The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

VPC-VSM System Administration Guide, StarOS Release 19

© 2015 Cisco Systems, Inc. All rights reserved.
# CONTENTS

**About this Guide** ........................................................................................................... xv
  Conventions Used ........................................................................................................... xvi
  Supported Documents and Resources .......................................................................... xvii
  Related Cisco VPC-VSM Documentation ....................................................................... xvii
  ASR 9000 Documentation ............................................................................................... xvii
  Obtaining Cisco Documentation ...................................................................................... xvii
  Contacting Customer Support ......................................................................................... xviii

**Introduction to VPC-VSM** ............................................................................................ 19
  Product Overview ............................................................................................................ 20
  Feature Set ....................................................................................................................... 21
    Interfaces and Addressing ............................................................................................... 21
    Encryption ....................................................................................................................... 21
    Security .......................................................................................................................... 21
  Redundancy and Availability ............................................................................................ 22
  Capacity, CEPS and Throughput ...................................................................................... 23
  Diagnostics and Monitoring .............................................................................................. 24
  Software Installation and Network Deployment ............................................................. 25

**StarOS Operation and Configuration** .......................................................................... 27
  Terminology ..................................................................................................................... 28
    Contexts ......................................................................................................................... 28
    Logical Interface ........................................................................................................... 28
    Management Interface .................................................................................................. 28
    Bindings ......................................................................................................................... 28
    Services .......................................................................................................................... 29
    AAA Servers .................................................................................................................. 29
    Subscribers .................................................................................................................... 29
  How StarOS Selects Contexts .......................................................................................... 31
    Context Selection for Context-level Administrative User Sessions ............................ 31
    Context Selection for Subscriber Sessions .................................................................... 33
  Understanding Configuration Files .................................................................................. 34
  IP Address Notation ........................................................................................................ 36
    IPv4 Dotted-Decimal Notation ....................................................................................... 36
    IPv6 Colon-Separated-Hexadecimal Notation ............................................................... 36
    CIDR Notation ............................................................................................................... 36
  Alphanumeric Strings ..................................................................................................... 38
    Character Set ................................................................................................................ 38
    Quoted Strings .............................................................................................................. 38

**Getting Started** ......................................................................................................... 41
  Using the StarOS Quick Setup Wizard ............................................................................ 42
  Using the StarOS CLI for Initial Configuration ............................................................... 45
    Configuring the Management Interface with a Second IP Address .......................... 47
    Configuring the System for Remote Access .............................................................. 48

