoring for one H.323 stack configuration. This example shows one instance of the alarm-threshold sub-configuration being established; remember that you can set three—critical, major, and minor. Simply repeat the configuration steps to add more severity levels.

**To set up H.323 stack monitoring:**

1. In Superuser mode, type `configure terminal` and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type `session-router` and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type `h323` and press <Enter> to access the global H.323 configuration.

   ```
   ACMEPACKET(session-router)# h323
   ACMEPACKET(h323)#
   ```

4. Type `h323-stack` and press <Enter>. If you are adding H.323 stack monitoring to an existing H.323 stack configuration, then remember you must select the stack you want to edit.

   ```
   ACMEPACKET(h323)# h323-stack
   ACMEPACKET(h323-stack)#
   ```
5. Type `alarm-threshold` and press <Enter> to configure this feature.

```
ACMEPACKET(h323-stack) # alarm-threshold
ACMEPACKET(alarm-threshold) #
```

6. **severity**—Enter the type of severity level for the alarm you want to define. Choose from: critical, major, or minor. This value is required, and defaults to minor.

7. **value**—Enter the percentage of the number of calls defined in the `max-calls` parameter that triggers the alarm. For example, if you want to set a minor alarm to fire when the call rate through the stack reaches half the `max-calls` value, enter 50 (meaning 50%). The default value for this parameter is 0, which disables the alarm.

Remember that if the number of calls falls to below 1% of the `max-calls` threshold you set, the clear trap fires.

8. Save your work.

For example:

```
ACMEPACKET# alarm-threshold
  severity minor
  value 50
ACMEPACKET# alarm-threshold
  severity major
  value 80
ACMEPACKET# alarm-threshold
  severity critical
  value 90
```

---

**Management: ACLI**

This section provides ACLI management information related to the H.323 stack monitoring feature.

**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. As described in the Management: SNMP (241) section below, you can also access this information with an SNMP query.

**Viewing Alarm Information**

Two ACLI commands support this feature, and provide different information:

- **show alarms current**—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.

- **show h323 stack-alarms**—This command refers to specific stacks by stack name, and displays the alarm severity and 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.

```
Management: SNMP
The ap-H323.mib MIB provides the information required to generate a trap and also includes a trap table of current call data for each stack so you can access it externally.

External Policy Servers Management
The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its External Policy Servers and Diameter implementation.

Policy Server Show Commands
The following external policy server show commands display various details of external policy server system functionality.

show policy-server bandwidth
You can view external bandwidth manager statistics with the show policy-server bandwidth command. For example:

ACMEPACKET# show policy-server bandwidth
19:40:28-105 eps@0.1.0
Bandwidth Policy Server

<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>Sockets</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Connections</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Client Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reserve Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Update Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Remove Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Re-Trans</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Install Resp Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reject Resp Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Errors Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Server Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dup Req Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Success Resp Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error Resp Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

You may also add the standby argument to view external policy server statistics on the standby SPU. For example:

ACMEPACKET# show policy-server standby
14:11:41-2957 eps@1.1.0
Bandwidth Policy Server

<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>Sockets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connections</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reserve Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Category</td>
<td>Count 1</td>
<td>Count 2</td>
<td>Count 3</td>
<td>Count 4</td>
<td>Count 5</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Update Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Remove Requests Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Re-Trans</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Install Resp Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reject Resp Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Errors Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Transaction Timeouts</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Server Transactions</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dup Req Received</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Success Resp Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error Resp Sent</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Requests Dropped</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The statistics and display commands described in this section are used for TLS and IPsec.

**TLS Maintenance**

The following commands are used for TLS maintenance and troubleshooting.

**Viewing Certificates**

You can view either a brief version or detailed information about the certificates. The `show security certificates` command has the following syntax:

```
show security certificate [brief | details | list | pem]
```

**show security certificate brief**

Obtaining the brief version uses this syntax, and will appear like the following example:

```
ACMEPACKET# show security certificate brief acmepacket

certificate-record:acmepacket

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 02:13:02:50:00:84:00:71
  Issuer:
    C=US
    ST=California
    L=San Jose
    O=sipit
    OU=Sipit Test Certificate Authority
  Subject:
    C=US
    ST=MA
    L=Burlington
    O=Engineering
    CN=acme
```

**show security certificate details**

Obtaining the detailed version uses this syntax, and will appear like the following example:

```
ACMEPACKET#show security certificate details acmepacket

certificate-record:acmepacket

Certificate:
Data:
  Version: 3 (0x2)
```
show security certificate list

The show security certificate list command lists all installed certificates. For example:

ACMEPACKET# show security certificate list
1: acmepacket

TLS Cache Statistics

You can view the number of entries in the TLS session cache, and then clear this cache as needed.

To view number of entries in the TLS session cache use the following command:

show security tls cache-count

To clear the entries in the TLS session cache use the following command:

security tls cache-clear

IPsec Maintenance

The following commands are used for IPsec maintenance and troubleshooting.

show security ipsec sad

This command shows the security association database entries which are programmed into the IPsec processor. In the case of manual keying, the entries should match that of the running configuration. This command is entered as:

show security ipsec sad [network-interface] <brief | verbose> [selectors]
The [selectors] field allows you to specify which SA entries you would like to display according to the following table:

<table>
<thead>
<tr>
<th>Selector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;enter&gt;</td>
<td>Display all entries</td>
</tr>
<tr>
<td>direction</td>
<td>Direction (IN</td>
</tr>
<tr>
<td>dst-addr-prefix</td>
<td>Destination address prefix, Default: match any</td>
</tr>
<tr>
<td>dst-port</td>
<td>Destination port, Default: match any</td>
</tr>
<tr>
<td>ipsec-protocol</td>
<td>IPsec protocol (AH</td>
</tr>
<tr>
<td>spi</td>
<td>security-policy-index, Default: match any</td>
</tr>
<tr>
<td>src-addr-prefix</td>
<td>Source address prefix, Default: match any</td>
</tr>
<tr>
<td>src-port</td>
<td>Source port, Default: match any</td>
</tr>
<tr>
<td>trans-proto</td>
<td>Transport protocol (UDP</td>
</tr>
</tbody>
</table>

For example:

```
ACMEPACKET# show security ipsec sad M10 brief
IPSEC security-association-database for interface 'M10':

Total number of inbound SA records : 1
Total number of outbound SA records : 1

Displaying SA's that match the following criteria:
   spi             : "any"
   direction       : both
   ipsec-proto     : "any"
   src-addr-prefix : "any"
   src-port        : "any"
   dst-addr-prefix : "any"
   dst-port        : "any"
   trans-proto     : ALL
   vlan-id         : "any"

Inbound, SPI: 257
   destination-address       : 192.168.1.2
   vlan-id                   : 0
   sal-mask                  : 3
   ipsec-protocol            : ESP
   sad-index                 : 0
   encr-algo                 : aes-128-cbc
   auth-algo                 : hmac-sha1
   ipsec-mode                : transport
   match fields:
      src-ip            : 192.168.1.1
      dst-ip            : 192.168.1.2
      src-port          : 0
      dst-port          : 0
      vlan-id           : 0
      trans-proto       : ALL
   mask fields:
```

Proprietary & Confidential
**show security ipsec statistics sad**

This command shows the security policy database entries which are programmed into the IPsec processor. This command is entered as:

```
show security ipsec spd [network-interface]
```

For example:

```
ACMEPACKET# show security ipsec spd M10
Inbound SPD records:
SPD Record, Priority: 0
  action : "ipsec"
  match fields:
    local-ip-addr : 192.168.1.1
    remote-ip-addr : 192.168.1.2
    local-port : 0
    remote-port : 0
    protocol : "all"
    vlan-id : 0
  mask fields:
    local-ip-addr : 255.255.255.255
    remote-ip-addr : 255.255.255.255
    local-port : "disabled"
    remote-port : "disabled"
    protocol : "disabled"
    vlan-id : 0

Outbound SPD records:
SPD Record, Priority: 0
  action : "ipsec"
  match fields:
    local-ip-addr : 192.168.1.2
    remote-ip-addr : 192.168.1.1
    local-port : 0
    remote-port : 0
    protocol : "all"
    vlan-id : 0
```

```
Key Generation

The generate-key command generates keys for the supported encryption or authentication algorithms supported by the Net-Net SBC's IPsec implementation. The generate-key commands generate random values which are not stored on the Net-Net SBC, but are only displayed on the screen. This command is a convenient function for users who would like to randomly generate encryption and authentication keys. The generate-key usage is as follows:

```
security generate-key [hmac-md5 | hmac-sha1 | aes-128 | aes-256 | 3des]
```

IPsec Hardware Statistics

You can query the IPsec processor for hardware identification or Ethernet counts.

show security ipsec statistics gmac

The show security ipsec statistics gmac command displays values for the GMAC interface on an IPsec phy card. You can display either all, or only error, receive, or transmit statistics. This command is entered as:

```
show security ipsec statistics gmac [network-interface] <enter | error | rx | tx>
```

For example:

```
ACMEPACKET# show security ipsec statistics gmac M10
Host 0 Status:
Receive Statistics:
  Total bytes     : 458422
  Total frames    : 1802
  Pause frames    : 0
  Frames < 64 bytes: 403
  Frames 65-127 bytes: 1053
  Frames 128-255 bytes: 5
  Frames 256-511 bytes: 0
  Frames 512-1024 bytes: 4
  Frames 1024-1500 bytes: 336
  Frames > 1500 bytes: 1
Transmit Statistics:
  Total bytes     : 1180666
```
show security status

The `show security status` command displays whether a particular interface on a session-director is IPsec enabled. If so, the hardware status of the security processor will be displayed. This command is entered as:

```
show security status [slot] [port]
```

For example:

```
ACMEPACKET# show security status 1 0
Interface '1, 0' IPSEC hardware status:
  Structure version       = 2
  Payload length (words)  = 8
  Boot ROM code device ID = 0x0025
  Vendor ID               = 0x13a3
  Device ID               = 0x8450
  Hardware version        = 0x0000
  Subsystem type          = 0x00
  Software type           = 0x01
  Major software version  = 0x01
  Minor software version  = 0x02
  Memory config value     = 0x00000000
  System config register  = 0x00000000
  System clock 2 register = 0x00000000
  Saved parity status     = 0x0000
  Current parity status   = 0x0002
  POST test number        = 0x00
  POST sub-test number    = 0x00
  POST test result        = 0x00
  SW major revision       = 0x01
  SW minor revision       = 0x02
  SW maintenance revision = 0x00
```
Protected Password Configuration

In the Net-Net 9200’s configuration files, sensitive data is encrypted with the fixed protected configuration password (PCP). The fixed password provides security and convenience when migrating configurations to different Net-Net 9200s. You can also change the PCP to a password of your own choosing for added security.

Protected Data

The following data within a Net-Net 9200 configuration is protected by the PCP:

1. Security certificate’s private key in the certificate record. This information is imported from the ACLI or imported from a text file. Once imported it is not viewable from the ACLI.
2. IPsec authentication and encryption key in the security association. This information is entered in the security -> ipsec -> manual-security-association configuration element.
3. FTP credentials (login password) for Historical Data Reporting. This information is entered in the system ->collect -> push-receiver configuration element.
4. CDR push-receiver credential (FTP/SFTP login password)
5. LI X1 agent (auth-user and auth-password), SS8 (auth-serial-number)
6. SSH private key

Configuring the PCP

Use the set password config command to change the PCP. Initiating this command walks you through changing the PCP. Remember that your new PCP is subject to the Setting the Password Policy (134) you set. For example:

```plaintext
ACMEPACKET# set password config
WARNING:
Proceed with caution!
Changing the configuration password will result any previous backup/archive configuration file unusable.
The process will also update and activate the configuration once the password is updated
Are you sure [y/n]? : y
Enter old password:
verifying the input password...
password verified

verifying configuration with the password ...
7 cert-record verified
1 sec-assco verified
2 cdr push receiver verified
1 ssh-pub-key-record verified
x1 agent (agent1) credential verified
ss8 agent [ss8] credential verified
the configuration and the password are in sync
Enter new password:
Enter password again:
```

Proprietary & Confidential
Verifying the PCP

You can verify that a password is correct for a configuration before you change the PCP with the `set password config verify <password>` command. If the password you entered matches the active configuration’s password, a confirmation message is printed at the ACLI.