**System Settings** .......................................................................................................... 51
Configuring a Second Management Interface .......................................................... 52
Verifying and Saving Your Interface and Port Configuration .................................. 53
Configuring System Timing ....................................................................................... 54
  Setting the StarOS System Clock and Time Zone .................................................. 54
  Verifying and Saving Your Clock and Time Zone Configuration ......................... 54
  Configuring Network Time Protocol Support ....................................................... 54
  Configuring NTP Servers with Local Sources ....................................................... 56
  Using a Load Balancer ......................................................................................... 56
  Verifying the NTP Configuration ........................................................................ 56
Enabling CLI Timestamping ..................................................................................... 57
Configuring System Administrative Users ................................................................ 57
  Configuring Context-level Administrative Users .................................................. 57
    Configuring Context-level Security Administrators .............................................. 58
    Configuring Context-level Administrators ......................................................... 58
    Configuring Context-level Operators ................................................................ 58
    Configuring Context-level Inspectors ................................................................ 59
    Verifying Context-level Administrative User Configuration ............................ 59
  Configuring Local-User Administrative Users ...................................................... 60
  Verifying Local-User Configuration ................................................................... 60
Updating Local User Database .................................................................................. 61
Restricting User Access to a Specified Root Directory ............................................ 61
  Configuring an SFTP root Directory .................................................................... 61
  Associating an SFTP root Directory with a Local User ....................................... 62
  Associating an SFTP root Directory with an Administrator ............................... 62
  Associating an SFTP root Directory with a Config Administrator ...................... 62
Configuring TACACS+ for System Administrative Users ........................................ 62
  Operation ............................................................................................................. 62
    User Account Requirements .............................................................................. 63
      TACACS+ User Account Requirements ............................................................ 63
    User Account Requirements .............................................................................. 64
  Configuring TACACS+ AAA Services ................................................................. 64
  Configuring TACACS+ for Non-local VPN Authentication .................................. 65
  Verifying the TACACS+ Configuration ............................................................... 66
SNMP Configuration ............................................................................................... 69
  SNMP Support ...................................................................................................... 70
  Configuring SNMP and Alarm Server Parameters .............................................. 71
  Verifying SNMP Parameters ................................................................................ 72
  Controlling SNMP Trap Generation .................................................................... 74
Verifying and Saving Your Configuration .................................................................. 75
  Verifying the Configuration .................................................................................. 76
    Feature Configuration ......................................................................................... 76
  Service Configuration ........................................................................................... 77
    Context Configuration ......................................................................................... 77
    System Configuration ........................................................................................ 77
    Finding Configuration Errors ............................................................................ 77
  Saving the Configuration ...................................................................................... 79
    save Command Syntax ...................................................................................... 79
    USB Devices ...................................................................................................... 79
Interfaces and Ports ............................................................................................... 81
  Contexts ............................................................................................................... 82
    Creating Contexts .............................................................................................. 82
    Viewing and Verifying Contexts ......................................................................... 82
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Interfaces and Virtual Ports</td>
<td>83</td>
</tr>
<tr>
<td>Creating an Interface</td>
<td>83</td>
</tr>
<tr>
<td>Configuring a Virtual Port and Binding It to an Interface</td>
<td>84</td>
</tr>
<tr>
<td>Configuring a Static Route for an Interface</td>
<td>84</td>
</tr>
<tr>
<td>Viewing and Verifying Port Configuration</td>
<td>85</td>
</tr>
<tr>
<td>VLANS</td>
<td>87</td>
</tr>
<tr>
<td>StarOS Security</td>
<td>89</td>
</tr>
<tr>
<td>Encrypted SNMP Community Strings</td>
<td>90</td>
</tr>
<tr>
<td>Lawful Intercept Restrictions</td>
<td>91</td>
</tr>
<tr>
<td>LI Server Addresses</td>
<td>91</td>
</tr>
<tr>
<td>Modifying Intercepts</td>
<td>91</td>
</tr>
<tr>
<td>Adding, Modifying and Removing Users</td>
<td>92</td>
</tr>
<tr>
<td>Notification of Users Being Added or Deleted</td>
<td>92</td>
</tr>
<tr>
<td>Notification of Changes in Privilege Levels</td>
<td>92</td>
</tr>
<tr>
<td>User Access to Operating System Shell</td>
<td>92</td>
</tr>
<tr>
<td>Hidden Commands</td>
<td>93</td>
</tr>
<tr>
<td>Enabling cli test-commands Mode</td>
<td>93</td>
</tr>
<tr>
<td>Enabling Password for Access to CLI-test commands</td>
<td>93</td>
</tr>
<tr>
<td>Exec Mode cli test-commands</td>
<td>94</td>
</tr>
<tr>
<td>Configuration mode cli test-commands</td>
<td>94</td>
</tr>
<tr>
<td>List of Exec and Configuration Mode cli test-commands</td>
<td>94</td>
</tr>
<tr>
<td>StarOS Management Operations</td>
<td>95</td>
</tr>
<tr>
<td>Understanding the Local File System</td>
<td>96</td>
</tr>
<tr>
<td>File Types Used by the Local File System</td>
<td>96</td>
</tr>
<tr>
<td>Understanding the boot.sys File</td>
<td>96</td>
</tr>
<tr>
<td>Maintaining the Local File System</td>
<td>97</td>
</tr>
<tr>
<td>File System Management Commands</td>
<td>97</td>
</tr>
<tr>
<td>Creating Directories</td>
<td>97</td>
</tr>
<tr>
<td>Renaming Files and Directories</td>
<td>97</td>
</tr>
<tr>
<td>Copying Files</td>
<td>97</td>
</tr>
<tr>
<td>Deleting Files</td>
<td>98</td>
</tr>
<tr>
<td>Removing Directories</td>
<td>98</td>
</tr>
<tr>
<td>Formatting Local Devices</td>
<td>99</td>
</tr>
<tr>
<td>Applying Pre-existing CLI Configuration Files</td>
<td>99</td>
</tr>
<tr>
<td>Viewing Files on the Local File System</td>
<td>99</td>
</tr>
<tr>
<td>Viewing the Contents of a Local Device</td>
<td>99</td>
</tr>
<tr>
<td>Viewing CLI Configuration and boot.sys Files</td>
<td>100</td>
</tr>
<tr>
<td>Validating an StarOS File</td>
<td>100</td>
</tr>
<tr>
<td>Configuring the Boot Stack</td>
<td>102</td>
</tr>
<tr>
<td>Local-Boot Method</td>
<td>102</td>
</tr>
<tr>
<td>Viewing the Current Boot Stack</td>
<td>102</td>
</tr>
<tr>
<td>Adding a New Boot Stack Entry</td>
<td>103</td>
</tr>
<tr>
<td>Deleting a Boot Stack Entry</td>
<td>103</td>
</tr>
<tr>
<td>Upgrading StarOS</td>
<td>104</td>
</tr>
<tr>
<td>StarOS Release Version</td>
<td>104</td>
</tr>
<tr>
<td>Download the StarOS Image from the Support Site</td>
<td>104</td>
</tr>
<tr>
<td>Transfer the StarOS Image to /flash</td>
<td>104</td>
</tr>
<tr>
<td>Saving a Copy of the Current Configuration File</td>
<td>105</td>
</tr>
<tr>
<td>Off-line Software Upgrade</td>
<td>105</td>
</tr>
<tr>
<td>Configure a Newcall Policy</td>
<td>105</td>
</tr>
<tr>
<td>Configure a Message of the Day Banner</td>
<td>105</td>
</tr>
<tr>
<td>Back up the Current CLI Configuration File</td>
<td>105</td>
</tr>
<tr>
<td>Create a New Boot Stack Entry</td>
<td>106</td>
</tr>
</tbody>
</table>
Save the Running Configuration ................................................................. 106
Reboot StarOS .......................................................................................... 107
Verify the Running Software Version ...................................................... 107
Restoring the Previous Software Image .................................................... 107
Upgrading ICSR ......................................................................................... 107
Performing Dynamic Software Updates .................................................... 108
Managing License Keys ............................................................................ 109
  New System License Keys ....................................................................... 109
  Session Use and Feature Use Licenses ..................................................... 109
  Installing New License Keys .................................................................... 109
  Cutting and Pasting the Key ..................................................................... 109
  Adding License Keys to Configuration Files ............................................ 110
License Expiration Behavior ....................................................................... 111
Requesting License Keys ........................................................................... 111
Viewing License Information ...................................................................... 111
Deleting a License Key ................................................................................ 111
Managing Local-User Administrative Accounts ........................................ 112
  Configuring Local-User Password Properties ......................................... 112
  Configuring Local-User Account Management Properties .................. 112
    Local-User Account Lockouts .............................................................. 112
    Local-User Account Suspensions ......................................................... 113
  Changing Local-User Passwords .............................................................. 113
Monitoring VPC ......................................................................................... 115
  StarOS SNMP Notifications .................................................................... 116
  Monitoring VPC Status and Performance ............................................... 117
  Clearing Statistics and Counters .............................................................. 119
Bulk Statistics .......................................................................................... 121
  Configuring Communication with the Collection Server ....................... 122
    Configuring Standard Settings .............................................................. 122
    Configuring Optional Settings .............................................................. 122
    Configuring Bulk Statistic Schemas ....................................................... 123
    Verifying Your Configuration ............................................................... 123
    Saving Your Configuration ................................................................... 125
  Viewing Collected Bulk Statistics Data .................................................. 126
  Manually Gathering and Transferring Bulk Statistics ............................. 128
  Clearing Bulk Statistics Counters and Information ................................. 129
  Bulk Statistics Event Log Messages ......................................................... 130
System Logs ............................................................................................... 131
  System Log Types .................................................................................. 132
  Configuring Event Logging Parameters ............................................... 133
    Configuring Event Log Filters .............................................................. 133
    Configuring syslog Servers ................................................................. 133
  Configuring Active Logs ........................................................................ 135
  Specifying Facilities ................................................................................ 136
  Configuring Trace Logging ...................................................................... 144
  Configuring Monitor Logs ....................................................................... 145
    Enabling Monitor Logs ........................................................................ 145
    Disabling Monitor Logs ....................................................................... 145
  Viewing Logging Configuration and Statistics ....................................... 146
  Viewing Event Logs Using the CLI ......................................................... 147
  Configuring and Viewing Crash Logs ..................................................... 148
    Crash Logging Architecture .................................................................. 148
<table>
<thead>
<tr>
<th>Troubleshooting</th>
<th>163</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring StarOS VPC-VSM</td>
<td>164</td>
</tr>
<tr>
<td>Verifying StarOS Network Connectivity</td>
<td>165</td>
</tr>
<tr>
<td>Using the ping or ping6 Command</td>
<td>165</td>
</tr>
<tr>
<td>Syntax</td>
<td>165</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>166</td>
</tr>
<tr>
<td>Using the traceroute or traceroute6 Command</td>
<td>166</td>
</tr>
<tr>
<td>traceroute – IPv4</td>
<td>166</td>
</tr>
<tr>
<td>traceroute6 – IPv6</td>
<td>167</td>
</tr>
<tr>
<td>Viewing IP Routes</td>
<td>167</td>
</tr>
<tr>
<td>Viewing the Address Resolution Protocol Table</td>
<td>168</td>
</tr>
<tr>
<td>Using StarOS Diagnostic Utilities</td>
<td>169</td>
</tr>
<tr>
<td>Using the Monitor Utility</td>
<td>169</td>
</tr>
<tr>
<td>Using the Protocol Monitor</td>
<td>169</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Control Lists</th>
<th>171</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>172</td>
</tr>
<tr>
<td>Understanding ACLs</td>
<td>172</td>
</tr>
<tr>
<td>Rule(s)</td>
<td>173</td>
</tr>
<tr>
<td>Actions</td>
<td>173</td>
</tr>
<tr>
<td>Criteria</td>
<td>173</td>
</tr>
<tr>
<td>Rule Order</td>
<td>174</td>
</tr>
<tr>
<td>Configuring ACLs on the System</td>
<td>175</td>
</tr>
<tr>
<td>Creating ACLs</td>
<td>175</td>
</tr>
<tr>
<td>Configuring Action and Criteria for Subscriber Traffic</td>
<td>175</td>
</tr>
<tr>
<td>Configuring an Undefined ACL</td>
<td>176</td>
</tr>
<tr>
<td>Verifying the ACL Configuration</td>
<td>176</td>
</tr>
<tr>
<td>Applying IP ACLs</td>
<td>178</td>
</tr>
<tr>
<td>Applying an ACL to an Individual Interface</td>
<td>179</td>
</tr>
<tr>
<td>Applying the ACL to an Interface</td>
<td>179</td>
</tr>
<tr>
<td>Verifying the ACL Configuration on an Interface</td>
<td>180</td>
</tr>
<tr>
<td>Applying an ACL to All Traffic Within a Context</td>
<td>181</td>
</tr>
<tr>
<td>Applying the ACL to a Context</td>
<td>181</td>
</tr>
<tr>
<td>Verifying the ACL Configuration in a Context</td>
<td>182</td>
</tr>
<tr>
<td>Applying an ACL to a RADIUS-based Subscriber</td>
<td>183</td>
</tr>
<tr>
<td>Applying an ACL to an Individual Subscriber</td>
<td>183</td>
</tr>
<tr>
<td>Verifying the ACL Configuration to an Individual Subscriber</td>
<td>184</td>
</tr>
<tr>
<td>Applying a Single ACL to Multiple Subscribers</td>
<td>185</td>
</tr>
<tr>
<td>Applying an ACL to the Subscriber Named default</td>
<td>185</td>
</tr>
<tr>
<td>Applying an ACL to Service-specified Default Subscriber</td>
<td>187</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Congestion Control</th>
<th>193</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>194</td>
</tr>
<tr>
<td>Configuring Congestion Control</td>
<td>195</td>
</tr>
<tr>
<td>Configuring the Congestion Control Threshold</td>
<td>195</td>
</tr>
<tr>
<td>Configuring Service Congestion Policies</td>
<td>195</td>
</tr>
<tr>
<td>Configuring Overload Reporting on the MME</td>
<td>196</td>
</tr>
<tr>
<td>Enabling Congestion Control Redirect Overload Policy</td>
<td>196</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Verify the Service Overload Policies</td>
<td>197</td>
</tr>
<tr>
<td>Verify the Congestion Control Configuration</td>
<td>197</td>
</tr>
<tr>
<td>Verify MME Congestion Action Profiles</td>
<td>200</td>
</tr>
<tr>
<td>Disconnecting Subscribers Based on Call or Inactivity Time</td>
<td>201</td>
</tr>
<tr>
<td>Routing</td>
<td>203</td>
</tr>
<tr>
<td>Routing Policies</td>
<td>204</td>
</tr>
<tr>
<td>Creating IP Prefix Lists</td>
<td>204</td>
</tr>
<tr>
<td>Creating Route Access Lists</td>
<td>204</td>
</tr>
<tr>
<td>Creating AS Path Access Lists</td>
<td>205</td>
</tr>
<tr>
<td>Creating Route Maps</td>
<td>205</td>
</tr>
<tr>
<td>Sample Configuration</td>
<td>205</td>
</tr>
<tr>
<td>Static Routing</td>
<td>207</td>
</tr>
<tr>
<td>Adding Static Routes to a Context</td>
<td>207</td>
</tr>
<tr>
<td>Deleting Static Routes From a Context</td>
<td>208</td>
</tr>
<tr>
<td>OSPF Routing</td>
<td>209</td>
</tr>
<tr>
<td>OSPF Version 2 Overview</td>
<td>209</td>
</tr>
<tr>
<td>Basic OSPFv2 Configuration</td>
<td>210</td>
</tr>
<tr>
<td>Enabling OSPF Routing For a Specific Context</td>
<td>210</td>
</tr>
<tr>
<td>Enabling OSPF Over a Specific Interface</td>
<td>210</td>
</tr>
<tr>
<td>Redistributing Routes Into OSPF (Optional)</td>
<td>210</td>
</tr>
<tr>
<td>Confirming OSPF Configuration Parameters</td>
<td>211</td>
</tr>
<tr>
<td>OSPFv3 Routing</td>
<td>212</td>
</tr>
<tr>
<td>OSPFv3 Overview</td>
<td>212</td>
</tr>
<tr>
<td>Basic OSPFv3 Configuration</td>
<td>212</td>
</tr>
<tr>
<td>Enabling OSPFv3 Routing For a Specific Context</td>
<td>212</td>
</tr>
<tr>
<td>Enabling OSPFv3 Over a Specific Interface</td>
<td>212</td>
</tr>
<tr>
<td>Redistributing Routes Into OSPFv3 (Optional)</td>
<td>213</td>
</tr>
<tr>
<td>Confirming OSPFv3 Configuration Parameters</td>
<td>213</td>
</tr>
<tr>
<td>Equal Cost Multiple Path (ECMP)</td>
<td>214</td>
</tr>
<tr>
<td>BGP-4 Routing</td>
<td>215</td>
</tr>
<tr>
<td>Overview of BGP Support</td>
<td>215</td>
</tr>
<tr>
<td>Configuring BGP</td>
<td>216</td>
</tr>
<tr>
<td>Redistributing Routes Into BGP (Optional)</td>
<td>216</td>
</tr>
<tr>
<td>BGP Communities and Extended Communities</td>
<td>216</td>
</tr>
<tr>
<td>BGP Communities</td>
<td>217</td>
</tr>
<tr>
<td>BGP Extended Communities</td>
<td>218</td>
</tr>
<tr>
<td>BGP Local Preference</td>
<td>219</td>
</tr>
<tr>
<td>ICSR and SRP Groups</td>
<td>219</td>
</tr>
<tr>
<td>Advertising BGP Routes from a Standby ICSR Chassis</td>
<td>219</td>
</tr>
<tr>
<td>Configurable BGP Route Advertisement Interval for ICSR</td>
<td>220</td>
</tr>
<tr>
<td>Bidirectional Forwarding Detection</td>
<td>221</td>
</tr>
<tr>
<td>Overview of BFD Support</td>
<td>221</td>
</tr>
<tr>
<td>Configuring BFD</td>
<td>221</td>
</tr>
<tr>
<td>Configuring a BFD Context</td>
<td>222</td>
</tr>
<tr>
<td>Configuring IPv4 BFD for Static Routes</td>
<td>222</td>
</tr>
<tr>
<td>Configuring IPv6 BFD for Static Routes</td>
<td>222</td>
</tr>
<tr>
<td>Configuring BFD for Single Hop</td>
<td>222</td>
</tr>
<tr>
<td>Configuring Multihop BFD</td>
<td>223</td>
</tr>
<tr>
<td>Scaling of BFD</td>
<td>223</td>
</tr>
<tr>
<td>Associating BGP Neighbors with the Context</td>
<td>224</td>
</tr>
<tr>
<td>Associating OSPF Neighbors with the Context</td>
<td>224</td>
</tr>
<tr>
<td>Associating BFD Neighbor Groups with the BFD Protocol</td>
<td>225</td>
</tr>
<tr>
<td>Enabling BFD on OSPF Interfaces</td>
<td>225</td>
</tr>
<tr>
<td>Monitoring BFD Connection for ICSR</td>
<td>225</td>
</tr>
</tbody>
</table>
Contents

Verifying SRP Configuration ................................................................. 261
Configure ICSR and OneP/CA Interfaces ........................................ 261
Configuring an ICSR Traffic Interface ............................................. 261
Configuring a OneP/CA Interface .................................................... 261
Set Subscriber to Default Mode ..................................................... 262
Disable Bulk Statistics Collection on a Standby Instance ................. 262
Verify the Primary and Backup Configurations ................................. 263
Configure the Subscriber State Management Audit Process ............... 263
Save the Configuration ..................................................................... 263
Additional Configuration Requirements ........................................... 263
StarOS Updates in an ICSR Configuration ........................................ 264
Both ICSR Instances ......................................................................... 268
Standby Backup Instance ................................................................. 268
Performing Health Checks ............................................................... 269
Performing SRP Checks .................................................................. 269
Updating the Boot Record ................................................................ 269
Reloading StarOS ............................................................................. 270
Updating the Configuration File ....................................................... 270
Verifying the Software Version ....................................................... 270
Saving the Configuration File .......................................................... 270
Completing the Update Process ...................................................... 270
Waiting for Session Synchronization ................................................ 271
Primary Instance .............................................................................. 271
Initiating an SRP Switchover .......................................................... 271
Checking AAA Monitor Status on the Newly Active Instance .......... 271
Completing the Software Update ...................................................... 271
Initiating an SRP Switchover .......................................................... 272
Checking AAA Monitor Status ......................................................... 272
Making Test Calls ............................................................................ 272
Fallback Procedure ........................................................................ 272

Support Data Collector ..................................................................... 275
Overview .......................................................................................... 276
Configuring SDR Collection ............................................................ 277
Displaying the SDR Collection Configuration ................................ 278
Collecting and Storing the SDR Information .................................... 279
Managing Record Collection ........................................................... 280
Using SDRs to Diagnose Problems .................................................. 282
SDR CLI Commands ......................................................................... 283
Configuration Commands (Global Configuration Mode) ................. 283
  support record .............................................................................. 283
  support collection ................................................................------- 283
Exec Mode Commands ..................................................................... 284
  show support record .................................................................... 284
  delete support record .................................................................. 285
  show support collection ............................................................... 285

Installation Guidelines ...................................................................... 287
OVA Packaging ................................................................................ 288
Installation Procedure ..................................................................... 289
How to Install StarOS VMs — Asynchronous distribution ............... 289
RSP virtual-service Sample Configuration ...................................... 290
How to Install StarOS VMs — Synchronous distribution .................. 292
Miscellaneous Procedures ............................................................... 293
How to Uninstall StarOS VMs ................................................................. 293
How to Upgrade form the StarOS CLI .................................................. 293
How to Upgrade StarOS VMs from RSP ................................................. 293

Engineering Rules .............................................................................. 295
StarOS CLI Session Rules ................................................................. 296
VPC Interface and Port Rules ............................................................. 297
vNIC Ethernet Ports ......................................................................... 297
Packet Data Network (PDN) Interface Rules ....................................... 297
Context Rules .................................................................................... 298
Subscriber Rules ............................................................................... 300
Service Rules .................................................................................... 301
Access Control List (ACL) Engineering Rules ..................................... 302

StarOS Tasks ...................................................................................... 303
Overview .......................................................................................... 304
Primary Task Subsystems .................................................................. 305
Controllers and Managers .................................................................. 307
Subsystem Tasks ............................................................................... 308
  System Initiation Subsystem .......................................................... 308
  High Availability Subsystem ......................................................... 308
  Resource Manager Subsystem ...................................................... 309
  Virtual Private Networking Subsystem ......................................... 310
  Network Processing Unit Subsystem .............................................. 311
  Session Subsystem ....................................................................... 312
  Platform Processes ....................................................................... 319
  Management Processes .................................................................. 322

ICSR Checkpointing ......................................................................... 323
Overview of Checkpointing .............................................................. 324
Macro-checkpoints .......................................................................... 325
  GGSDN_APN ID MAPPING ............................................................ 325
  INSTANCE_LEVEL_CHECKPOINT .............................................. 325
  SERVICE_ID MAPPING .............................................................. 325
  VPCMGR_ID MAPPING ............................................................... 326
Micro-checkpoints ............................................................................ 327
  Uncategorized ............................................................................... 327
  SESS_UCHKPT_CMD_INVALIDATE_CRR .................................. 327
  SESS_UCHKPT_CMD_UPDATE_CLPSTAS .................................. 327
  SESS_UCHKPT_CMD_UPDATE_IDLESECS .................................. 328
DCCA Category .................................................................................. 328
  SESS_UCHKPT_CMD_DCCA_SESS_INFO .................................. 328
ECS Category ..................................................................................... 329
  SESS_UCHKPT_CMD_ACS_CALL_INFO .................................... 329
  SESS_UCHKPT_CMD_ACS_GX_LI_INFO .................................... 329
  SESS_UCHKPT_CMD_ACS_SESS_INFO ...................................... 329
  SESS_UCHKPT_CMD_DEL_ACS_CALL_INFO .................................. 330
  SESS_UCHKPT_CMD_DEL_ACS_SESS_INFO .................................. 330
  SESS_UCHKPT_CMD_DYNAMIC_CHRG_CA_INFO ......................... 330
  SESS_UCHKPT_CMD_DYNAMIC_CHRG_DEL_CA_INFO .................... 331
  SESS_UCHKPT_CMD_DYNAMIC_CHRG_DEL_QG_INFO .................... 331
  SESS_UCHKPT_CMD_DYNAMIC_CHRG_QG_INFO ............................ 331
  SESS_UCHKPT_CMD_DYNAMIC_RULE_DEL_INFO ......................... 332
  SESS_UCHKPT_CMD_DYNAMIC_RULE_INFO .................................. 332
ePDGDG Category .............................................................................. 332
About this Guide

This preface describes the *VPC-VSM System Administration Guide*, how it is organized and its document conventions. Cisco Virtualized Packet Core-VSM (VPC-VSM) consists of a single StarOS instance running in a virtual machine (VM) on a Cisco ASR 9000 Virtualized Services Module (VSM). This guide describes how to configure and administer the StarOS instance running within the VM.
Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Information Note" /></td>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td><img src="icon" alt="Caution" /></td>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td><img src="icon" alt="Warning" /></td>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

**Typeface Conventions**

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Text represented as a screen display</strong></td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td><strong>Text represented as commands</strong></td>
<td>This typeface represents commands that you enter, for example: <code>show ip access-list</code> This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.</td>
</tr>
<tr>
<td><strong>Text represented as a command variable</strong></td>
<td>This typeface represents a variable that is part of a command, for example: <code>show card slot_number</code> <code>slot_number</code> is a variable representing the desired chassis slot number.</td>
</tr>
<tr>
<td><strong>Text represented as menu or sub-menu names</strong></td>
<td>This typeface represents menus and sub-menus that you access within a software application, for example: Click the <strong>File</strong> menu, then click <strong>New</strong></td>
</tr>
</tbody>
</table>
Supported Documents and Resources

Related Cisco VPC-VSM Documentation

The most up-to-date information for VPC-VSM is available in the product Release Notes provided with each product release.

The following common documents are available for StarOS products:

- Security Gateway Administration Guide
- Command Line Interface Reference
- IPSec Reference
- AAA Interface Administration and Reference
- GTPP Interface Administration and Reference
- Release Change Reference
- SNMP MIB Reference
- Statistics and Counters Reference
- Thresholding Configuration Guide

ASR 9000 Documentation

The following user documents describe how to install and configure the ASR 9000 Virtualized Service Module (VSM).


- Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router

- Cisco ASR 9000 Series Aggregation Services Router Carrier Grade IPv6 (CGv6) Configuration Guide – Carrier Grade IPv6 over Virtualized Services Module (VSM)

Obtaining Cisco Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

Use the following URL to access the StarOS (ASR 5000 Series) documentation:


Use the following URLs to access the ASR 9000 documentation:

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
Introduction to VPC-VSM

This chapter introduces Cisco Virtualized Packet Core-Virtualized Services Module (VPC-VSM).

This chapter encompasses the following topics:

- Product Overview
- Feature Set
- Redundancy and Availability
- Capacity CEPS and Throughput
- Diagnostics and Monitoring
- Software Installation and Network Deployment
Product Overview

VPC-VSM consists of the set of virtualized mobility functions that implement mobility specific services and applications within the core of the network. The StarOS image that supports these functions runs within a virtual machine (VM) initiated by a hypervisor.

VPC-VSM runs on an ASR 9000 Virtualized Services Module (VSM). The VSM is a service blade that supports multiple services and applications running simultaneously on top of a virtualized hardware environment. The VSM blade runs Cisco NGOS Linux and a KVM hypervisor. This combination brings virtualization the ASR 9000 IOS-XR platform. OneP communication (also known as ConnectedApps [CA]) allows IOS-XR to offer control plane, data plane and management plane access to VPC-VSM via the ASR 9000 route processor (RP).

A VPC-VSM instance (StarOS VM) runs on each of the four CPUs on a VSM (four VMs per VSM). You enable Security Gateway (SecGW) functionality within each StarOS VM as a Wireless Security Gateway (WSG) service. For additional information, refer to the SecGW Administration Guide.