Migrating a PCP-Protected Configuration

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 move
- Net-Net SBC2 is the system to which you want to migrate the configuration from Net-Net SBC1

To migrate a configuration from Net-Net SBC1 (where the password configuration has been set) to Net-Net SBC2:

1. Confirm that you know the protected configuration password for Net-Net SBC1’s configuration.
2. Backup the configuration file on Net-Net SBC1 using the `save backup` command as explained in the Back-up File Management section.
3. Backup the configuration file on Net-Net SBC2 using the save backup command.
4. Download the configuration file on Net-Net SBC1 using an FTP or SCP client.
5. Upload the configuration file to Net-Net SBC2 using an FTP or SCP client.
6. Delete the old configuration file on Net-Net SBC2 using the `delete configuration` command.
7. Use the `set password config verify` to ensure that the PCP password for this moved configuration is correct before activating it.

```
ACMEPACKET# set password config verify
Enter old password:
```

8. Use the `set password config` command to change the configuration password on Net-Net SBC2 to that of the password that protected the Net-Net SBC1’s configuration. See Configuring the PCP (249).

9. Restore the configuration file on Net-Net SBC2 using the `restore backup` command as explained in the Backup File Management (263) section.

10. Activate the configuration on Net-Net SBC2.

### SSH Public Key Support

#### SSHv2 Public Key Authentication

The Net-Net SBC supports importing, generating, viewing, and deleting public keys used for authentication of SSHv2 sessions from administrative remote users.

#### Importing an SSH Host Key

Importing a host key requires access to the SFTP server or servers. Access is generally most easily accomplished with a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

**To import an SSHv2 host key:**

1. Access the SSH file system on a configured SFTP server using a terminal emulation program.

2. Copy the server’s base64 encoded public file, including the Begin and End markers as specified by RFC 4716, *The Secure Shell (SSH) Public Key File Format*.

   For OpenSSH implementations, host files are generally found at `/etc/ssh/ssh_host_dsa_key.pub`, or `etc/ssh/ssh_host_rsa.pub`. Other SSH implementations can differ.

3. Use the `security ssh-pub-key import known-host <name>` command (where `<name>` is an alias or handle assigned to the imported host key, generally the server name or a description of the server function) to import the host key to the SBC.

4. Paste the public key with the bracketing Begin and End markers at the cursor point.

5. Enter a semi-colon (`;`) to signal the end of the imported host key.

6. Save and activate the configuration.
The entire import sequence is shown below.

ACMEPACKET# security ssh-pub-key import known-host fedallah

IMPORTANT:
Please paste ssh public key in the format defined in rfc4716.
Terminate the key with ";" to exit.

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted from OpenSSH by klee@acme54"
AAAAB3NzaC1yc2EAAAABIsIwAAAQEA7OBf08jjeTMSMgerjDTgZpbPbIkrX4n17LOjgPC7cILcDGeTKSiV5MjcsAv3v6AENpZyiOhxz2Zzjismppoo19kkjS5e/ijGstEzqXMMcKU9mBV
qv3iEToqb0wiSsz2AP31GujjTCvRIFXOOxo8A44vH2Cm93/jfNRsnWQ1hmHma2MMTS2LSh04/ilp+pvpsvdo/1V6ftz3eiVfgoxDrjNcVtsAMYLbPdlb69XebQzGSS92TPuRP/yqzLt2G5NFVdxw5i+fvHz1V8dvB5QyZOP//iziu3TA/307tyntB0b7beDylrg64AzC0G7E3AIGh49Lb1Q/"/a=yw==
---- 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

ACMEPACKET# save config

checking configuration

---------------------------------------------------------------------
...
...
...
---------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Current configuration and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.

ACMEPACKET# activate config

Activate-Config received, processing.
waiting for request to finish
SD is not QOS-capable
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
ACMEPACKET#

## Importing an SSH Public Key

Prior to using SSH public key-based authentication you must import a copy of the public key of each user who will authenticate using this method. The public key identifies the user as a trusted entity when the Acme Packet Net-Net SBC performs authentication.

During the SSH login, the user presents its public key to the SBC. Upon receiving the offered public key, the SBC validates it against the previously obtained trusted copy of the key to identify and authenticate the user.

Importing a public key requires access to the device on which the public key was generated, or on which it is currently stored along with its associated private key. Access is generally attained with a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

To import a public key:
1. Access the system from which the public key will be obtained using a terminal emulation program.

2. Copy the base64 encoded public key, including the Begin and End markers as specified by RFC 4716, *The Secure Shell (SSH) Public Key File Format*.

3. Use the `security ssh-pub-key import authorized-key <name>` command (where `<name>` is an alias or handle assigned to the imported public key, often the user’s name) to import the public key to the SBC. For example:

   ```
   ACMEPACKET# security ssh-pub-key import authorized-key key1
   ```

   Use the optional `<"admin">` argument to import a public key who will be authorized for admin privileges. For example:

   ```
   ACMEPACKET# security ssh-pub-key import authorized-key key1 admin
   ```

4. Paste the public key with the bracketing Begin and End markers at the cursor point.

5. Enter a semi-colon (;) to signal the end of the imported host key.

6. Save and activate the configuration.

   The entire import sequence is shown below.

   ```
   ACMEPACKET# security ssh-pub-key import authorized-key Matilda admin
   **IMPORTANT:**
   Please paste ssh public key in the format defined in rfc4716.
   Terminate the key with ";" to exit.
   
   ---- BEGIN SSH2 PUBLIC KEY ----
   Comment: "1024-bit RSA, converted from OpenSSH by abhat@acme74"
   AAAAB3NzaC1yc2EAAAABIwAAAIEAxcYTV595VqdHy12P+mILpeOZx9sX/m5AFiHDyLD
   qjIw6iZ6wmy6H2IxtIC6a+6ZID25mIEdLHa1Y0uknKjC7U5smwzdD4ldLLWZ1brQHZe3b1q
   3Tb8au97jJ1p4ws39PT42C0R0D2P8RkV+0g1NE/83C1y055j8BjC9LEw==
   ---- 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
   ```

--- BEGIN SSH2 PUBLIC KEY ---
Comment: "1024-bit RSA, converted from OpenSSH by abhat@acme74"
AAAAB3NzaC1yc2EAAAABIwAAAIEAxcYTV595VqdHy12P+mILpeOZx9sX/m5AFiHDyLD
qjIw6iZ6wmy6H2IxtIC6a+6ZID25mIEdLHa1Y0uknKjC7U5smwzdD4ldLLWZ1brQHZe3b1q
3Tb8au97jJ1p4ws39PT42C0R0D2P8RkV+0g1NE/83C1y055j8BjC9LEw==
--- END SSH2 PUBLIC KEY ---

Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIGN' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.

ACMEPACKET# activate config
Activate-Config received, processing.
waiting for request to finish
SD is not QOS-capable
Request to 'ACTIVATE-CONFIGN' has Finished,
Activate Complete
ACMEPACKET#

Generating an SSH Key Pair

To generate an SSH key pair you must initially configure a public key record which will serve as a container for the generated key pair.
To configure a public key record:

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 `public-key` and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.
   
   ```
   ACMEPACKET(security)# public-key
   ACMEPACKET(public-key)#
   ```

4. `name`—Enter the name of this public key.
   
   ```
   ACMEPACKET(public-key)# name tashtego
   ```

5. `type`—Select the type of key you want to create. Valid values are `rsa` and `dsa`. The default value is `rsa`.
   
   ```
   ACMEPACKET(public-key)# type rsa
   ```

6. `size`—Enter the size of the key you are creating. Valid key sizes are 512, 1024, or 2048. The default value is 1024.
   
   ```
   ACMEPACKET(public-key)# size 1024
   ```

7. Save and activate the configuration.

To generate an SSH key pair:

1. Enter the `security ssh-pub-key generate` command along with the name of the public key you created in the previous step as follows.
   
   ```
   ACMEPACKET# security ssh-pub-key generate tashtego
   Please wait...
   public-key 'tashtego' (RFC 4716/SECSH format):
   ----- BEGIN SSH2 PUBLIC KEY ----
   Comment: "1024-bit rsa"
   AAAAB3NzaC1yc2EAAAABJxMwAAECgEAIwAAAIEArZEP1/WhYsdGd/Pi8V6pn5wV4cVG4U+jV
   OwI5WNVCC9Nk82I/FKyi1eLZevy9D3Iz8ytvu+sCYyOuK4nHVz20c2N+r86kD
   ru88jkuYapeljDx1AR7181cpr72A1x2L+e7cpreRSXG8bQR7xrU2H3b9jC0VhR
   2fmlcmrGAl7Gnc=
   ----- END SSH2 PUBLIC KEY ----
   ```

2. Copy the base64-encoded public key. Copy the public key including the bracketing Begin and End markers. Shortly you will paste the public key to one or more SFTP servers.

3. Save and activate the configuration.

Copying a Client Key or an SSH or SFTP Server

Copying the client public key to the SFTP server requires server access generally using a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.
1. Use a terminal emulation program to access the SSH file system on a configured SFTP server.

2. Copy the client key to the SFTP server.
   
   On OpenSSH implementations, public keys are usually stored in the
   `~/.ssh/authorized_keys` file. Each line this file (1) is empty, (2) starts with a
   pound(#) character (indicating a comment), or (3) contains a single public key.
   Refer to the sshd manual pages for additional information regarding file format.
   Use a text editor such as `vi` or `emacs` to open the file and paste the public key to
   the tail of the `authorized_keys` file.

For SSH implementations other than OpenSSH, consult the system administrator
for file structure details.

**Viewing SSH Imported Keys**

You can use the `show security ssh-pub-key` command to display information
about SSH keys imported to the SBC with the `ssh-pub-key` command; you cannot
display information about keys generated by the `ssh-pub-key` command. You can
view either a brief version of detailed information about the certificates.

**Viewing a Brief SSH Imported Key Version**

When you use the `show security ssh-pub-key brief [name]` command, the
following information is displayed:

- **login-name**—Contains the name assigned to the RSA or DSA public key when
  it was first imported
- **finger-print**—Contains the output of an MD5 hash computed across the
  base64-encoded public key
- **finger-print-raw**—Contains the output of an MD5 hash computed across the
  binary form of the public key

To view the brief version for all imported SSH public keys:

```
ACMEPACKET# show security ssh-pub-key brief
login-name:
    acme74
finger-print:
finger-print-raw:

login-name:
    fedallah
finger-print:
finger-print-raw:
ACMEPACKET#
```

To view the brief version for a specified imported SSH public key:

```
ACMEPACKET# show security ssh-pub-key brief fedallah
login-name:
    fedallah
finger-print:
finger-print-raw:
ACMEPACKET#
```
ACMEPACKET #

Viewing a Detailed SSH Imported Key Version

When you use the `show security ssh-pub-key detail <name>` command, the following information is displayed:

For an RSA key:

- **host-name**—Contains the name assigned to the RSA key when it was first imported
- **finger-print**—Contains the output of an MD5 hash computed across the base64-encoded RSA public key
- **finger-print-raw**—Contains the output of an MD5 hash computed across the binary form of the RSA public key
- **public key**—Contains the base64-encoded RSA key
- **modulus**—Contains the hexadecimal modulus (256) of the RSA key
- **exponent**—Contains an integer value that is used during the RSA key generation algorithm. Commonly used values are 17 and 65537. A prime exponent greater than 2 is generally used for more efficient key generation.

For a DSA key:

- **host name**—Contains the name assigned to the DSA public key when it was first imported
- **comment**—Contains any comments associated with the DSA key
- **finger-print**—Contains the output of an MD5 hash computed across the base64-encoded DSA public key
- **finger-print-raw**—Contains the output of an MD5 hash computed across the binary form of the DSA public key
- **public key**—Contains the base64 encoded DSA key
- **p**—Contains the first of two prime numbers used for key generation
- **q**—Contains the second of two prime numbers used for key generation
- **g**—Contains an integer that together with p and q are the inputs to the DSA key generation algorithm

To view the detailed version for a specific RSA key:

ACMEPACKET# show security ssh-pub-key detail fedallah

```
host-name: fedallah
comment:
"2048-bit RSA, converted from OpenSSH by klee@acme54"
finger-print:
finger-print-raw:
pub-key:
AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08f08jje7MSMgerjDTgZbpPbxrX4n17LQjgP
C7cLLcDEGfKSIIVt5MjC5Sa3v6AN2zYzihoxd22zismpoo019kkj56s/lGstEzqX
MKHKUr9bVqqlEQTqboWEi5sz2AP31GUjQTCKZRF1XOQx8A4vHZCum93jfNRsn
WQlmHmaZmT2LShOr4jJdIp+PsyvdolmV6Fz5eiVfgoxrDmNcVsAMyLbpDd
L6e9XeQozGzS92TPuKP/yqzLjZ5NVFhXdw5i+FvdHz1vBdvB505y2OPj/iz1u3TA
/307ytB0B7bDylrg64Azc8G7E3AGiH49Lb1Qf/a==
```
modulus: (256)
ECE05FD3C8C978B3132307A88C34E06696CF6E5AD7E27D7B2D26303C2EDC94870
314B44A256DE4CD4CA9BF78FA004376A506662844E959D9CE2B6A8A34D7D9
24279EACFB68C6B2013A9730A1CA528F66055A68A8810E46A6E80C48B933D80
3F7D4652341308A6511755CE41F00E548C7624A6767F37CD46C9D64359A11E
66993264F62D284EAEB27F3635A7EB92FA5DE8955E85B73E5E8957E0A1C6B0
EB8C8D715B6C00CC8B0690DD2F1A7B6D5E6D0CC6492F764CFBA33FCAACCBB2761B9
355161C5D3C98B161F747CF58C176F079D39CB640F86F8BB36D5D303FDCEDDCA
7B4139ED6783C88AEOE8803373C18B137006887E3D2E706D9507FF6B
exponent: (1)
23

ACMEPACKET#

To view the detailed version for a specific DSA key:
ACMEPACKET# show security ssh-pub-key detail acme74
host-name: acme74
comment: DSA Public Key
pub-key: AAAAB3NzaC1kc3MAACABAPY8Z0HY2yFSJ A6XYC9HRwNHaehv5x5W0j OrzZdzoSDxX
bETW6ToHV8D1Uj z/zHo9Flko5xyZnDl aBDHtl bO+Yp7StXyl tHnXf1ylvKD1G4T
6j YrHDYl 140mleg9e4NnCRIeaeq0ZPFIUqFZi a6bXrGTOF3j gq2e7YIsk/gF+fIvAA
AQDob8DsCvWHWTDpdfX0D299Rd7NBvQAAL EAI 9N2+Bb7D4KLkYk3i wRbXbl wXdkPq
g4ApFd W9vGfj 0/Rhd+Nj B4eo 0D+0di xEt nXwG7NPK5R/F XFPNwxHPCacj 9U11i n2
AQW2dskn+i /FAAvi oUPkmDC0zuWoS0E5NhVdtkX3WdvVcGcB9cetzKt OKW0oCj
mj 80qaxTRHtUAAACBN7CY+Kkv1gHpRzFwdOq7KH9bb1LA0Kwa0nd этап fepe NBQ
eSXGlvo+J svphVMB9 c9H5n824YVLVYtsMu74qXvij Yzi VucWkjjKEb11Juqnn0F0D1B3
VVVmxHLmxanAz643WK42Z7dLM5sY29ouez4vXz2PumCh5VGPP+CDqzCM41oWgV

p: (128)
F63C64E1D8DB2152240E97602F47470347C5A7A1BF1E70389D2B2CD9773A12397C
SB115B5A4EB8EF03D5427FCCFECCT7A3D162928E5798670C68B10C7B5B59F0F9B
A784ADC72961DE57C5D582DF0283D46E13E8962B74768D7B3A6DE83D7B836709
195E6AA1935CD5D419F66268A6D7AC64D07F7809AB67BB22B24F0E17ED55

q: (128)
DBF03E5C8F01D64D90CF7D7D03DAF5177B341BD

g: (128)
94DF76F816FB0F828B624DC8C116D76E3C177643E0800E297DBB56F6F19F274FD
11D0DF808C1E1A35OFED1DB81EAD5F060637B3CA4897F1573CD311CF6A9732F
6E2F5267D0859090D8249DFAA2FC008E2A14349931DC3B69A1234B12361
543B37D06765F55C60AFC57ADCBB8E42963A870989F34A9A7714D11ED5
pub_key: (128)
DEC263E2BA8FBFS807A51CC5C1D426EC728D6DB40B2D68AC1A179DA74581EAD63
4114E49718B5ECF8982A6143049731D29F6156262D8CB8E625E8F988F3
8959B5C8A8EE32846FD638A95C5D06E0577555911CB9B19C0FAE3758A3667
B74B33981BDBA2EB73BF85F3D8FB8C721E5518F3FE083AB308CE25A16815

ACMEPACKET#

To view the detailed version for all SSH imported keys:
ACMEPACKET# show security ssh-pub-key detail
Deleting a Public Key Record

This section shows you how to delete a public key record. Note that this process requires you to save and activate your configuration.

To delete an SSHv2 public key record:

1. In Superuser mode, type the command `security 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 delete.

   The Net-Net SBC confirms you have successfully deleted the key, and then reminds you to save your configuration.

   After you complete this procedure, you can confirm the public key has been deleted by using either of the `show security ssh-pub-key` commands.

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

   ```
   ACMEPACKET# security ssh-pub-key delete jdoe
   record (jdoe) does not exist
   ```

2. Save and activate your configuration.
7 Configuration Management

System Configuration Process

Net-Net 9200 Configuration

There are three steps you must follow to proceed from setting a configuration parameter to enabling the Net-Net OS to use the changed parameter.

1. While you are in configuration mode, use the `done` command to save your work. This command saves all changes you’ve made in a configuration element to memory.

2. Once you are satisfied with your edits, save all of them to the current configuration space with the `save config` command. This creates a configuration file that is persistent across reboot.

   In addition, a copy of the previously saved configuration is maintained and labeled as the previous configuration version.

3. Finally, execute the `activate config` command to make the Net-Net 9200 go “live” using the configuration. This is called the running configuration, reflecting the running state of the Net-Net SD.

Configuration Process

The following example walks through configuring one configuration element (ntp), saving the configuration, and then activating the configuration.

To set a configuration element, create a current configuration, and execute the running configuration:

1. Set all the necessary parameters on the SD. Each time you complete configuring a full configuration element, type `done` to save that element.

   ```
   ACMEPACKET(ntp)# server 10.10.10.15
   ACMEPACKET(ntp)# done
   ntp
   server 10.10.10.15
   last-modified-date 2000-01-01 19:15:21
   ```

2. When all configuration elements are set, back out of configuration tree to the topmost ACLI level at the superuser prompt.

   ```
   ACMEPACKET(ntp)# exit
   ACMEPACKET(system)# exit
   ACMEPACKET(terminal)# exit
   ACMEPACKET#
   ```

3. Save all configurations to the current configuration by using the `save config` command.

   ```
   ACMEPACKET# save config
   copying file /code/config/dataDoc.gz -> /code/config/dataDoc_299.gz
   copying file /code/config/tmp/editing/dataDoc.gz -> /code/config/dataDoc.gz
   Save complete
   ```
4. Set the Net-Net SD to enact the current configuration into the running state by using the `activate config` command. This will make the current configuration the running configuration.

   ```
   ACMEPACKET# activate config
   Activate Complete
   ```

---

**Configuration Versions**

The Net-Net SD maintains counts of the running configuration version and current configuration version. It can be helpful to know when the running and current configurations are out of sync.

No matter how many times you increment the current configuration by executing the `save config` command, once you execute the `activate config` command, the current and running configuration versions will be identical.

To check the version of each configuration:

1. Type `show version software` at a command prompt to display the version number of the current configuration.

   ```
   ACMEPACKET# show version software
   NN9200 Software Version:      5.0.0 Beta Workspace (Build 01)
   NN9200 Software Build Date:   07/07/07
   Built in /home/NEOBETA on acme29
   
   Current config version:      301
   Running config version:      300
   ```

---

**Deleting Configurations**

You can completely delete the data in the current configuration with two commands. This can be useful if you want to reconfigure your Net-Net SD starting with a blank configuration.

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
   ```

2. Save and activate the cleared configuration with the `save config` and `activate config` commands.

   **Note:** There is no confirmation for this command.

---

**Displaying Configurations**

The Net-Net OS can display the current and running configurations to the screen. These commands are used to inspect how the Net-Net system is configured.

---

**Configuration Show Commands**

The Net-Net system provides a flexible means for displaying the system configurations with the `show` command.

```
ACMEPACKET# show [config | running-config] [<configuration element> <element identifier>] [<"short">]
```
Basic Show Configuration Usage

The `show config` command displays the current configuration, while the `show running-config` command displays the running configuration. The output of these commands might span several screens.

Show Configuration by Element

Both the `show config` 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 valid configuration elements you can use as an argument are:

- access-control
- account-config
- authentication
- class-policy
- collect
- enforcement-profile
- host-route
- local-policy
- media-manager
- media-policy
- media-profile
- net-management-control
- network-interface
- ntp
- password-policy
- phy-interface
- realm-config
- session-agent
- session-constraints
- session-group
- session-translation
- sip-config
- sip-feature
- sip-interface
- sip-manipulation
- sip-nat
- sip-response-map
- snmp-community
- soap-config
- static-flow
- steering-pool
- surrogate-agent
- system-config
- timezone
- transcoding-policy
- translation-rules
- trap-receiver

If multiple instances of a configuration element are configured, the Net-Net OS will display all elements. In the following example, the two phy-interface instances, private and public, are displayed.

```
ACMEPACKET# show config phy-interface
phy-interface
  name                            private
  operation-type                  Media
  slot                            1
  port                            0
  admin-state                     enabled
  auto-negotiation                enabled
  duplex-mode
  speed
  virtual-mac
  last-modified-date              3000-05-23 17:31:11
phy-interface
  name                            public
  operation-type                  Media
  slot                            0
  port                            0
  admin-state                     enabled
  auto-negotiation                enabled
  duplex-mode
  speed
  virtual-mac
  last-modified-date              2000-05-23 17:31:26
```

**Configuration Element Identifier**

To view a specific instance of a configuration element, you must include the element identifier argument in the `show config` command. The element identifier is usually the `name` parameter of that configuration element. In the following example, only the phy-interface configuration element named `public` is displayed:

```
ACMEPACKET# show config phy-interface public
phy-interface
  name                            public
  operation-type                  Media
  slot                            0
  port                            0
  admin-state                     enabled
  auto-negotiation                enabled
  duplex-mode
  speed
  virtual-mac
```

**Configuration Summary**

By adding the `short` argument to the end of any `show config` or `show running-config` command, the Net-Net system will display an abbreviated output. The short
argument forces the Net-Net OS to display only those parameters that have changed from the defaults. In the following example, parameters which have not been altered from default, duplex-mode and speed, are omitted:

```
ACMEPACKET# show config phy-interface short
phy-interface
  name                            private
  operation-type                  Media
  slot                            1
  admin-state                     enabled
  auto-negotiation                enabled
```

**Backup File Management**

The Net-Net OS saves the full system configuration to a single backup file. You can perform a limited set of actions on backup files, such as saving, backing up, listing, deleting, and restoring the files back to the full system configuration. All backup files are compressed using gzip compression to save disk space.

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. Backups are created as gzipped files in a .gz format. They are stored in the `/code/bkups` directory on the Net-Net 9200.

**Creating Backups**

To create a backup file:

1. In the ACLI at the superuser prompt, enter the `save backup` command followed by a descriptive filename for the backup you are creating. You do not need to add a file extension.

```
ACMEPACKET# save backup 01_July
```

**Listing Backups**

Listing backups is the process of viewing all files in the Net-Net system’s standard backup file directory.

To display backup files:

1. In the ACLI at the superuser prompt, enter the `show backup` command. A list of available backup files from the `/code/bkups` directory is displayed on the screen.