For additional information on VSM installation and configuration, refer to the following ASR 9000 user documents:

- Cisco ASR 9000 Series Aggregated Services Router VSM (Virtualized Services Module) Line Card Installation Guide (OL-30446-01) [available March, 2014]
- Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router
- Cisco ASR 9000 Series Aggregation Services Router Carrier Grade IPv6 (CGv6) Configuration Guide – Carrier Grade IPv6 over Virtualized Services Module (VSM)

For additional information on how to configure a Security Gateway (SecGW) for high availability (HA), refer to the Reverse Route Injection (RRI) chapter of the SecGW Administration Guide.
Feature Set

Interfaces and Addressing

The VM is represented as a virtual card with a single CPU subsystem. This makes many CLI commands, logs, and functions work similarly to StarOS running on ASR 5x00 platforms.

Applications written for StarOS see VPC-VSM as just another platform with a one-slot virtual chassis supporting a single virtual card.

StarOS concepts of contexts, services, pools, interfaces, cards, and ports exist on VPC-VSM just as on existing platforms. When the VM boots, the vNICs configured in the VM profile are detected and an equivalent number of ‘Virtual Ethernet’ type ports appear in the StarOS CLI.

- VPC-VSM assigns the vNIC interfaces in the order offered by the hypervisor.
  - First interface offered by the hypervisor: 1/10 for service traffic.
  - Second interface offered by the hypervisor: 1/11 for service traffic.
  - Third interface offered by the hypervisor: 1/1 for management.

- It is critical to confirm that the interfaces listed in the supported hypervisors line up with the KVM BR group in the order in which you want them to match the VPC-VSM interfaces.

- You cannot be guaranteed that the order of the vNICs as listed in the hypervisor CLI/GUI is the same as how the hypervisor offers them to VPC-VSM. On initial setup you must use the `show hardware` CLI command to walk through the MAC addresses shown on the hypervisor's vNIC configuration and match them up with the MAC addresses learned by VPC-VSM. This will confirm that the VPC-VSM interfaces are connected to the intended BR group/Vswitch.

Encryption

VPC-VSM performs encryption and tunneling of packets using the VSM crypto hardware. This hardware facilitates call models that make heavy use of encryption for bearer packets or have significant PKI (Public Key Infrastructure) key generation rates.

For additional information, see the `IPSec Reference`.

Security

Security of external traffic including tunneling, encryption, Access Control Lists (ACLs), context separation, and user authentication function as on existing StarOS platforms. User ports and interfaces are protected through StarOS CLI configuration.
Redundancy and Availability

SecGW supports High Availability (HA) capabilities for VSM service cards within an ASR 9000. HA functions are triggered for the following events:

- Route Processor (RP) failure
- Virtual Machine (VM) failure
- VSM failure
- Link failure

**Important:** The VPC-VSM HA architecture utilizes StarOS Interchassis Session Recovery (ICSR). For a complete description of the HA architecture, see the *Reverse Route Injection (RRI)* chapter of the *SecGW Administration Guide*. 
Capacity, CEPS and Throughput

Sizing a VPC-VSM instance requires modeling of the expected call model.

Many service types require more resources than others. Packet size, throughput per session, CEPS (Call Events per Second) rate, IPSec usage (site-to-site, subscriber, LI), contention with other VMs, and the underlying hardware type (CPU speed, number of vCPUs) will further limit the effective number of maximum subscribers. Qualification of a call model on equivalent hardware and hypervisor configuration is required.
Diagnostics and Monitoring

Because VPC-VSM runs within a VM, no hardware diagnostics or monitoring are provided. Retrieval of hardware sensor data (temperature, voltage, memory errors) are accomplished via the IOS-XR monitoring systems.

VPC-VSM monitors and exports vCPU, vRAM, and vNIC usage through existing mechanisms including CLI `show` commands, bulkstats and MIB traps. However, an operator may find that monitoring physical CPU, RAM, and NIC values in the hypervisor is more useful.

Because vNICs have a variable maximum throughput, counters and bulkstats that export utilization as a percentage of throughput may have little value. Absolute values (bps) should be obtained from VPC-VSM where possible; physical infrastructure utilization should be obtained from the hypervisor or IOS-XR via the ASR 9000 route processor (RP).
Software Installation and Network Deployment

This guide assumes that VPC-VSM has been properly installed to run in a virtual machine (VM) on an ASR 9000 VSM. Refer to the *Installation Guidelines* appendix for information on how to install a StarOS VM on each of the four CPUs on the VSM.

For additional information, refer to the *Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router*. 
Chapter 2
StarOS Operation and Configuration

StarOS provides subscriber management services for Mobile Packet Core networks.
Before you connect to the StarOS command line interface (CLI) and begin the configuration process, you must understand how StarOS supports these services. This chapter provides terminology and background information to consider before you configure StarOS. The following sections are included:

- Terminology
- How StarOS Selects Contexts
- Understanding Configuration Files
- IP Address Notation
- Alphanumeric Strings
Terminology

This section defines important StarOS terms used throughout this guide.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

StarOS supports the configuration of multiple contexts. Each context is configured and operates independently of the others. Once a context has been created, administrative users can configure services, logical IP interfaces, and subscribers for that context and then bind the logical interfaces to physical ports.

You can also assign a domain alias to a context; if a subscriber’s domain name matches one of the configured alias names for a context, that context is used.

Logical Interface

You must associate a port with a virtual circuit or tunnel called a logical interface before the port can allow the flow of user data. A logical interface within StarOS is the assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

There are several types of logical interfaces to configure to support Simple and Mobile IP data applications.

Management Interface

This interface provides the point of attachment to the management network. The interface supports remote access to the StarOS command line interface (CLI). It also supports event notification via the Simple Network Management Protocol (SNMP).

Bindings

A binding is an association between elements within StarOS. There are two types of bindings: static and dynamic.

Static binding is accomplished through system configuration. Static bindings associate:

- A specific logical interface (configured within a particular context) to a physical or virtual port. Once the interface is bound, traffic can flow through the context as if it were any physically-defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (that is, support the protocols) required by the service.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility, as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Management ports can only be bound in the local context. Traffic or subscriber ports can only be bound in a non-local context.
Services

You configure services within a context to enable certain functionality. The Security Gateway is configured as a WSG (Wireless Security Gateway) service in a dedicated context to enable SecGW service with a StarOS VM.

AAA Servers

Authentication, Authorization and Accounting (AAA) servers store profiles, perform authentication, and maintain accounting records for each mobile data subscriber. The AAA servers communicate with StarOS over an AAA interface. StarOS supports the configuration of up to 128 interfaces to AAA servers.

It is important to note that for Mobile IP, there can be Foreign AAA (FAAA) and Home AAA (HAAA) servers. FAAA servers typically reside in the carrier’s network. HAAA servers could be owned and controlled by either the carrier or the home network. If the HAAA server is owned and controlled by the home network, accounting data is transferred to the carrier via an AAA proxy server.

**Important:** Mobile IP support depends on the availability and purchase of a standalone license or a license bundle that includes Home Agent (HA).

Subscribers

Subscribers are the end-users of the service; they gain access to the Internet, their home network, or a public network through StarOS.

There are three primary types of subscribers:

- **RADIUS-based Subscribers:** The most common type of subscriber, these users are identified by their International Mobile Subscriber Identity (IMSI) number, an Electronic Serial Number (ESN), or by their domain name or user name. They are configured on and authenticated by a RADIUS AAA server.

  Upon successful authentication, various attributes that are contained in the subscriber profile are returned. The attributes dictate such things as session parameter settings (for example, protocol settings and IP address assignment method), and what privileges the subscriber has.

**Important:** Attribute settings received by StarOS from a RADIUS AAA server take precedence over local-subscriber attributes and parameters configured on StarOS.

- **Local Subscribers:** These are subscribers, primarily used for testing purposes, that are configured and authenticated within a specific context. Unlike RADIUS-based subscribers, the local subscriber’s user profile (containing attributes like those used by RADIUS-based subscribers) is configured within the context where they are created.

  When local subscriber profiles are first created, attributes for that subscriber are set to StarOS’s default settings. The same default settings are applied to all subscriber profiles, including the subscriber named *default* which is created automatically by StarOS for each system context. When configuring local profile attributes, the changes are made on a subscriber-by-subscriber basis.

**Important:** Attributes configured for local subscribers take precedence over context-level parameters. However, they could be over-ridden by attributes returned from a RADIUS AAA server.
**Management Subscribers**: A management user is an authorized user who can monitor, control, and configure StarOS through the CLI. Management is performed either locally, through the hypervisor vConsole port, or remotely through the use of the Telnet or secure shell (SSH) protocols. Management users are typically configured as a local subscriber within the Local context, which is used exclusively for StarOS management and administration. As with a local subscriber, a management subscriber’s user profile is configured within the context where the subscriber was created (in this case, the Local context). However, management subscribers may also be authenticated remotely via RADIUS, if an AAA configuration exists within the local context, or TACACS+.
How StarOS Selects Contexts

This section describes the process that determines which context to use for context-level administrative users or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces you need to configure.

Context Selection for Context-level Administrative User Sessions

StarOS comes configured with a context called local that you use specifically for management purposes. The source and destination contexts for a context-level administrative user responsible for managing the entire system should always be the local context.

A context-level administrative user can also connect through other interfaces on StarOS and still have full management privileges.

A context-level administrative user can be created in a non-local context. These management accounts have privileges only in the context in which they are created. This type of management account can connect directly to a port in the context in which they belong, if local connectivity is enabled (SSHD, for example) in that context.

For all FTP or SFTP connections, you must connect through a management interface. If you SFTP or FTP as a non-local context account, you must use the username syntax of username@contextname.

The context selection process becomes more involved if you are configuring StarOS to provide local authentication or work with a AAA server to authenticate the context-level administrative user.

StarOS gives you the flexibility to configure context-level administrative users locally (meaning that their profile will be configured and stored in its own memory), or remotely on an AAA server. If a locally-configured user attempts to log onto StarOS, StarOS performs the authentication. If you have configured the user profile on an AAA server, StarOS must determine how to contact the AAA server to perform authentication. It does this by determining the AAA context for the session.