```
ACMEPACKET# show backup
test.gz
bmc_pbrb_20120.gz
bmc_snb_20120.gz
test34.gz
normal.gz
01_July.gz
```

**Restoring Backups**

Restoring a backup writes a backup file’s contents to the current configuration.
To restore a backup configuration:

1. In the ACLI at the superuser prompt, enter the `restore backup` command followed by a backup filename. You must explicitly name the backup file you wish to restore, including the file extension.

   ACMEPACKET# restore backup 01_July.gz

   Need to perform 'save config' and 'activate config' for changes to take effect

   ACMEPACKET#

   You must still save and activate the configuration to apply the backup configuration.

   You can also restore the last saved configuration with the `restore previous` command.

To restore the last saved configuration:

1. In the ACLI at the superuser prompt, enter the `restore previous` command followed by a backup filename. You must explicitly name the backup file you wish to restore, including the file extension.

   ACMEPACKET# restore previous

   Restoring previous configuration dataDoc_001.gz

   Need to perform 'save config' and 'activate config' for changes to take effect

   You must still save and activate the configuration to apply the backup configuration.

Deleting Backups

Deleting backups deletes a specified backup file from the Net-Net 9200’s standard backup file directory.

1. In the ACLI at the superuser prompt, enter the `delete backup` command, followed by the backup file you wish to delete. You must explicitly name the backup file you wish to restore, including the file extension

   ACMEPACKET# delete backup FEB_BACKUP.gz

   ACMEPACKET#

   There is no confirmation warning before executing this command.

Checking Free Space

You can see how much space is available and how much space is currently in use on the code flash.

`show space`

The `show space` command is used to view the amount of flash file space in use and the amount remaining. This command reports flash space on both SPU 0 and SPU 1. For example:

   ACMEPACKET# show space
   Slot 0 filesystem: 215339008/249675776 bytes (86%) remaining
   Slot 1 filesystem: 178262016/249675776 bytes (71%) remaining

   You can also see how much space is available on a CF card plugged into an MIU’s PCMCIA slot with the `show space pcmcia` command. For example:

   ACMEPACKET# show space pcmcia

   /sys: 19695716352/19695749120 bytes (99%) remaining
   /local: 19693335040/19693367808 bytes (99%) remaining
   /logs: 19693335040/19693367808 bytes (99%) remaining
Configuration Inventory Method

The following commands have been enhanced to provide more control when working with configurations:

- backup config
- restore
- show configuration
- show running-config

Backing Up Configurations

You can now specify which configuration you want to back up: the running configuration or the editing configuration. If you execute the backup config command without specifying a configuration type, the Net-Net SBC backs up the last saved configuration by default.

ACLI Instructions and Examples

In this sample, the editing configuration is being backed up.

To back up the editing or running configuration:

1. In Superuser mode, type `save backup` followed by a <Space>, the name of the backup file followed by a <Space>, and the word `editing`. Then press <Enter>.

   If you want to back up the running configuration, you simply type `running` instead of `editing`.

   ```
   ACMEPACKET# save backup 06092008_E.gz editing
   task done
   ACMEPACKET#
   ```

Restoring Configurations

You can restore the last running or the last saved configurations to use as the editing configuration. You use the `saved` or `running` argument with the ACLI `restore` command.

The two kinds of configurations are defined as follows:

- last running—Last copy of the configuration loaded from persistent storage to become the running configuration on the system using the ACLI `activate config` command
- last saved—Last copy of the configuration committed from the editing state to persistent storage on the system using the ACLI `save config` command

These two configurations might represent the same file, which is true when a configuration has been saved and activated. They might also represent different configurations, as is the case when a configuration has been saved but not activated.

Remember to type `save-config` to make the newly-restored last saved config persistent after a reboot, if it has not been activated.

ACLI Instructions and Examples

In this sample, the last running configuration is being restored.

To restore the last running or last saved configurations:
1. In Superuser mode, type \texttt{restore} followed by the word \texttt{running}. Then press <Enter>. This restores the last running configuration. For example:

\begin{verbatim}
ACMEPACKET# restore running
  task done
ACMEPACKET#
\end{verbatim}

To restore the last saved configuration, refer to the following example:

\begin{verbatim}
ACMEPACKET# restore saved
  task done
ACMEPACKET#
\end{verbatim}

**Configuration Inventory**

You can obtain inventory information using updated ACLI commands. The ACLI commands \texttt{show config} and \texttt{show running-config} commands accept an inventory argument. When you use the inventory argument, the system tells you the number of each type of configurations (elements) exist in the configuration.

The Net-Net SBC updates the inventories at these times:

- System boot
- Back-up configuration restoration
- Configuration activation
- Addition or deletion of a configuration element to the editing configuration

When there are no elements, the Net-Net SBC reports the number as zero.

Note that the Net-Net SBC does not compare the contents of these elements, and only top-level elements appear in the count.

**ACLI Instructions and Examples**

To see the inventory for configuration elements on your Net-Net SBC, simply add the inventory argument to either the \texttt{show config} or \texttt{show running-config} ACLI command. The example in this section shows you information for \texttt{show configuration}.

**To see the configuration inventory for show configuration:**

1. At the system prompt, type \texttt{show configuration inventory} and then press <Enter>.

\begin{verbatim}
ACMEPACKET# show configuration inventory
  Current Editing Configuration Inventory:
  Element:                        Count:
  ------------------------------- -------
  access-control                  0
  account-config                  1
  auth-config                     0
  capture-receiver                0
  certificate-record              0
  class-policy                    0
  dns-config                      0
  enforcement-profile             0
  enum-config                     0
  ext-policy-server               0
  h323-config                     0
  h323-stack                      0
  host-route                      1
\end{verbatim}
**Verify Configuration**

The `verify config` command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Net-Net SBC.
When the **verify config** command is run, anything configured that is inconsistent produces either an error or a warning message. An error message lets the user know that there is something wrong in the configuration that will affect the way Net-Net SBC runs. A warning message lets the user know that there is something wrong in the configuration, but it will not affect the way the Net-Net SBC runs. The following is an example of the verify config output:

```
ACMEPACKET# verify config
                                      
ERROR: network-interface [private:0] has reference to phy-interface [private] which does not exist
ERROR: network-interface [public:0] has reference to phy-interface [public] which does not exist
ERROR: sip-nat [northside] is missing home-address entry
ERROR: sip-nat [northside] is missing ext-proxy-address entry
WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects
ERROR: sip-nat [northside] does not have a sip-interface
ERROR: access-control [172.30.12.12; 0.0.0.0; northside] has reference to realm-id [northside] which does not exist
                                      
Total:
6 errors
1 warning
```

Every time a user executes the **save config** command, **verify config** is automatically run. If any configuration problems are found, you receive a message pointing to the number of errors found during the saving, along with a recommendation to run the **verify config** command to view the errors fully. The following is an example of the save config verification output:

```
ACMEPACKET# save config
                                      
Results of config verification:
6 configuration errors
1 configuration warning
Run 'verify config' for more details
                                      