The following table and flowchart describe the process that StarOS uses to select an AAA context for a context-level administrative user. Items in the table correspond to the circled numbers in the flowchart.
Figure 1. Context-level Administrative User AAA Context

Table 1. Context-level Administrative User AAA Context Selection

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>

Use AAA policies defined within the local context.
## How StarOS Selects Contexts

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>During authentication, StarOS determines whether local authentication is enabled in the <em>local</em> context. If it is, StarOS attempts to authenticate the administrative user in the <em>local</em> context. If it is not, proceed to item 2 in this table. If the administrative user’s username is configured, authentication is performed by using the AAA configuration within the <em>local</em> context. If not, proceed to item 2 in this table.</td>
</tr>
<tr>
<td>2</td>
<td>If local authentication is disabled in StarOS or if the administrative user’s username is not configured in the <em>local</em> context, StarOS determines if a domain was received as part of the username. If there is a domain and it matches the name of a configured context or domain, StarOS uses the AAA configuration within that context. If there is a domain and it does not match the name of a configured context or domain, Go to item 4 in this table. If there is no domain as part of the username, go to item 3 in this table.</td>
</tr>
<tr>
<td>3</td>
<td>If there was no domain specified in the username or the domain is not recognized, StarOS determines whether an <em>AAA Administrator Default Domain</em> is configured. If the default domain is configured and it matches a configured context, the AAA configuration within the <em>AAA Administrator Default Domain</em> context is used. If the default domain is not configured or does not match a configured context or domain, go to item 4 item below.</td>
</tr>
<tr>
<td>4</td>
<td>If a domain was specified as part of the username but it did not match a configured context, or if a domain was not specified as part of the username, StarOS determines if the <em>AAA Administrator Last Resort context parameter</em> is configured. If a last resort, context is configured and it matches a configured context, the AAA configuration within that context is used. If a last resort context is not configured or does not match a configured context or domain, the AAA configuration within the <em>local</em> context is used.</td>
</tr>
</tbody>
</table>

## Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users. Subscriber session context selection information for specific products is located in the *SecGW Administration Guide*. 
Understanding Configuration Files

StarOS supports the use of a file or script to modify configurable parameters. Using a file for offline system configuration reduces the time it takes to configure parameters on multiple systems.

A StarOS configuration file is an ASCII text file that contains commands and configuration parameters. When you apply the configuration file, StarOS parses through the file line-by-line, testing the syntax and executing the command. If the syntax is incorrect, a message is displayed to the CLI and StarOS proceeds to the next command. Lines that begin with # are considered remarks and are ignored.

**Important:** Pipes (|), used with the `grep` and `more` keywords, can potentially cause errors in configuration file processing. Therefore, StarOS automatically ignores keywords with pipes during processing.

**Important:** Always save configuration files in UNIX format. Failure to do so can result in errors that prevent configuration file processing.

The commands and configuration data within the file are organized and formatted just as they would be if they were being entered at the CLI prompt. For example, if you wanted to create a context called `source` in the CLI, you would enter the following commands at their respective prompts:

```
[local] host_name# config
[local] host_name(config)# context source
[wsg] host_name(config-ctx)# end
```

To create a context called `source` using a configuration file, you would use a text editor to create a new file that consists of the following:

```
config

    context source

end
```

There are several important things to consider when using configuration files:

- StarOS automatically applies a configuration file at the end of the boot process. After StarOS boots up for the first time, a configuration file that you have created and that is tailored to your network needs, can be applied. To make StarOS use your configuration file, modify StarOS boot parameters according to the instructions located in the *StarOS Management Operations* chapter.

- In addition to being applied during the boot process, you can also apply configuration files manually at any time by executing the appropriate commands at the CLI prompt. Refer to the instructions in the *StarOS Management Operations* chapter.
**Important:** When you apply a configuration file after the boot process, the file does not delete the configuration loaded as part of the boot process. Only those commands that are duplicated are overwritten.

- Configuration files can be stored in any of the following locations:
  - **Network Server:** Any workstation or server on the network that StarOS can access using the Secure File Transfer Protocol (SFTP). This is recommended for large network deployments in which multiple systems require the same configuration.
  - **/flash:** A solid-state device with limited storage.
  - **/hd-raid:** Internal RAID storage.
- Each time you save configuration changes you made during a CLI session, you can save those settings to a configuration file.
IP Address Notation

When configuring a port interface via the CLI you may be required to enter an IP address. The CLI always accepts an IPv4 address, and in some cases accepts an IPv6 address as an alternative.

For some configuration commands, the CLI also accepts CIDR notation when entering an IP address. Always view the online Help for the CLI command to verify acceptable forms of IP address notation.

IPv4 Dotted-Decimal Notation

An Internet Protocol Version 4 (IPv4) address consists of 32 bits divided into four octets. These four octets are written in decimal numbers, ranging from 0 to 255, and are concatenated as a character string with full stop delimiters (dots) between each number.

For example, the address of the loopback interface, usually assigned the host name localhost, is 127.0.0.1. It consists of the four binary octets 01111111, 00000000, 00000000, and 00000001, forming the full 32-bit address.

IPv4 allows 32 bits for an Internet Protocol address and can, therefore, support $2^{32}$ (4,294,967,296) addresses.

IPv6 Colon-Separated-Hexadecimal Notation

An Internet Protocol Version 6 (IPv6) address has two logical parts: a 64-bit network prefix, and a 64-bit host address part. An IPv6 address is represented by eight groups of 16-bit hexadecimal values separated by colons (:).

A typical example of a full IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334

The hexadecimal digits are case-insensitive.

The 128-bit IPv6 address can be abbreviated with the following rules:

- Leading zeroes within a 16-bit value may be omitted. For example, the address fe80:0000:0000:0000:0202:b3ff:fe1e:8329 may be written as fe80:0:0:202:b3ff:fe1e:8329
- One group of consecutive zeroes within an address may be replaced by a double colon. For example, fe80:0:0:202:b3ff:fe1e:8329 becomes fe80::202:b3ff:fe1e:8329

IPv6 allows 128 bits for an Internet Protocol address and can support $2^{128}$ (340,282,366,920,938,000,000,000,000,000,000,000,000,000,000,000) internet addresses.

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation is a compact specification of an Internet Protocol address and its associated routing prefix. It is used for both IPv4 and IPv6 addressing in networking architectures.

CIDR is a bitwise, prefix-based standard for the interpretation of IP addresses. It facilitates routing by allowing blocks of addresses to be grouped into single routing table entries. These groups (CIDR blocks) share an initial sequence of bits in the binary representation of their IP addresses.

CIDR notation is constructed from the IP address and the prefix size, the latter being the number of leading 1 bits of the routing prefix. The IP address is expressed according to the standards of IPv4 or IPv6. It is followed by a separator character, the slash (/) character, and the prefix size expressed as a decimal number.
**Important:** On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

The address may denote a single, distinct, interface address or the beginning address of an entire network. In the latter case the CIDR notation specifies the address block allocation of the network. The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix. This is often called the host identifier.

For example:

- the address specification 192.168.100.1/24 represents the given IPv4 address and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0.
- the IPv4 block 192.168.0.0/22 represents the 1024 IPv4 addresses from 192.168.0.0 to 192.168.3.255.
- the IPv6 block 2001:DB8::/48 represents the IPv6 addresses from 2001:DB8:0:0:0:0:0:0 to 2001:DB8:0:FFFF:FFFF:FFFF:FFFF.
- ::1/128 represents the IPv6 loopback address. Its prefix size is 128, the size of the address itself, indicating that this facility consists of only this one address.

The number of addresses of a subnet defined by the mask or prefix can be calculated as 2, in which the address size for IPv4 is 32 and for IPv6 is 128. For example, in IPv4, a mask of /29 gives 8 addresses.
Alphanumeric Strings

Some CLI commands require the entry of a string of characters that can contain a contiguous collection of alphabetic, numeric, or alphanumeric characters with a defined minimum and maximum length (number of characters).

Character Set

The alphanumeric character set is a combination of alphabetic characters (Latin letters) and numeric characters (Arabic numerals). The set consists of the letters A to Z (uppercase) and a to z (lowercase) and the numbers 0 to 9. The underscore character (_) and dash/hyphen character (-) can also be used.

Blank spaces (whitespaces or SPACE characters) should mostly be avoided in alphabetic, numeric, and alphanumeric strings, except in certain ruledef formats, such as time/date stamps.

The following special characters can be used in ruledefs, APNs, license keys and other configuration/display parameters:

- < > (arrow brackets) [less than or greater than]
- * (asterisk) [wildcard]
- : (colon)
- $ (dollar sign) [wildcard]
- . (dot)
- = (equals sign)
- ! (exclamation point)
- % (percent)
- / (slash - forward)
- | (vertical bar)

The following special characters can be used to delimit the domain from the user name for global AAA functions:

- @ (at sign)
- - (dash or hyphen)
- # (hash or pound sign)
- % (percent)
- \ (slash - backward) [must be entered as double slash \\]
- / (slash - forward)

Quoted Strings

If descriptive text requires the use of spaces between words, the string must be entered within double quotation marks (" ").

```
interface "Rack 3 Chassis 1 port 5/2"
```
Chapter 3
Getting Started

Following successful installation of a VPC-VSM instance (StarOS VM), you must configure a set of StarOS parameters. You then save these settings in a configuration file that is launched whenever the system is reloaded.

This chapter provides instructions for connecting to the console port of a StarOS VM and creating the initial local context management configuration. It includes the following sections:

- Using the StarOS Quick Setup Wizard
- Using the StarOS CLI for Initial Configuration

**Important:** An ASR 9000 VSM contains four physical CPUs. Each CPU runs an individual VPC-VSM instance (StarOS VM). StarOS parameters must be separately configured on each instance.
Using the StarOS Quick Setup Wizard

The Quick Setup Wizard consists of three parts:

- Configuring a context-level security administrator and hostname
- Configuring the Ethernet interface for out-of-band (OOB) management
- Configuring the system for remote CLI access via Telnet, Secure Shell (SSH), or File Transfer Protocol (FTP)

The following figure and table provides a flow diagram that shows the run logic of the wizard along with additional information and notes.
Getting Started

Using the StarOS Quick Setup Wizard

Figure 2. StarOS Quick Setup Wizard Logic Diagram

Table 2. Quick Setup Wizard Logic Diagram Callout Descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Task</th>
<th>Description/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter or exit the wizard. Enter no at the prompt to automatically be directed to the command line interface (CLI). Proceed to Using the StarOS CLI for Initial Configuration for instructions on performing an initial system configuration with the CLI. Enter setup at the command prompt to re-invoke the wizard.</td>
<td></td>
</tr>
</tbody>
</table>
### Item | Task | Description/Notes
---|---|---
2 | Configure an administrative username/password and the a hostname for the system. | The name of the default administrative user configured through the wizard is `admin`.  
Administrative user name is an alphanumeric string of 1 through 32 characters that is case sensitive.  
Administrative user password is an alphanumeric string of 1 through 63 characters that is case sensitive.  
Configure a valid, non-null hostname. The hostname is an alphanumeric string of 1 through 63 characters that is case sensitive.  

3 | Configure a single out-of-band management interface for the system. | Traffic on the management LAN is not transferred over the same media as user data and control signaling.  
For security reasons, it is recommended that management functions be maintained on a separate network from user data and control signaling.  
Configure an IP address, subnet mask, and gateway for the interface.  

4 | Enable the remote access protocol for accessing the system. | Secure Shell (SSH) uses TCP port number 22 by default, if enabled.  
SSH V1 and/or V2 are supported.  
**For maximum security, use only SSH v2.**  

5 | Enable file transfer protocols for copying files to/from the system. | If SSH is enabled, you can also enable SSH File Transfer Protocol (SFTP) server functionality.  
Telnet uses TCP port number 23 by default, if enabled.  
The File Transfer Protocol (FTP) uses TCP port number 21 by default, if enabled.  

6 | Review and/or modify the configuration of previous prompts. | 1. Enter the number of the prompt to be modified.  
2. Configure the parameter.  
3. *Optional.* Repeat *step 1* and *step 2* to modify additional settings.  
4. Enter “done” when you have completed all changes.  

7 | Review the configure script created by the wizard based on your inputs. | An sample of a created script is displayed in the example below. Variables are displayed in italics *(variable)*.  

8 | Apply the configuration file to the system. | Once applied, the parameter configuration is automatically saved to the system.cfg file stored in /flash memory.  

Using the StarOS CLI for Initial Configuration

The initial configuration consists of the following:

- Configuring a context-level security administrator and hostname
- Configuring the Ethernet interface on the vNIC
- Configuring the system for remote CLI access via Telnet, SSH, or FTP (secured or unsecured)

This section provides instructions for performing these tasks using the CLI.

Step 1  Log into the Console port via the hypervisor.

Step 2  At the CLI prompt, enter:

```
[local]host_name# configure
[local]host_name(config)#
```

Step 3  Enter the context configuration mode by entering the following command:

```
[local]host_name(config)# context local
[local]host_name(config-ctx)#
```

The `local` context is the system’s management context. Contexts allow you to logically group services or interfaces. A single context can consist of multiple services and can be bound to multiple interfaces.

Step 4  Enter the following command to configure a context-level security administrator for the system:

```
administrator user_name [ encrypted ] password password | [ ecs ] [ expiry-date date_time ] [ ftp ] [ li-administration ] [ nocli ] [ noecs ] [ timeout-absolute timeout_absolute ] [ timeout-min-absolute timeout_min_absolute ] [ timeout-idle timeout_idle ] [ timeout-min-idle timeout_min_idle ]
```

**Important:** You must configure a context-level security administrator during the initial configuration. After you complete the initial configuration process and end the CLI session, if you have not configured a security administrator, CLI access will be locked. See the Context Configuration Mode Commands chapter in the Command Line Interface Reference for complete information about this command.

Step 5  Enter the following command at the prompt to exit the context configuration mode:

```
[local]host_name(config-ctx)# exit
[local]host_name(config)#
```

Step 6  Enter the following command to configure a hostname by which the system will be recognized on the network:

```
[local]host_name(config)# system hostname host_name
```

`host_name` is the name by which the system will be recognized on the network. The hostname is an alphanumeric string of 1 through 63 characters that is case sensitive.
Step 7 Configure the network interfaces on the vNIC as follows:

**Step a** Enter the context configuration mode by entering the following commands:

```
[local]host_name(config)# context local
[local]host_name(config-ctx)#
```

**Step b** Enter the following command to specify a name for the interface:

```
[local]host_name(config-ctx)# interface interface_name
```

*interface_name* is the name of the interface expressed as an alphanumeric string of 1 through 79 characters that is case sensitive. The following prompt appears as the system enters the Ethernet Interface Configuration mode:

```
[local]host_name(config-if-eth)#
```

**Step c** Configure an IP address for the interface configured in the previous step by entering the following command:

```
{ ip address | ipv6 address } ipaddress subnetmask
```

**Important:** If you are executing this command to correct an address or subnet that was mis-configured with the Quick Setup Wizard, you must verify the default route and port binding configuration. Use step 11 and step 6 of this procedure. If there are issues, perform steps 7e through 7k to reconfigure the information.

**Step d** Enter the following command to exit the Ethernet interface configuration mode:

```
[local]host_name(config-if-eth)# exit
[local]host_name(config-ctx)#
```

**Step e** Configure a static route, if required, to point the system to a default gateway. Entering the following command:

```
{ ip | ipv6 } route gw_address interface_name
```

**Step f** Enter the following to exit from the context configuration mode:

```
[local]host_name(config-ctx)# exit
[local]host_name(config)#
```

**Step g** Enter the Ethernet Port Configuration mode:

```
port ethernet slot#/port#
```

For VPC, the slot number is always “1”. The vNIC traffic ports are 10 through 21. Port 1 is the management port.

**Step h** Bind the port to the interface that you created in step 7b. Binding associates the port and all of its settings to the interface. Enter the following command:

```
[local]host_name(config-port-slot#/port#)# bind interface interface_name local
[local]host_name(config-port-slot#/port#)# no shutdown
```
interface_name is the name of the interface that you configured in step 7b.

**Step 1** Exit the Ethernet Interface Configuration mode by entering the command:

```
[local]host_name(config-port-slot#/port#)# exit
[local]host_name(config)#
```

**Important:** Refer below for instructions on configuring the vNIC management interface with a second IP address.

### Configuring the Management Interface with a Second IP Address

If necessary, you can configure a second IP address on the vNIC management interface.

**Step 1** Enter the configuration mode by entering the following command at the prompt:

```
[local]host_name# configure
[local]host_name(config)#
```

**Step 2** Enter the following to enter the context configuration mode:

```
[local]host_name(config)# context local
[local]host-name(config-ctx)#
```

**Step 3** Enter the interface slot number and port number via the following command:

```
[local]host_name(config-ctx)# 1/1
[local]host_name(config-if-eth)#
```

**Step 4** Enter the secondary IP address and subnet mask by entering the following command:

```
[local]host_name(config-if-eth)# { ip | ipv } address ipaddr subnet_mask secondary
```

**Step 5** Exit the configuration mode by entering the following command:

```
[local]host_name(config-if-eth)# end
```

**Step 6** Confirm the interface ip addresses by entering the following command:

```
[local]host_name# show config context local
```

The CLI output should look similar to this example:

```
config

context local

    interface interface_name
```
Step 7  Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## Configuring the System for Remote Access

Configure the system for remote access. An administrative user may access the system from a remote location over a local area network (LAN) or wide area network (WAN):

- Telnet
- Secure Shell (SSH)
- File Transfer Protocol (FTP) (secured or unsecured)
- Trivial File Transfer Protocol (TFTP)

### Important:
If there are two simultaneous telnet sessions, and one administrator deletes the context into which the other administrator is logged, the administrator in the deleted context will not be automatically kicked into the local context. Although the deleted context will still appear in the CLI prompt, context specific commands will generate errors.

### Important:
For maximum security, use SSH v2.

### Steps:

#### Step 1
Enter the context configuration mode by entering the following command:

```
[local]host_name(config)# context local
[local]host_name(config-ctx)#
```

#### Step 2
Configure the system to allow Telnet access, if desired:

```
[local]host_name(config-ctx)# server telnetd
```

#### Step 3
Configure the system to allow SSH access, if desired:

```
[local]host_name(config-ctx)# ssh generate key [ type { v1-rsa | v2-rsa | v2-dsa } ]
```

### Important:
`v2-rsa` is the recommended key type.

```
[local]host_name(config-ctx)# server sshd
[local]host_name(config-sshd)# subsystem sftp
[local]host_name(config-sshd)# exit
```
Step 4  Configure the system to allow FTP access, if desired, by entering the following command:

```
[local]host_name(config-ctx)# server ftpd
```

Step 5  Exit the configuration mode by entering the following command:

```
[local]host_name(config-ctx)# end
[local]host_name#
```

Step 6  Verify the configuration by entering the following command:

```
[local]host_name# show configuration
```

The CLI output should be similar to the sample output:

```
context local
    interface interface_name
        ip address ipaddress subnetmask
        exit
    subscriber default
        exit
    administrator admin_name password admin_password
    server telnetd
    server ftpd
    ssh generate key
    server sshd
    subsystem sftp
        exit
    port ethernet 1/1
        bind interface interface_name local
        exit
    port ethernet 1/1
        no shutdown
        exit
    snmp engine-id local 800007e580ed826c191ded2d3d
end
```
Step 7  Verify the configuration of the IP routes by entering the following command:

```
[local]host_name# show ip route
```

The CLI output should be similar to the sample output:

```
"*" indicates the Best or Used route.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0.0.0.0/0</td>
<td>ipaddress</td>
<td>static</td>
<td>1</td>
<td>0</td>
<td>vnic1</td>
</tr>
<tr>
<td>*network</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td>vnic1</td>
</tr>
</tbody>
</table>
```

Step 8  Verify the interface binding by entering the following command:

```
[local]host_name# show ip interface name interface_name
```

`interface_name` is the name of the interface that was configured in step 7b. The CLI output should be similar to the sample output:

```
Intf Name: vnic1 Intf Type: Broadcast
Description:
IP State: UP (Bound to 1/1 untagged, ifIndex 83951617)
IP Address: ipaddress Subnet Mask: subnetmask
Bcast Address: bcastaddress MTU: 1500
Resoln Type: ARP ARP timeout: 3600 secs
L3 monitor LC-port switchover: Diasabled
Number of Secondary Addresses: 0
```

Step 9  Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
Chapter 4
System Settings

This chapter provides instructions for configuring the following StarOS options for a VPC-VSM instance:

- Configuring a Second Management Interface
- Verifying and Saving Your Interface and Port Configuration
- Configuring System Timing
- Enabling CLI Timestamping
- Configuring System Administrative Users
- Configuring TACACS+ for System Administrative Users

It is assumed that the procedures to initially configure a VPC-VSM instance as described in the Getting Started chapter have been completed.

**Important:** An ASR 9000 VSM contains four physical CPUs. Each CPU runs an individual VPC-VSM instance (StarOS VM). StarOS must be separately configured on each instance.