moving file /code/config/tmp/editing/dataDoc.gz ->
/code/config/dataDoc.gz
Save complete
```

### 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:

- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

The following tables display the entire list of addresses which are checked for duplication, the network-interface or realm which they are checked against, and the port range:
### Network-Interface

<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>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>

<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>

### 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 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>

### 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>
</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 (If different from ip-address)</td>
<td>UDP or TCP</td>
<td>realm-id</td>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>host-name (If different from ip-address)</td>
<td>UDP or TCP</td>
<td>realm-id</td>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>ip-address (If different from 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 (If different from 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>
</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-server-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 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 protocol 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 Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</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>
<tr>
<td>Auth-config</td>
<td></td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<tr>
<td>ERROR: auth-config has specified unsupported protocol [x] for type [y]</td>
<td>Unsupported protocols for given type</td>
</tr>
<tr>
<td>ERROR: auth-config has no configured active radius servers for authentication type [x]</td>
<td>No configured active radius for given type</td>
</tr>
<tr>
<td>Capture-Receiver</td>
<td></td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<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>
<tr>
<td>Certificate-Record</td>
<td></td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<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>
<tr>
<td>Class-Policy</td>
<td></td>
</tr>
<tr>
<td>Error Text</td>
<td>Reason for Error</td>
</tr>
<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>
<tr>
<td>Collect</td>
<td></td>
</tr>
<tr>
<td>Error text</td>
<td>Reason for error</td>
</tr>
<tr>
<td>ERROR: collect has sample-interval [x] greater than push-interval [y]</td>
<td>sample-interval greater than push-interval</td>
</tr>
<tr>
<td>ERROR: collect has start-time [x] greater than end-time [y]</td>
<td>start-time greater than end-time</td>
</tr>
<tr>
<td>ERROR: collect has group [xyz] with sample-interval [x] greater than collection push-interval [y]</td>
<td>group [xyz] has incorrect sample interval</td>
</tr>
</tbody>
</table>
### DNS-Config

<table>
<thead>
<tr>
<th>Error text</th>
<th>Reason for error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: 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: collect has no push-receivers defined</td>
<td>no push-receivers defined</td>
</tr>
<tr>
<td>ERROR: 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: collect has reference to push-receiver [xyz] which does not have password set</td>
<td>no password set</td>
</tr>
<tr>
<td>ERROR: collect has reference to push-receiver [xyz] which does not have address set</td>
<td>no address set</td>
</tr>
<tr>
<td>ERROR: collect has reference to push-receiver [xyz] which does not have data-store set</td>
<td>no data-store set</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>
</tbody>
</table>
### CONFIGURATION MANAGEMENT

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>ERROR: ext-policy-server [id] does not have valid operation type</td>
<td>has invalid protocol</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>ERROR: 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/lrt folder</td>
</tr>
</tbody>
</table>

### Manual-security-association

<table>
<thead>
<tr>
<th>Error text</th>
<th>Reason for error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: manual-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 NI table</td>
</tr>
<tr>
<td>ERROR: manual-security-association [id] has invalid local-ip-addr</td>
<td>Invalid local-ip-addr entry</td>
</tr>
<tr>
<td>ERROR: manual-security-association [id] has invalid remote-ip-addr</td>
<td>Invalid remote-ip-addr</td>
</tr>
<tr>
<td>ERROR: manual-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: manual-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: manual-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>
</tbody>
</table>
### Error Text

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ERROR: manual-security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this system's configuration password</strong></td>
<td>failed to decrypt encr-key</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 64 bits (odd parity in hex)</strong></td>
<td>invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 192 bits (odd parity in hex)</strong></td>
<td>invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 128 bits (odd parity in hex)</strong></td>
<td>invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 256 bits (odd parity in hex)</strong></td>
<td>invalid encr-key length for given algorithm</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]</strong></td>
<td>has invalid aes-ctr-nonce for given algorithm</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)</strong></td>
<td>invalid tunnel-mode local-ip-addr</td>
</tr>
<tr>
<td><strong>ERROR: manual-security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)</strong></td>
<td>invalid tunnel-mode remote-ip-addr</td>
</tr>
</tbody>
</table>

### Network-Interface

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist</strong></td>
<td>Phy-interface [xyz] was not found in phy-interface table</td>
</tr>
<tr>
<td><strong>ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty</strong></td>
<td>Dns-domain is empty. Word “address” will be plural “addresses” if there are more DNS addresses entered</td>
</tr>
<tr>
<td><strong>ERROR: network-interface [id] has reference to DNS address, but ip-address is empty</strong></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><strong>ERROR: phy-interface [id] has invalid operation-type value [x]</strong></td>
<td>Operation-type value is invalid</td>
</tr>
</tbody>
</table>
### Public-Key

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: phy-interface [id] has invalid name</td>
<td>If type is MAINTENANCE or CONTROL name has to start with either &quot;eth&quot; or &quot;wancom&quot;</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>

### Realm-Config

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: public-key [id] has not generated public/private key pair</td>
<td>No public/private key generated</td>
</tr>
<tr>
<td>ERROR: public-key [id] has empty private key</td>
<td>empty private key</td>
</tr>
<tr>
<td>ERROR: public-key [id] cannot extract private key</td>
<td>Cannot extract private key</td>
</tr>
<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 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 session-constraints [xyz] which does not exist</td>
<td>session-constraints was not found in session-constraints table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference sip-profile [xyz] which does not exist</td>
<td>sip-profile was not found sip-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference sip-isup-profile [xyz] which does not exist</td>
<td>sip-profile was not found sip-isup-profile table</td>
</tr>
<tr>
<td>ERROR: realm-config [id] has reference transcoding-policy [xyz] which does not exist</td>
<td>transcoding-policy was not found transcoding-policy 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>
</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>

## 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</td>
<td>Empty local-ip-addr-match</td>
</tr>
<tr>
<td>ERROR: security-policy [id] has invalid remote-ip-addr</td>
<td>empty remote-ip-addr</td>
</tr>
<tr>
<td>ERROR: security-policy [id] is missing network-interface entry</td>
<td>missing network-interface entry</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 NI table</td>
</tr>
<tr>
<td>ERROR: security-policy [id] priority [xyz] is identical to security-policy [id2] priority</td>
<td>priority duplication</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 in-translationid [xyz] which does not exist</td>
<td>translation id was not found in translation 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 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 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>ERROR: session-agent [id] has reference sip-profile [xyz] which does not exist</td>
<td>sip-profile was not found in sip-profile table</td>
</tr>
<tr>
<td>ERROR: session-agent [id] has reference sip-isup-profile [xyz] which does not exist</td>
<td>sip-isup-profile was not found in sip-isup-profile 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>
</tbody>
</table>

**SIP-Config**

<table>
<thead>
<tr>
<th>Error text</th>
<th>Reason for error</th>
</tr>
</thead>
<tbody>
<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 [$INTERNAL$]</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>
</tbody>
</table>
### Error text

<table>
<thead>
<tr>
<th>Error text</th>
<th>Reason for error</th>
</tr>
</thead>
<tbody>
<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 object 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>
<tr>
<td>ERROR: sip-config [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-config [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>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] is missing tls-profile entry</td>
<td>sip-port missing tls-profile entry when protocol is TLS or DTLS</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-interface [id] has reference sip-profile [xyz] which does not exist</td>
<td>sip-profile was not found in sip-profile table</td>
</tr>
<tr>
<td>ERROR: sip-interface [id] has reference sip-isup-profile [xyz] which does not exist</td>
<td>sip-isup-profile was not found in sip-isup-profile table</td>
</tr>
<tr>
<td><strong>ERROR text</strong></td>
<td><strong>Reason for error</strong></td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing name</td>
<td>name missing from the object</td>
</tr>
<tr>
<td>WARNING: %SIP_MANIP% has name which contains invalid characters</td>
<td>name has invalid characters</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% has invalid reject status code</td>
<td>invalid reject status code</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing new-value entry</td>
<td>missing new-value entry</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% has new-value that refers to itself from sip-manipulation [xyz]</td>
<td>sip-manipulation calling itself in a loop</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing mime-header-name</td>
<td>missing mime-header-name</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing content-type</td>
<td>missing content-type</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% has sub-rule with invalid type</td>
<td>sub-rule with invalid type</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing parameter-name</td>
<td>missing parameter-name</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% has invalid type</td>
<td>invalid type</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% is missing header-name</td>
<td>missing header-name</td>
</tr>
<tr>
<td>ERROR: %SIP_MANIP% has sub-rule with invalid type</td>
<td>sub-rule with invalid type</td>
</tr>
<tr>
<td>ERROR: sip-manipulation requires a name</td>
<td>name missing</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [xyz] name overlaps with built-in-sip-manipulation name</td>
<td>name overlaps with built-in-sip-manipulation name</td>
</tr>
<tr>
<td>ERROR: sip-manipulation [xyz] has no header-rules defined</td>
<td>no header-rules defined</td>
</tr>
</tbody>
</table>

In order to cover all the possible cases for each entry %SIP_MANIP% was used instead of the actual path for the individual errors and warnings. At this time the path could have two or three levels of depth with each level separated with "from" string as shown below:

- header-rule [hr-name] from sip-manipulation [test]
- element-rule [ser-name] from header-rule [hr-name] from sip-manipulation [test]

In the case of missing name for the object only CLI name will be show for any error or warning as shown below:

ERROR: header-rule from sip-manipulation [test] is missing name
# 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>
<tr>
<td>WARNING: sip-nat [id] checking is aborted because home-realm is missing or invalid</td>
<td>sip-nats are configured, but home realm in sip-config is missing</td>
</tr>
<tr>
<td>WARNING: sip-nat [id] checking is aborted because home-realm sip-port is invalid</td>
<td>associated sip-interface has no sip-ports and sip-nat is missing home-address entry</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] for TFTP ALG</td>
<td>Invalid protocol entry</td>
</tr>
<tr>
<td>ERROR: ext-policy-server [id] has illegal protocol value [xyz] for NAPT ALG</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 NI 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>

### TLS-Profile

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Reason for error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR: tls-profile [id] is missing end-entity-certificate entry</td>
<td>missing end-entity-certificate entry</td>
</tr>
<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] 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 no trusted-ca-certificates, but mutual-authentication is enabled</td>
<td>no trusted certificates, but enabled mutual-authentication</td>
</tr>
</tbody>
</table>
Overview

You can upgrade your Net-Net 9200 software so that there is no impact or interruption to service.

Net-Net OS S-D7.1.0 Upgrade Prerequisites

Caution: The bootloader MUST be upgraded to bootloader package SWR-0012-00r2p03.tar prior to loading any Net-Net OS version S-D7.1.0 image/baseline of nnSD710b4 or later on the Net-Net 9000. This bootloader is backward compatible to all D600, D700, D710b3 or earlier images.

After upgrading the bootloader, on the next reboot the new bootloader will be running. This can be verified with the `show version hardware` command.

For X86 processors (SPU2/NPU2) the bootloader should be dated:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Cpu</th>
<th>Core</th>
<th>Boot Loader Rev</th>
<th>CPLD1 Rev</th>
<th>CPLD2 Rev</th>
<th>Memory Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>09/27/2010</td>
<td>2.0.1</td>
<td>2.0.2</td>
<td>3029MB</td>
</tr>
</tbody>
</table>

For MIPS processors (SPU1/NPU1/TCU1) the bootloader should be dated:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Cpu</th>
<th>Core</th>
<th>Boot Loader Rev</th>
<th>CPLD1 Rev</th>
<th>CPLD2 Rev</th>
<th>Memory Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>09/27/2010</td>
<td>c.3.2</td>
<td>Unknown</td>
<td>1024MB</td>
</tr>
</tbody>
</table>

Caution: It is advised to upload NN9200 Diagnostic Image SWR-0016-00, Rev 2.05 (filename: nnD_diags205.tar) or greater to the Net-Net 9200's `/code/images` directory before upgrading the bootloader. Older diagnostics images will not work with the 09/27/2010 bootloader.

Automatic Online Upgrade

System upgrades are the process of loading a new OS image on the Net-Net 9200. You can load either a newer (upgrade) or older (downgrade) version of the Net-Net OS compared to what is currently running on your system. This section uses the term upgrade interchangeably for an upgrade or downgrade. Bootloader images can be found on the Acme Packet Support Portal.
When upgrading the Net-Net 9200, the upgrade manager determines if the incoming OS is compatible with the existing OS, hardware, and bootloader. The upgrade manager then precedes or halts the upgrade based on the comparison.

System upgrade can be performed without interrupting service. This feature is referred to as an online software upgrade and can only be performed on a Net-Net 9200 with redundant hardware.

**Upgrade Overview**

During an upgrade, the SPU you initiate the upgrade from goes out of service and reboots with the new image. Before the reboot, you will be prompted to reconnect to the other SPU/MIU and continue guiding the upgrade to completion.

Upgrading from a remote (Telnet or SSH) session is not necessary but is advised because during the upgrade the system displays status messages on the console, which can interfere with your ability to clearly read instructional text. Monitoring console output on both active and standby SPU/MIUs is essential to observe and visually log the system during upgrades.

The upgrade manager guides you through the complete process, offering you the opportunity to confirm and proceed, or halt roll back the upgrade at the following key points.

- After the first reset
- After the first switchover
- After the second reset

At the completion of the upgrade, you can choose to commit, or rollback the upgrade. Committing the upgrade completes the upgrade process, leaving the system running a new image. Rolling back the upgrade reverts the system to its pre-upgrade state.

After the system has been upgraded, the SPUs, NPUs, and TCUs will have switched roles, relative to their pre-upgrade state.

**Upgrade Path**

To perform an online software upgrade to a newer or older release, your Net-Net 9200 must be running a version that is compatible with the release you are upgrading or downgrading to. This upgrade requirement is known as the roll-through. Roll-through releases are often used as a bridge when upgrading between major OS releases. If you are not running a compatible version, you must first upgrade your system to a valid roll-through.

Please contact TAC to confirm compatibility between your target upgrade software release and your current release.

**Note:** You can still upgrade from any image to any other image with an offline upgrade or by changing the boot parameters and rebooting, but this action results in a system-wide loss of service.

**Online vs. Offline**

You can perform an online upgrade or an offline upgrade.

- Online upgrade—the system remains in service during the procedure with no loss of connected calls and minimal disruption of calls in transient states.
- Offline upgrade—the system performs a hard reset of all cards, resulting in the loss of any and all traffic present.
Both the online and offline upgrades are invoked similarly. After the upgrade begins, the ACLI informs you if the system is sufficiently redundant to perform an online OS upgrade. If the Net-Net 9200 is redundant, you can choose either an online or offline upgrade. If the Net-Net 9200 is insufficiently redundant, you can only perform an offline upgrade.

A Net-Net 9200 is considered redundant if each SPU/MIU pair, NPU, or TCU has at least one standby. NIUs are not reset in the OS upgrade process and thus need not be redundant.

**Duration**

The time needed to complete an OS upgrade depends on:

- Whether the upgrade is online or offline
- Whether an image is located on the Flash RAM, or is downloaded from the network
- The type of image downloaded
- The types of processing units (cards) present

The following times should only be used as an estimate:

- Download a system image: ~3 minutes
- Perform online upgrade with 7 cards: ~15 minutes
- Perform offline upgrade: ~ system reset time

**Note:** The download duration must be added to the upgrade time. If the image booted from the network, just the upgrade time can be used as an estimate.

**Net-Net 9200 Software Upgrade**

This section describes how to perform the upgrade procedure.

**Virtual Management Interface**

To simplify the upgrade, configure the Net-Net 9200's bootparams with a virtual management interface. A virtual management interface is a single IP address that connects you to the active SPU/MIU. To configure and view the virtual management
interface’s IP address, view the final section of a show bootparams system query. For example:

```
ACMEPACKET# show bootparams

Boot parameters stored on ACTIVE SPU:

--- Slot 0 Boot Parameters ---
<...>
--- Slot 1 Boot Parameters ---
<...>
--- Virtual Management Interface Parameters ---