**Important:** You must log into the StarOS VM to complete the procedures described in this chapter.

**Important:** The commands used in the configuration examples in this section are the most likely-used commands and/or keyword options. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information.
Configuring a Second Management Interface

Refer to the Getting Started chapter for instructions on configuring a system management interface for the StarOS VM. This section provides described how to configure a second management interface.

Use the following example to configure a second management interface:

```
configure
  context local
    interface interface_name
      ip address ipaddress subnetmask
    exit
    ip route 0.0.0.0 0.0.0.0 gw_address interface_name
    exit
    port ethernet slot#/port#
      bind interface interface_name local
      no shutdown
      media [ rj45 | sfp ]
    end
```

Notes:
- For port ethernet slot#, always use slot number 1.
- Enter IP addresses using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- For port ethernet port#, always use slot 1, port 1.
- Option: In the Ethernet Port configuration mode, configure the port speed, if needed, by entering the medium command. Refer to the Command Line Interface Reference for a complete explanation of this command.
- In the { ip | ipv6 } route command, other keyword options, instead of the gateway IP address, are available and include: next-hop IP address, point-to-point, and tunnel.
Verifying and Saving Your Interface and Port Configuration

Verify that your interface configuration settings are correct by entering the following CLI command:

```
show ip interface
```

The output from this command should be similar to that shown below. In this example an interface named `management1` was configured in the local context.

```
Intf Name: LOCAL1
Intf Type: Broadcast
Description: management1
VRF: None
IP State: UP (Bound to 1/1 untagged, ifIndex 16842753)
IP Address: 192.168.100.3 Subnet Mask: 255.255.255.0
Bcast Address: 192.168.100.255 MTU: 1500
Resoln Type: ARP ARP timeout: 60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
```

Verify that the port configuration settings are correct by entering the following command:

```
show configuration port slot#/port#
```

`slot#` is the chassis slot number of the line card where the port resides. For VPC `slot#` is always 1. `port#` is the number of the port (1, 10 – 21).

This previous command produces an output similar to the one shown below. It displays the configuration of port 1 in slot 1.

```
config

port ethernet 1/1

no shutdown

bind interface LOCAL1 local
```

Save your configuration as described in the Verifying and Saving Your Configuration chapter.
Configuring System Timing

After the initial configuration of the StarOS system clock, you should configure StarOS to communicate with one or more Network Time Protocol (NTP) server(s) to ensure that the clock is always accurate. In addition to configuring the timing source, you must configure the system’s time zone.

Setting the StarOS System Clock and Time Zone

Use the following command example to configure the StarOS system clock and time zone:

```
clock set date:time
clock timezone timezone [ local ]
```

Notes:
- Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
- Refer to the online Help for the `clock timezone` command for a complete list of supported time zones.
- The optional `local` keyword indicates that the time zone specified is the local timezone.
- Daylight Savings Time is automatically adjusted for time zones supporting it.

Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Verifying and Saving Your Clock and Time Zone Configuration

Enter the following command to verify that you configured the time and time zone correctly:

```
show clock
```

The output displays the date, time, and time zone that you configured.

Configuring Network Time Protocol Support

This section provides information and instructions for configuring StarOS to enable the use of the Network Time Protocol (NTP).

**Important:** Configure the StarOS system clock and time zone prior to implementing NTP support. This greatly reduces the time period that must be corrected by the NTP server.
**Important:** NTP should also be configured on the ASR 9000. The StarOS NTP configuration should match that of the ASR 9000.

Many of the services offered by StarOS require accurate timekeeping derived through NTP. If the time reference(s) used by StarOS are not accurate, the services may be unreliable. For this reason it should be assumed that normal system operation requires that NTP be configured.

StarOS uses NTP to synchronize internal clocks on the chassis to external time sources (typically GPS NTP sources, or other Stratum 2 or 3 servers, switches or routers).

By default, NTP is not enabled and should be configured when StarOS is initially installed. When enabled, StarOS will synchronize with external sources. If not enabled, StarOS will use its local clock (VSM) as a time source. In the event of an NTP server or network outage, StarOS will continue to use NTP to maintain time accuracy, but in a holdover mode.

StarOS should have:
- NTP enabled.
- NTP configured for use in the **local** context only. Use of other contexts (which can be specified in the enable configurable) will cause issues.
- NTP configured for at least **three** external NTP servers. With three or more servers, outliers and broken or misconfigured servers can be detected and excluded. Generally, the more servers the better (within reason).

**Important:** Do not configure any external NTP servers using the `prefer` keyword. The NTP clock selection algorithms already have the built-in ability to pick the best server. Use of `prefer` usually results in a poorer choice than NTP can determine for itself.

**Important:** Do not change the `maxpoll`, `minpoll`, or `version` keyword settings unless instructed to do so by Cisco TAC.

Use the following example to configure the necessary NTP association parameters:

```
configure
  ntp
    enable
    server ip_address1
    server ip_address2
    server ip_address3
  end
```

**Notes:**
- By default `context_name` is set to `local`. This is the recommended configuration.
- A number of options exist for the `server` command. Refer to the `NTP Configuration Mode Commands` chapter in the `Command Line Interface Reference` for more information.
Enter the IP address of NTP servers using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** Configure StarOS with at least three (preferably four) NTP servers.

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

### Configuring NTP Servers with Local Sources

NTP can use network peers, local external clocks (such as GPS devices), or a local clock with no external source. A local clock with no external source is usually a last-resort clock when no better clock is available. It is typically configured on a site's intermediate NTP server so that when a WAN network outage occurs, hosts within the site can continue to synchronize amongst themselves.

You can configure this in ntpd or on many commercially available NTP devices. This local clock should always have a high stratum number (8+) so that under normal conditions (when real sources are available) this local clock will not be used.

### Using a Load Balancer

The NTP daemon and protocol assume that each configured server is running NTP. If an NTP client is configured to synchronize to a load balancer that relays and distributes packets to a set of real NTP servers, the load balancer may distribute those packets dynamically and confuse the NTP client. NTP packets are latency and jitter sensitive. Relaying them through a load balancer can confuse the NTP client and is not a supported practice.

### Verifying the NTP Configuration

Verify the NTP configuration is correct. Enter the following command at the Exec mode prompt:

```
show ntp associations
```

The output displays information about all NTP servers. See the output below for an example deploying two NTP servers.

```
+-----Peer Selection: ( ) - Rejected / No Response
| (x) - False Tick
| (. ) - Excess
| (-) - Outlyer
| (+) - Candidate
| (#) - Selected
| (*) - System Peer
| (o) - PPS Peer
```
Enabling CLI Timestamping

To display a timestamp (date and time) for every command that is executed on the CLI, enter the following command at the root prompt for the Exec mode:

```
timestamps
```

The date and time appear immediately after you execute the command.

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring System Administrative Users

Getting Started describes how to configure a StarOS context-level security administrator.

This section provides instructions for configuring additional administrative users having the following privileges:

- **Security Administrators**: have read-write privileges and can execute all CLI commands, including those available to Administrators, Operators, and Inspectors

- **Administrators**: have read-write privileges and can execute any command in the CLI except for a few security-related commands that can only be configured by Security Administrators. Administrators can configure or modify system settings and execute all system commands, including those available to the Operators and Inspectors.

- **Operators**: have read-only privileges to a larger subset of the Exec Mode commands. They can execute all commands that are part of the inspector mode, plus some system monitoring, statistic, and fault management functions. Operators do not have the ability to enter the Config Mode.

- **Inspectors**: are limited to a few read-only Exec Mode commands. The bulk of these are show commands for viewing a variety of statistics and conditions. An Inspector cannot execute show configuration commands and does not have the privilege to enter the Config Mode.

Configuration instructions are categorized according to the type of administrative user: context-level or local-user.

**Important**: For information on the differences between these user privileges and types, refer to the *Getting Started* chapter.

Configuring Context-level Administrative Users

This section contains information and instructions for configuring context-level administrative user types.
Configuring Context-level Security Administrators

Use the example below to configure additional security administrators:

```plaintext
configure

class local

administrator user_name { [ encrypted ] [ nopassword ] password password }

end
```

Notes:

- Additional keyword options are available that identify active administrators or place time thresholds on the administrator. Refer to the Command Line Interface Reference for more information about the `administrator` command.

- The `nopassword` option allows you to create an administrator without an associated password. Enable this option when using ssh public keys (`authorized key` command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an administrator password to gain access to the user account.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Configuring Context-level Administrators

Use the example below to configure context-level administrators:

```plaintext
configure

class local

config-administrator user_name { [ encrypted ] [ nopassword ] password password }

end
```

Notes:

- Additional keyword options are available that identify active administrators or place time thresholds on the administrator. Refer to the Command Line Interface Reference for more information about the `config-administrator` command.

- The `nopassword` option allows you to create a config-administrator without an associated password. Enable this option when using ssh public keys (`authorized key` command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using a config-administrator password to gain access to the user account.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Configuring Context-level Operators

Use the example below to configure context-level operators:

```plaintext
configure
```
context local

operator name { password pwd | encrypted password pwd }

d end

Notes:
- Additional keyword options are available that identify active administrators or place time thresholds on the administrator. Refer to the Command Line Interface Reference for more information about the operator command.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Configuring Context-level Inspectors

Use the example below to configure context-level inspectors:

configure

context local

inspector name { password pwd | encrypted password pwd }

d end

Notes:
- Additional keyword options are available that identify active administrators or place time thresholds on the administrator. Refer to the Command Line Interface Reference for more information about the inspector command.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Verifying Context-level Administrative User Configuration

Verify that the configuration was successful by entering the following command:

show configuration context local

This command displays all of the configuration parameters you modified within the Local context during this session. The following displays sample output for this command. In this example, a security administrator named testadmin was configured.

config
context local
interface mgmt1
ip address 192.168.1.10 255.255.255.0
#exit
subscriber default
#exit

administrator testadmin encrypted password fd01268373c5da85
inspector testinspector encrypted password 148661a0bb12cd59

exit

port ethernet 1/1
bind interface mgmt1 local
#exit
end

Configuring Local-User Administrative Users

Use the example below to configure local-user administrative users:

```
configure
  local-user username name
end
```

Notes:

- Additional keyword options are available identify active administrators or place time thresholds on the administrator. Refer to the Command Line Interface Reference for more information about the `local-user username` command.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Verifying Local-User Configuration

Verify that the configuration was successful by entering the following command:

```
show local-user verbose
```

This command displays information on configured local-user administrative users. A sample output for this command appears below. In this example, a local-user named `SAUser` was configured.