Interface IP Address: 172.30.92.96
Gateway IP Address: 172.30.0.1
ACMEPACKET#
```

The virtual management interface IP address follows the active SPU/MIU after a switchover by binding to the active SPU/MIU’s MAC address. This means that you can open a remote ACLI session to this address to initiate the upgrade, and when the SPU/MIU pair switches over and you are disconnected from the Net-Net 9200, you can open a new remote ACLI session to the same address to continue the upgrade.

**Netmask Requirement**

If you configure a virtual management interface on your Net-Net 9200, and you wish to specify the netmask for the management IP addresses:

- You must explicitly configure the netmask for MIU0’s IP address (inet on ethernet), MIU1’s IP address (inet on ethernet), and the virtual management IP address (inet on ethernet).
• These three IP addresses must exist within the same network and use the name bitmask.

ACMEPACKET# set bootparams

Please specify boot parameters for Slot 0:

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

boot device : eth2
processor number : 0
host name : nethost
file name : /tftpboot/nnSD700m6p1.tar
inet on ethernet (e) : 172.30.251.55:ffff0000
inet on backplane (b):
host inet (h) : 172.30.0.125
gateway inet (g) : 172.30.0.1
user (u) : abcftp
ftp password (pw) (blank = use rsh): abcftp
flags (f) : 0x0
target name (tn) : ACMEPACKET
startup script (s) :
other (o) :

Please specify boot parameters for Slot 1:

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

boot device : eth2
processor number : 0
host name : nethost
file name : /tftpboot/nnSD700m6p1.tar
inet on ethernet (e) : 172.30.251.54:ffff0000
inet on backplane (b):
host inet (h) : 172.30.0.125
gateway inet (g) : 172.30.0.1
user (u) : abcftp
ftp password (pw) (blank = use rsh): abcftp
flags (f) : 0x0
target name (tn) : ACMEPACKET
startup script (s) :
other (o) :

Please specify virtual management IP parameters:

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

inet on ethernet (e) : 172.30.251.54:ffff0000
gateway inet (g) : 172.30.0.1

Boot parameters have been updated and will take effect on the next reboot.
**Note:** The above bootparameters are applicable for an SPU 1. SPU 2-based systems use a bootdevice of eth0.

**File Location Prerequisites**
The previously-booted image file, i.e., the image file currently running, must remain present in its original boot location until the upgrade is complete.

**Upgrade from Flash**
If the previously-booted image file was on the Net-Net SBC’s flash, it must remain at the original path with the original filename until the upgrade has successfully completed.

In addition, the image file must also exist on the other SPU at the same path and with the same filename. By convention, you should ensure that the target image file is available on both SPUs in the same absolute location too. For example, if you are upgrading from nnSD700m2.tar to nnSD700m3.tar from flash:

```
SPU0: /boot/nnSD700m3.tar
     /boot/nnSD700m2.tar
SPU1: /boot/nnSD700m3.tar
     /boot/nnSD700m2.tar
```

**Note:** When uploading image files to the Net-Net SBC’s SPUs, be sure to connect directly to SPU0 and SPU1 using their individual static IP addresses and not the virtual management IP address.

**Upgrade from Network**
If the Net-Net SBC was previously-booted from an FTP server, you must ensure that the booted image file remains available at the same network location from where it was originally booted.

For example, if the system's currently booted image is nnSD700m2.tar located on 192.168.20.22 in the /bootimages directory, the same named file must be available at the same address and path when performing an upgrade to later image file, regardless of where the target image file is located.

**Process Overview**
The following list outlines the major steps that make up an online upgrade.

- Determine if the system can accommodate online upgrade based on redundancy configuration
- Retrieve and validate new OS compatibility with hardware, bootloader, and current running version
- Load new software onto standby cards by resetting them
- Verify upgraded cards are stable and healthy in standby roles
- Switchover to newly upgraded cards
- Load new software only previously-active cards by resetting
- Verify upgraded cards are in a healthy standby state
- Perform third TCU upgrade if applicable
- Commit the upgrade
To begin an online upgrade, configure the Net-Net 9200 to upgrade from either:

- local flash OS image file
- FTP server based OS image file

If you are upgrading from an FTP server, you can choose to boot directly from the downloaded image file or to save the image file first to local flash storage, then boot from there. By downloading to flash first, the OS image file remains locally available after the Net-Net 9200 is rebooted.

You can specify a path in the image file name if the image file is not located in the FTP account's root location.

The `upgrade os` command syntax is as follows:

```
upgrade os <file name> [<FTP server IP> <username> <password>] <flash | network>
```

### Boot From Local Image File

To upgrade from an OS image file located on the local file system:

You must specify the full path to the image file name. For example, if the OS image file exists on the active SPUs' `/code/images` directory, use the following syntax to start the upgrade:

```
ACMEPACKET# upgrade os /code/images/nnD600m4.tar
```

This syntax upgrades the OS software to the image contained in the file `/code/images/nnD600m4.tar`.

Continue to the Redundancy Check (292) section.

### Boot From FTP Server

To upgrade from an OS image file located on an FTP server:

1. If the OS image is on a remote FTP server and you want the Net-Net 9200 to boot directly from that system, use the following syntax to start the upgrade.

   ```
   ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 user password network
   ```

   Continue to the Redundancy Check (292) section.

### Download and Boot From Remote Image File

You can download an OS image in advance of the upgrade, and optionally postpone the upgrade until a suitable time without network dependency. If you direct the upgrade manager to download the OS image file from a network server, you can specify to download the file to the local file system. Image files are downloaded to both SPUs' `/code/images` directory. When fully retrieved, the system then boots from this locally stored file.

To download OS image file located on an FTP server to both SPUs and boot from there:
TO DOWNLOAD AN OS IMAGE FROM A REMOTE FTP SERVER AND THEN BOOT FROM IT LOCALLY, USE THE FOLLOWING SYNTAX:

ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password flash
Preparing for upgrade ...

System is fully redundant and ready for upgrade.

Starting download ...
UPGRADE: Download has started, please stand by...
SPU1 : '+'
SPU0 : '*'
++++++*****+++++++++++++++*****+++++++++++++++*****+++++++++++++++*****+++++++++++++++*****
++++++*****+++++++++++++++*****+++++++++++++++*****+++++++++++++++*****+++++++++++++++*****
Download finished.

Keep system in service during upgrade [y/n]? n

* * * Continuing this upgrade will INTERRUPT SERVICE.

Continue with OFFLINE upgrade [y/n]? n
Upgrade cancelled.

ACMEPACKET#

NOTE: As the file is downloading, hash marks are printed on the screen in the form of *'s and +s. The *'s indicate a portion of the file being written to the active SPU and the +s indicate the file as written to the standby SPU. If this succeeds, the OS image is written to both the active and standby SPUs' file systems.

Continue to the Redundancy Check (292) section.

Redundancy Check

After instructing the Net-Net 9200 to begin an OS upgrade, the system indicates whether or not it is sufficiently redundant to perform an online upgrade without an interruption in service. A Net-Net 9200 is considered redundant if each active processor unit (front panel card) has at least one standby.

ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password network
Preparing for upgrade ...

System is fully redundant and ready for upgrade.

If the hardware cannot support a live upgrade, the user will be warned of an interruption.

ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password network
Preparing for upgrade ...

*** System is NOT redundant. ***
There will be a LOSS OF SERVICE for this upgrade.
After you configure the Net-Net 9200 with an OS image boot location (and optionally download it to the local file system), and you have chosen either an online or offline upgrade, you are prompted to begin the upgrade.

**Note:** Minimize network traffic during an online upgrade.

---

**Caution:** An offline upgrade is service-interrupting and fails all traffic currently flowing over the Net-Net 9200.

---

### Offline Upgrade

To perform an offline upgrade on a redundant system, reply **N** <enter> to the prompt that questions if you want to perform an online upgrade. The system will offer to perform an offline upgrade at the next prompt.

```
ACMEPACKET# upgrade os /code/images/nnD600m4.tar
Preparing for upgrade ...
System is fully redundant and ready for upgrade.

Keep system in service during upgrade [y/n]?: n

* * * Continuing this upgrade will INTERRUPT SERVICE.

Continue with OFFLINE upgrade [y/n]?: y
Upgrade in place, ready to reboot!
```

### Online Upgrade

To perform an online upgrade on a redundant system, reply **Y** <enter> to the prompt that questions if you want to perform an online upgrade. The Net-Net 9200 will begin the upgrade process immediately.

```
System is fully redundant and ready for upgrade.

Keep system in service during upgrade [y/n]?: y
UPGRADE: Loading current release information...
UPGRADE: Exploding new OS tarball...
UPGRADE: Upgrade files in place...
UPGRADE: Ready to load version D6.0.0m4 04/01/09
UPGRADE: Performing first reset of standby cards...
UPGRADE: Parsing new manifest
UPGRADE: Received info for new task eps.
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x4a

Standby upgrade complete. Ready to perform first switchover.
```
First Switchover

The upgrade begins after you choose either an online or offline upgrade. The ACLI displays all upgrade messages with the `UPGRADE:` or `DOWNGRADE:` prefix. These messages inform you of the upgrade’s progress and prompt you for required action. In addition, the active SPU’s console session can be monitored for general system output as the system transitions through the phases of a full upgrade (switchovers, resets, etc.).

The first upgrade milestone is after the standby cards reboot with the new image. Type `y <enter>` at this point to continue. For example:

```
...  
UPGRADE: Ready to load version D6.0.0m4 04/01/09
UPGRADE: Performing first reset of standby cards...
UPGRADE: Parsing new manifest
UPGRADE: Received info for new task eps.
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x4a

Standby upgrade complete. Ready to perform first switchover.
```

```
Continue [y/n]?: y
continuing...
UPGRADE: Synchronizing peer Upgrade Manager...
UPGRADE: Synchronizing SNR database with peer...
UPGRADE: Starting switchover....
UPGRADE: Switching over TCU in slot 4 by resetting...
```

The Upgrade Manager pauses at certain milestones to prompt you for confirmation that the system is stable and to allow the upgrade to continue. Answering `No` to any of the `Continue` prompts starts an OS rollback. The `upgrade cancel` command will rollback any upgrade in progress if the ACLI is not waiting for a response or prompting you for a response. Use `<CTRL + C>` to break and then use the `upgrade cancel` command.

**Note:** The `UPGRADE:` or `DOWNGRADE:` prompts change to `ROLLBACK:` once a rollback has been initiated.

When the SPU/MIU that you initiate the upgrade from is ready to reboot with the new OS image, the ACLI alerts you must re-login to the other SPU/MIU to continue...
the upgrade process. If you are connected to a virtual management IP, you will be
disconnected due to the changeover.

UPGRADE: Synchronizing peer Upgrade Manager...
UPGRADE: Starting switchover....
UPGRADE: Switching over TCU in slot 4 by resetting...
UPGRADE: Slot 4 has transitioned to the STANDBY state...
UPGRADE: Initiating switchover of slot 2 to standby...
UPGRADE: Slot 2 has transitioned to the STANDBY state...
UPGRADE: Initiating switchover of slot 0 to standby...
UPGRADE:

*** You are connected to an SPU which is about to become STANDBY.
*** Please log in to the MIU in slot 1
    and type 'upgrade resume' to continue the upgrade.

Shortly after the last line is printed to the ACLI, if you are connected through a
virtual management IP address, this Telnet or SSH session is terminated by the Net-
Net 9200 and the SPU reboots.

Second SPU
Connection

Connect to the active SPU/MIU using either the virtual management IP address or
the static IP address for the appropriate SPU. Log in to the Net-Net 9200 and enter
superuser mode. At this point, type upgrade resume <enter> to continue the
upgrade. The Net-Net 9200 prompts you to continue with the upgrade. Type y
<enter>, and the upgrade continues. For example:

Running acliT1
Password:
ACMEPACKET> en
Password:

ACMEPACKET# upgrade resume
UPGRADE: Resuming in-progress os upgrade from state WAIT_RESUME_ACTIVE [OS]

Switchover complete. Ready to perform second virtual upgrade.

Continue [y/n]? y
continuing...

UPGRADE: Exploding OS tarball...
UPGRADE: Upgrade files in place...
UPGRADE: Continuing upgrade to version D6.0.0m4 04/01/09...
UPGRADE: Resetting standby cards.
UPGRADE: Parsing new manifest
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x15

Upgrade Completion

After the upgrade completes, you are prompted to commit the upgrade.
Type y <enter> and the ACLI prints messages confirming the final cleanup on the screen. At this point you have completed the online upgrade.

A Net-Net 9200 should never be left with more than one OS version running across all cards. After each card reset, and before each switchover, the Net-Net 9200 checks that all active images are the expected version. If there is a version mismatch, the upgrade manager will rollback the upgrade. If you find that mixed OS versions exist on complimentary cards when an upgrade is not in progress, then you must reset any cards that are not running the version specified in the bootparams. Redundancy allows this without interruption. Use the `show version software all` command to confirm like OS versions on all cards. Use the `upgrade status` command to see if an upgrade is in progress.

**Canceling an Upgrade**

Canceling an upgrade stops the upgrade in progress and begins a rollback to the previous version. The rollback resembles an upgrade but the process functions roughly in reverse and results in the entire system running the original release.

To cancel an upgrade, break out of the upgrade process using <ctrl> + C. Then issue the `upgrade cancel` command. Do not use this command unless the system is stable (i.e., not resetting or switching over). All cards should be in either active or standby state only.

**Upgrade Cancellation Warning**

Issuing `upgrade cancel` while an upgrade is already being canceled, results in the upgrade process halting, leaving the system in an undefined state. This should only be used to regain control of an unstable system, i.e. to reset cards by hand. If this
command is issued during a rollback, a warning will be issued and the user must confirm the desire to abort the rollback. For example:

```
ACMEPACKET# upgrade cancel

*** WARNING :
*** You are about to ABORT this rollback.
*** This will leave the system in an undetermined state,
*** which may require manual intervention to correct.
*** Choose 'y' to continue with abort, 'n' to allow rollback to finish.

Continue [y/n]?: y
continuing...
```

Choosing n to this prompt results in the 'upgrade cancel' command returning without interrupting the rollback. If the rollback is aborted, the following message advises the user to manually check and possibly manually restore the proper running versions to all cards:

```
ROLLBACK:

*** Rollback ABORTED !!
*** Note that all cards may not be running the correct software version.
*** Use 'show version software all' to determine which cards to reset.
```

```
ACMEPACKET#
```

**Upgrade Support Tools**

The following tools can aid you in the upgrade process.

**Useful ACLI Commands**

The following ACLI commands are useful during the upgrade procedure.

- **show version software**—Displays running version information on all or specified processor units (cards) in the system. In the case of an aborted or failed upgrade, the show version command can determine which cards have and have not been upgraded.

  ```
  show version software [slot # | all]
  ```

- **show version hardware**<slot #>—Displays installed hardware part numbers for system or an individual card. Use this command to query your system and determine hardware / software compatibility before beginning an upgrade. Please contact TAC for hardware / software compatibility.

- **switchover**—Swaps activity state of a specified card with its redundant card.

  ```
  switchover <slot #> [active | standby]
  ```

- **show health**—Displays the health score and status of all installed cards on the Net-Net 9200. To view the health of a particular card, include the slot number.
After printing the system health to the ACLI, the show health command also displays a redundancy history (not shown below). For example:

```
ACMEPACKET# show health
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>Health Score</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>50</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>100</td>
<td>STANDBY</td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>FNCTRL 0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>14</td>
<td>FNCTRL 1</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>15</td>
<td>POWER0</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>16</td>
<td>POWER1</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>17</td>
<td>POWER2</td>
<td>100</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>18</td>
<td>POWER3</td>
<td>Not Installed</td>
<td></td>
</tr>
</tbody>
</table>

Redundancy Event List

Local File Space

If there is insufficient storage space for the OS image on either SPU, the system displays a warning message on the ACLI. In this event, you can only upgrade the system without copying the file locally, i.e., upgrade from FTP server.

If a like-named file already exists, you will be prompted to accept overwriting it with the new download. To free local file system disk space, use the following commands:

- **show images**—Lists image files located in the `/code/images` directory on SPU0 and SPU1.

  ```
  ACMEPACKET# show images
  Images stored on SPU 0:
  nnD600m3p3.tar 3693560 bytes
  Images stored on SPU 1:
  nnD600m3p3.tar 3693560 bytes
  ```

- **delete image**—Deletes a selected image file from the `/code/images` directory on a specified SPU.

  ```
  delete image image_name [SPU number]
  ```

  For example:

  ```
  ACMEPACKET#delete image nnD600m3p3.tar 0
  ```

Upgrade Commands

This section defines ACLI commands used for upgrade.

- **upgrade status**—Shows the upgrade manager’s current state: what type of upgrade is in progress, what stage it is in.
• **upgrade cancel**—Cancels an upgrade in progress by starting a rollback. Do not use this command unless the system is stable (i.e., not resetting or switching over). All cards should be in either active or standby state only.

• **upgrade resume**—Resumes an upgrade in progress. The ACLI might prompt you to continuing waiting or will repeat the last question if still pending.

### Suspending Upgrade Output

The upgrade process continues separately from the ACLI session and command that is directing it.

You can exit the upgrade command’s output without terminating the upgrade by typing `<ctrl> + c`. This allows you to use the current ACLI session to inspect the system’s state, run a new command, or resume the upgrade.

You can then issue the `upgrade resume` command from the ACLI to continue where you left off. If the upgrade manager is waiting for user input, the question is reprinted on the terminal upon resuming the upgrade. If the upgrade manager is processing, and not waiting for user input, then resuming the ACLI session displays any progress messages.

### Net-Net 9200 Bootloader Upgrade

Upgrading a bootloader is the process of updating the flash memory with the executable code that each CPU uses to boot when the system is powered on.

You can load either a newer (upgrade) or older (downgrade) version of the bootloader compared to the version currently running on your system. This section uses the term upgrade interchangeably for an upgrade or downgrade.

The upgrade manager validates hardware compatibility between the bootloader package and the current hardware. It then precedes or halts the upgrade based on the comparison.

Bootloader upgrades can be performed without interrupting service. Redundant cards do not need to be present for a bootloader upgrade. However, after cards are inserted into the system, you may need to perform a bootloader upgrade again for these new cards.

### Bootloader Upgrade Precautions

Because a failed bootloader upgrade might render the Net-Net 9200 unbootable, special precautions must be taken when upgrading:

- The Net-Net 9200 disables HA switchovers when upgrading the bootloader. Therefore, ensure that the environmental and network conditions are minimized so that switchover-inducing-events do not occur.
- Perform all upgrades during low traffic periods.
- Ensure that both power supplies are powered by individual, backed-up circuits.

### Duration

The time needed to complete an bootloader upgrade varies based on the number of cards that are present. The following times should only be used as an estimate:
• Download a bootloader package: ~10 seconds
• Perform upgrade with 7 cards: ~ 2 minutes

Bootloader File Location
The Net-Net 9200 can upgrade the bootloader from either a locally stored bootloader package or a bootloader package located on an FTP server.

On Local Filesystem
Use an FTP client to upload the bootloader package file in the Net-Net 9200’s /code/images directory.

Note: Upload the bootloader package file to both SPUs.

On FTP Server
When the bootloader package file is booted from the FTP server, it is first downloaded to the active SPUs’ /code/images directory. The ACLI will notify you if there is insufficient storage space on the active SPU for the bootloader package file.

Not enough space to copy release to flash. You may need to make space using the ‘show|delete images’ commands.

The Net-Net 9200 then aborts the bootloader upgrade. You must free disk space by deleting files to continue. See the Backup File Management (263) section for how to fix this. If a like-named file already exists, you will be prompted to accept overwriting it with the new download.

Process Overview
The following list outlines the major steps that make up an online upgrade.
• Configure system to install bootloader from local filesystem or from FTP Server
• Commit bootloader upgrade

Upgrade Procedure Command Syntax
This section explains how to perform the bootloader upgrade procedure. Use the upgrade bl command to start the bootloader upgrade process. The upgrade bl command is entered as follows:

```
upgrade bl <filename> <card> [ <ip address> <username> <password> ]
```

- filename—bootloader package path and filename.
- card— all - upgrade all cards | 0-6 - specific processor card to upgrade

When upgrading the bootloader from file on an FTP server, you must supply the following additional credentials:

- ip address—IP address of FTP server
- username—username for FTP server
- password—password for FTP server

Upgrade Bootloader From Local File
To upgrade the bootloader from a local bootloader package file:

1. At the superuser prompt, type the command using the following syntax to begin bootloader upgrade from a local bootloader package file. You must specify the absolute path on the Net-Net 9200’s flash RAM in the upgrade bl command:

```
ACMEPACKET# upgrade bl /code/images/SWR-0012-00r2p01.tar all
```
Preparing for upgrade ...

***** WARNING: Do NOT powerdown, remove, or reset any card *****
Continue to the Commit Bootloader Upgrade (301) section of the documentation.

Upgrade Bootloader From FTP Server

To upgrade the bootloader from a bootloader package file on an FTP server:

1. At the superuser prompt, type the command using the following prototype to begin bootloader upgrade from a local bootloader package file. You must specify the absolute path on the Net-Net 9200’s flash RAM in the upgrade bl command:

```
ACMEPACKET# upgrade bl SWR-0012-00r2p01.tar all 172.30.0.34 username password
```

Preparing for upgrade ...
Starting download ...
SPU1 : ‘*’
***
...
Download finished.

***** WARNING: Do NOT powerdown, remove, or reset any card *****
Continue to the Commit Bootloader Upgrade (301) section of the documentation.

Commit Bootloader Upgrade

To commit the bootloader upgrade:

1. Type y <enter> to confirm that you want to begin the update process. From this point you may NOT remove power from the system.

```
Continue [y/n]? : y
slot 0 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 1 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 2 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 3 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 4 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 5 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 6 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01

Slot 0 successfully upgraded.
Slot 1 successfully upgraded.
Slot 2 successfully upgraded.
Slot 3 successfully upgraded.
Slot 4 successfully upgraded.
Slot 5 successfully upgraded.
Slot 6 successfully upgraded.
```

Slot 1 successfully upgraded.
Slot 2 successfully upgraded.
Slot 4 successfully upgraded.
Slot 3 successfully upgraded.
Slot 0 successfully upgraded.

Upgrade Completed.

Verify the Bootloader Upgrade

After each CPU’s bootloader is successfully upgraded, the device’s revision number is updated too. Each card’s functional revision is updated by appending an A to the functional revision number. This A designation is not viewable from older versions of the Net-Net software.

You can verify the upgrade by using the `show version hardware <card>` command. This command displays the bootloader that the Net-Net 9200 is currently booted with, i.e., the current runtime. The bootloader is indicated by date. For example, you can query card 0, SPU0. Observe the bootloader revision date for each CPU’s core 0:

```
ACMEPACKET# show version hardware 0
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Cpu</th>
<th>Core</th>
<th>Boot Loader Rev</th>
<th>CPLD1 Rev</th>
<th>CPLD2 Rev</th>
<th>Memory Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>09/10/2008</td>
<td>0.3.2</td>
<td>0.0.8</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>N/A</td>
<td>0.3.2</td>
<td>0.0.8</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>09/10/2008</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
<td>09/10/2008</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>0</td>
<td>09/10/2008</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>0</td>
<td>09/10/2008</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1024MB</td>
</tr>
</tbody>
</table>

You can view more information by using the `show version hardware` command for the whole system. This show command displays which bootloader, by version will be used to boot the Net-Net 9200 on next reboot (or restart).

When you upgrade the bootloader, the version number for the xx-xx40-xx device will change, but the date in the `show version hardware` command only changes after the system has been rebooted.

Notice the xxx-xx40-xx programmable device is at a higher revision than before the upgrade.

```
ACMEPACKET# show version hardware
```

<table>
<thead>
<tr>
<th>Type</th>
<th>Part Number</th>
<th>Serial Number</th>
<th>Func Rev</th>
<th>Artwk Rev</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPU0</td>
<td>002-0507-50</td>
<td>060712001671</td>
<td>4.11A</td>
<td>4.00</td>
</tr>
</tbody>
</table>

Programmable Devices:

1. 004-0025-xx Rev: 4.00
2. 004-0028-xx Rev: 1.10
3. 004-0029-xx Rev: 1.04
4. 004-0030-xx Rev: 1.01
5. 004-0031-xx Rev: 1.00
6. 004-0040-xx Rev: 2.01
TCU/TCM Upgrade

Hardware Upgrade Recommendation
When planning to upgrade transcoding hardware (TCUs and TCMs) in your Net-Net 9200 system, you should bias your equipment allocation toward 3 TCUs with fewer TCMs rather than 2 TCUs and maximized TCMs. This recommendation enables hitless upgrades for future increases in channel density.

Single to Double Active TCU Upgrade
Upgrading from a single active TCU configuration to a double active TCU configuration is not dynamically supported by the Net-Net 9200 and requires a reboot. The general procedure is:

1. Remove the blank TCU panel from the Net-Net 9200 System Chassis.
2. Insert the new TCU into the system.
3. Wait until the TCU is recognized and settles to the “OOS” state by using the `show status` command.
4. Set the system-config configuration element’s `tcu-double-active` parameter to `enabled`.
5. Reboot the system.

**Note:** See the Net-Net 9200 TCM Installation Guide (401-0106-00) for all prerequisites, requirements and procedures for this maintenance.

Offline Transcoding Hardware Maintenance
Removing TCMs from an TCUs is not a hitless procedure. To efficiently remove TCMs from a system, you should drain active traffic from the system and re-route it through an alternate Net-Net system if possible.

Hitless TCM Upgrades
Adding TCMs to existing TCUs can be preformed without affecting existing service. This is considered a hitless upgrade. The following overview lists how to perform a TCM upgrade with no impact to active transcoded sessions.

**Note:** Fan packs and power supply listing in show status commands are removed for brevity.

Definitions

- **1+1 Redundancy:** 1 Active TCU with 1 Standby TCU that can assume all transcoding traffic in the event of a failure.
- **2+1 Redundancy:** 2 Active TCUs with 1 Standby TCU that can assume up to half the transcoding traffic in the event of a failure.

Please have the Net-Net 9200 TCM Installation Guide (401-0106-00) on hand for reference and additional procedural explanations.
1. Identify the standby TCU by using the `show status` command.

   **ACMEPACKET# show status**

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>UNCONFIGURED</td>
<td>UNASSIGNED</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Note that TCU0 in slot 4 is the Active TCU, while TCU1 in slot 5 is in standby role.

   Verify that the expected number of TCMs are present on the active TCU with the `show xclient xlist` command. The following screen shot shows two active xservers, which control 2 TCMs, on the active TCU.

   **ACMEPACKET# show xclient xlist**

   Requesting XClient's list of XServers:

<table>
<thead>
<tr>
<th>VA_addr</th>
<th>VC_addr</th>
<th>Slot</th>
<th>Id</th>
<th>DSPs</th>
<th>#Sess</th>
<th>Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>XServ_1: 169.254.178.0</td>
<td>169.254.164.0:8012</td>
<td>4</td>
<td>0</td>
<td>10</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>XServ_2: 169.254.178.1</td>
<td>169.254.164.1:8012</td>
<td>4</td>
<td>0</td>
<td>10</td>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>Xserv_3: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_4: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_5: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_6: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_7: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_8: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xserv_9: -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Verify 2 TCMs are present on the standby TCU with the `show xserv 5.0.0 sysinfo` and `show xserv 5.0.1 sysinfo` commands. In the following screen shot,
the TCU in location A is present. The following screen shot omits querying TCM B, `show xserv 5.0.0 sysinfo`, which would be preformed in this procedure.

```
ACMEPACKET# show xserv 5.0.1 sysinfo
System not initialized for an active context.
Displaying STANDBY system information:

XSERVER System Info for Context #0
----------------------------------------------
core ID : 0
cpu ID : 0
slot ID : 0
tile ID : 2
numDevices : 10
numTiles : 1
sessions per DSP: 100
FAX per DSP: 5
Initialized : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax count: 50
Free Sess count: 985
Free Fax count: 50
VAPI Initialized: 1
----------------------------------------------
XSERVER System Info for Context #1
----------------------------------------------
core ID : 0
cpu ID : 0
slot ID : 0
tile ID : 2
numDevices : 10
numTiles : 1
sessions per DSP: 100
FAX per DSP: 5
Initialized : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax count: 50
Free Sess count: 1000
Free Fax count: 50
VAPI Initialized: 1
```

When querying the standby TCU to ascertain which TCMs are present, use the `show xserv xx.x sysinfo` command. Each time you execute this command for an xserver on a standby TCM, two contexts will be reported. The following table lists the core-to-TCM mapping:

<table>
<thead>
<tr>
<th>Core to query</th>
<th>Tile ID reported in software</th>
<th>Physical TCM location</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.0.0</td>
<td>0</td>
<td>C</td>
</tr>
<tr>
<td>x.0.1</td>
<td>2</td>
<td>A</td>
</tr>
</tbody>
</table>
The following image shows physical TCM location relative to the TCU:

2. Remove the standby TCU from the Net-Net 9200. In the following show status screen shot, note that TCU1 in Slot 5 has been removed.

<table>
<thead>
<tr>
<th>Core to query</th>
<th>Tile ID reported in software</th>
<th>Physical TCM location</th>
</tr>
</thead>
<tbody>
<tr>
<td>x1.0</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>x1.1</td>
<td>3</td>
<td>B</td>
</tr>
</tbody>
</table>

The following image shows physical TCM location relative to the TCU:

ACMEPACKET# show status

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>UNCONFIGURED</td>
<td>UNASSIGNED</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Add new TCMs to the TCU you removed from the Net-Net 9200 chassis by following the procedure in the TCM Installation section of the Net-Net 9200 TCM Installation Guide.

Caution: You must adhere to the mandatory TCM installation order illustrated on page 9 of the Net-Net 9200 TCM Installation Guide.

4. Reinsert the upgraded TCU by following the procedure in the TCU Replacement section of the Net-Net 9200 TCM Installation Guide.

5. Execute the show status command to confirm that the upgraded TCU has progressed through the normal progression of states until it reaches “CARD
RUNNING” state in the STANDBY role. This can take several minutes depending on the number of transcoded sessions that must be replicated across the redundant card. For example:

### ACMEPACKET# show status

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>UNCONFIGURED</td>
<td>UNASSIGNED</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Execute the `show xserv 5.x.x sysinfo` command, described in Step 3, to confirm that all new TCMs have properly powered up and are operating correctly.

7. Remove the active TCU, TCU0 in Slot 4. This forces TCU1 to become active and assume all transcoding traffic.

### ACMEPACKET# show status

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>UNCONFIGURED</td>
<td>UNASSIGNED</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ACMEPACKET# [RM: SPU Slot=0] - TCU in Slot 5 Assuming Active Role

ACMEPACKET# [SM: Slot=0] - Got ACTIVE COMPLETE from CM cm@5.0.0

ACMEPACKET# [RM: SPU Slot=0] - TCU Slot 5 has transitioned to ACTIVE

8. Add new TCMs to the TCU you removed from the Net-Net 9200 chassis by following the procedure in the TCM Installation section of the Net-Net 9200 TCM Installation Guide.
Caution: The TCMs on each card must be placed in the SAME physical locations for all TCUs for redundancy. All TCUs in the system must have the SAME number of TCMs.

9. Reinsert the upgraded TCU by following the procedure in the TCU Replacement section of the Net-Net 9200 TCM Installation Guide. The following appears as the card boots and assumes operation:

ACMEPACKET# [SM: Slot=0] - Got READY from CM cm@4.0.0
Card in Slot 4 Transitioning to Standby Role
[SM: Slot=0] - Got STANDBY COMPLETE from CM cm@4.0.0
[RM: SPU Slot=0] - TCU Slot 4 has transitioned to STANDBY

10. Execute the show status command to confirm that the upgraded TCU has progressed through the normal progression of states until it reaches “CARD RUNNING” state in the STANDBY role. This can take several minutes depending on the number of transcoded sessions that must be replicated across the redundant card. For example:

ACMEPACKET# show status

<table>
<thead>
<tr>
<th>Slot</th>
<th>Type</th>
<th>State</th>
<th>Role</th>
<th>Temperature</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>1</td>
<td>SPU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>NPU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>3</td>
<td>NPU1</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>4</td>
<td>TCU0</td>
<td>CARD RUNNING</td>
<td>STANDBY</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>5</td>
<td>TCU1</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>TCU2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>MIU0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>MIU1</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHY0</td>
<td>CARD RUNNING</td>
<td>ACTIVE</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>PHY1</td>
<td>UNCONFIGURED</td>
<td>UNASSIGNED</td>
<td>Normal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>PHY2</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>PHY3</td>
<td>Not Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11. Execute the `show xserv 4.x.x sysinfo` command, described in Step 3, to confirm that all new TCMs have are operating correctly.

Upgrade Procedure: 2+1 Redundancy

This abbreviated procedure is for upgrading TCUs running in a 2+1 configuration. Please reread the previous section for background about this procedure.

1. Remove the standby TCU from the Net-Net 9200.

2. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide

3. Replace the upgraded TCU in the Net-Net 9200.

4. Execute the `show xserv x.x.x sysinfo` command to confirm that all new TCMs are operating correctly.
5. Choose the second TCU to upgrade.

6. Ensure that each TCU’s State is “Card Running” in either ACTIVE or STANDBY role.

7. Remove the second TCU from the Net-Net 9200.

8. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide

9. Replace the upgraded TCU in the Net-Net 9200.

10. Execute the `show xserv x.x.x sysinfo` command to confirm that all new TCMs are operating correctly.

11. Ensure that each TCU’s State is “Card Running” in either ACTIVE or STANDBY role.

12. Remove the third, upgraded TCU from the Net-Net 9200.

13. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide

14. Replace the upgraded TCU in the Net-Net 9200.

15. Execute the `show xserv x.x.x sysinfo` command to confirm that all new TCMs are operating correctly.
Index

A

ACL table statistics 166
acme messaging protocol 96
Acme Packet Log Enumeration 25
acmelog 26
  configuration 26
  FTP retrieval 40
  location 27
add ARP table entry 165
alarm port 46
alarms 43–51
  application 66
  attributes 43
  categories 44
  clearing 50
  configuration 67
  displaying 49
  filtering 49
  hardware 54
  media 65
  network 64
  response table 46
  severity levels 44
  system 58
  system responses 45
ARP statistics
  resetting 166
ARP table addition, manual 165
ARP table statistics 161–164

B

backup configuration 263
backup configuration location 263
backup file
  creating 263
  deleting 264
  displaying 263
  restoring 264
BCM 56K switch ports 132

C

CAM entries 213
card status 116
check arp table 165
cfg config version
  current & running 69
configuration
  deleting 260
  process 259
  versions 260
configuration archive 263
configuration of system 259
cores
  switching between 132

display configuration 260
  summary 262

E

Ethernet interfaces 159

F

facility logging
  configuration 30
facility types 41
fan status 116
fault severity levels 25
flows, current 212

G

GMAC statistics 125, 176
generic display 46, 67
INDEX

H

hardware statistics 115
HIP statistics 179
resetting 179

I

IP address
ACL info 167
lookup per interface 177

L

licenses 71
Log File Message Levels 25
log file types
acmelog 25
process log 25
log files
compression 33
deletion 34
FTP retrieval 39
rotation 33
size 33
text insertion 34
trace log 34
log levels 25
logtype facility 26

M

MBCD application statistics 208–212
media interface statistics 174
mirroring 132

N

NAT Statistics 169
NAT table display 171
network interface statistics 174, 177
NPU statistics 123–127

P

panic log dump 36
period based statistics 75
ping 181
power supply status 116
process log 29

Q

QoS statistics 224
by flow 224

R

realm statistics 214
redundancy statistics 114
reliable datagram protocol 109

S

session management 74
show commands
ACL 166
amp 101–108
arp 163–164
bootparams 70
clock 70
config 261
configuration 260
cpu 72
HIP 179
manifest 73
MBCD 208–215
media 174–178
NAT 169–174
npu 124–126
rdp 109–113
running-config 261
sfe 93–94, 95–96
SIP 191–198, 236–??
snr 113
status 116
switch 127–129
system 69
task 77–92
uptime 69
version 69
xclient 233–234
xserv 225–231
SIP endpoint lookup 198
SIP local policy lookups 194
SIP media session statistics 194
SIP message counts 195–197
SNMP traps 52
socket front end 93, 95
sockets 160
software upgrades 285
SPU switch statistics 127
static flows statistics 215
statistics 75
  active period 76
  lifetime high 76
  lifetime permax 76
  lifetime total 76
  per task 76
  recent high 76
  recent total 76
switch port mirroring 132
syslog 27
  code 25
  configuration 27
  removing 28
system name registry 113
system operation 69
  boot parameters 70
  configuration version 69
  OS Version 69
  status 69
  system time 70
  uptime 69

T

  task log 28
    filename 35
    output location 28
  task logging
    configuration 30
    querying 32
    real-time configuration 32
  TCU link verification 133
  terminating sessions 74
  trace log file 34
    configuration 34
    filename 35
    output location 35
  transcoding statistics 225–234

U

  upgrading 285
  user management 74