<table>
<thead>
<tr>
<th>Username:</th>
<th>SAUser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Level:</td>
<td>secadmin</td>
</tr>
<tr>
<td>Last Login:</td>
<td>Never</td>
</tr>
<tr>
<td>Login Failures:</td>
<td>0</td>
</tr>
<tr>
<td>Password Expired:</td>
<td>Yes</td>
</tr>
<tr>
<td>Locked:</td>
<td>No</td>
</tr>
</tbody>
</table>
Suspended: No
Lockout on Pw Aging: Yes
Lockout on Login Fail: Yes

**Updating Local User Database**

Update the local user (administrative) configuration by running the following Exec mode command. This command should be run immediately after creating, removing or editing administrative users.

```
update local-user database
```

**Restricting User Access to a Specified Root Directory**

By default an admin user who has FTP/SFTP access can access and modify any files under the /mnt/user/ directory. Access is granted on an “all-or-nothing” basis to the following directories: /flash, /cdrom, /hd-rai, /records, /usb1 and /usb2

An administrator or configuration administrator can create a list of SFTP subsystems with a file directory and access privilege. When a local user is created, the administrator assigns an SFTP subsystem. If the user’s authorization level is not security admin or admin, the user can only access the subsystem with read-only privilege. This directory is used as the user’s root directory. The information is set as environmental variables passed to the openssh SFTP-server.

You must create the SFTP root directory before associating it with local users, administrators and config administrators. You can create multiple SFTP directories; each directory can be assigned to one or more users.

**Configuring an SFTP root Directory**

The `subsystem sftp` command allows the assignment of an SFTP root directory and associated access privilege level.

```
configure
class context local
  server sshd
    subsystem sftp [ name sftp_name root-dir pathname mode { read-only | readwrite } ]
```

Notes:
- `sftp_name` is an alphanumeric string that uniquely identifies this subsystem.
- `pathname` specifies the root directory to which SFTP files can be transferred. Options include:
  - `/hd-rai/records/cdr`
  - `/flash`
Associating an SFTP root Directory with a Local User

The `local-user username` command allows an administrator to associate an SFTP root directory with a specified username.

```
configure

local-user username user_name authorization-level level ftp sftp-server
sftp_name password password

exit
```

Associating an SFTP root Directory with an Administrator

The `administrator` command allows an administrator to associate an SFTP root directory for a specified administrator.

```
configure

context local

administrator user_name password password ftp sftp-server sftp_name

exit
```

Associating an SFTP root Directory with a Config Administrator

The `config-administrator` command allows an administrator to associate an SFTP root directory with a specified configuration administrator.

```
configure

context local

config-administrator user_name password password ftp sftp-server sftp_name

exit
```

Configuring TACACS+ for System Administrative Users

This section describes TACACS+ (Terminal Access Controller Access Control System+) AAA (Authentication Authorization and Accounting) service functionality and configuration for StarOS.

Operation

TACACS+ is a secure, encrypted protocol. By remotely accessing TACACS+ servers that are provisioned with the administrative user account database, StarOS can provide TACACS+ AAA services for system administrative users. TACACS+ is an enhanced version of the TACACS protocol that uses TCP instead of UDP.
StarOS serves as the TACACS+ Network Access Server (NAS). As the NAS the system requests TACACS+ AAA services on behalf of authorized system administrative users. For the authentication to succeed, the TACACS+ server must be in the same local context and network accessed by StarOS.

StarOS supports TACACS+ multiple-connection mode. In multiple-connection mode, a separate and private TCP connection to the TACACS+ server is opened and maintained for each session. When the TACACS+ session ends, the connection to the server is terminated.

TACACS+ AAA service configuration is performed in StarOS TACACS Configuration Mode. Enabling the TACACS+ function is performed in the StarOS Global Configuration Mode. StarOS supports the configuration of up to three TACACS+ servers.

Once configured and enabled in StarOS, TACACS+ authentication is attempted first. By default, if TACACS+ authentication fails, StarOS then attempts to authenticate the user using non-TACACS+ AAA services, such as RADIUS.

---

**Important:** For releases after 15.0 MR4, TACACS+ accounting (CLI event logging) will not be generated for Lawful Intercept users with privilege level set to 15 and 13.

### User Account Requirements

Before configuring TACACS+ AAA services for StarOS, note the following TACACS+ server and StarOS user account provisioning requirements.

#### TACACS+ User Account Requirements

The TACACS+ server must be provisioned with the following TACACS+ user account information:

- A list of known administrative users.
- The plain-text or encrypted password for each user.
- The name of the group to which each user belongs.
- A list of user groups.
- TACACS+ privilege levels and commands that are allowed/denied for each group.

---

**Important:** TACACS+ privilege levels are stored as Attribute Value Pairs (AVPs) in the network’s TACACS+ server database. Users are restricted to the set of commands associated with their privilege level. A mapping of TACACS+ privilege levels to the StarOS CLI administrative roles and responsibilities is provided in the table below.

<table>
<thead>
<tr>
<th>TACACS+ Privilege Level</th>
<th>StarOS CLI Administrative Access Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CLI</td>
</tr>
<tr>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
</tr>
</tbody>
</table>
### Configuring TACACS+ for System Administrative Users

<table>
<thead>
<tr>
<th>TACACS+ Privilege Level</th>
<th>StarOS CLI Administrative Access Privileges</th>
<th>CLI</th>
<th>FTP</th>
<th>ECSEMS</th>
<th>Lawful Intercept</th>
<th>CLI Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Inspector</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Inspector</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Operator</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Operator</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Operator</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Operator</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Operator</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Administrator</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Administrator</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Administrator</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Administrator</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Administrator</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Administrator</td>
</tr>
</tbody>
</table>

**Important:** TACACS+ priv-levels can be reconfigured from their default StarOS authorization values via the TACACS+ Configuration mode `priv-lvl` and `user-id` commands. For additional information, see the TACACS+ Configuration Mode Commands chapter of the Command Line Interface Reference.

### User Account Requirements

TACACS+ users who are allowed administrative access to the StarOS CLI must have the following user account information defined on the VPC:

- username
- password
- administrative role and privileges

**Important:** For instructions on defining StarOS users and administrative privileges, refer to Configuring System Administrative Users.

### Configuring TACACS+ AAA Services

This section provides an example of how to configure TACACS+ AAA services for StarOS administrative users.
Caution: When configuring TACACS+ AAA services for the first time, the administrative user must use non-TACACS+ services to log into StarOS. Failure to do so will result in the TACACS+ user being denied access to the StarOS CLI.

Log StarOS VPC using non-TACACS+ services.

Use the example below to configure TACACS+ AAA services in StarOS:

```
configure
tacacs mode
    server priority priority_number ip-address tacacs+srvr_ip_address
end
```

Note:
- **server priority priority_number**: Must be a number from 1 to 3, that specifies the order in which this TACACS+ server will be tried for TACACS+ authentication. 1 is the highest priority, and 3 is the lowest.
- **ip-address**: Must be the IPv4 address of a valid TACACS+ server that will be used for authenticating administrative users accessing this system via TACACS+ AAA services.
- By default, the TACACS+ configuration will provide authentication, authorization, and accounting services.

Enable TACACS+ via the StarOS CLI:

```
configure
    aaa tacacs+
end
```

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: For complete information on all TACACS+ Configuration Mode commands and options, refer to the *TACACS Configuration Mode Commands* chapter in the *Command Line Reference*.

**Configuring TACACS+ for Non-local VPN Authentication**

By default TACACS+ authentication is associated with login to the local context. TACACS+ authentication can also be configured for non-local context VPN logins. TACACS+ must configured and enabled with the option described below.

A stop keyword option is available for the TACACS+ Configuration mode on-unknown-user command. If TACACS+ is enabled with the command-keyword option, the VPN context name into which the user is attempting a login must match the VPN name specified in the username string. If the context name does not match, the login fails and exits out.

Without this option the login sequence will attempt to authenticate in another context via an alternative login method. For example, without the on-unknown-user stop configuration, an admin account could log into the local context via the non-local VPN context. However, with the on-unknown-user stop configuration, the local context login would not be attempted and the admin account login authentication would fail.

```
configure
```
```
tacacs mode
  on-unknown-user stop ?
end
```

Verifying the TACACS+ Configuration

This section describes how to verify the TACACS+ configuration.

Log out of StarOS, then log back in using TACACS+ services.

**Important:** Once TACACS+ AAA services are configured and enabled on the VPC, StarOS first will try to authenticate the administrative user via TACACS+ AAA services. By default, if TACACS+ authentication fails, StarOS then continues with authentication using non-TACACS+ AAA services.

At the Exec Mode prompt, enter the following command:

```
show tacacs [ client | privilege-level | session | summary ]
```

The output of the `show tacacs` commands provides summary information for each active TACACS+ session such as username, login time, login status, current session state and privilege level. Optional filter keywords provide additional information.

An example of this command’s output is provided below. In this example, a system administrative user named `ssiadmin` has successfully logged into StarOS via TACACS+ AAA services.

```
active session #1:
  login username : ssiadmin
  login tty : /dev/pts/1
  current login status : pass
  current session state : user login complete
  current privilege level : 15
  remote client application : ssh
  remote client ip address : 111.11.11.11
  last server reply status : -1
  total TACACS+ sessions : 1
```

**Important:** For details on all TACACS+ maintenance commands, refer to the Command Line Interface Reference.
Chapter 5
SNMP Configuration

This chapter provides instructions for configuring Simple Network Management Protocol (SNMP) options for a VPC-VSM instance (StarOS VM). It includes the following topics:

- SNMP Support
- Configuring SNMP and Alarm Server Parameters
- Verifying SNMP Parameters
- Controlling SNMP Trap Generation

*Important:* ASR 9000 SNMP MIBs may also be configured to monitor hardware and network events. For additional information, refer to the ASR 9000 user documentation.

*Important:* An ASR 9000 VSM contains four physical CPUs. Each CPU runs an individual VPC-VSM instance (StarOS VM). SNMP must be separately configured on each instance.
SNMP Support

StarOS uses the SNMP to send traps or events to alarm servers on the network. You must configure SNMP settings to communicate with those devices.

**Important:** Commands used in the configuration samples in this section provide base functionality. The most common commands and keyword options are presented. In many cases, other optional commands and keyword options are available. Refer to the *Command Line Interface Reference* for complete information.

The *SNMP MIB Reference* describes the MIBs and SNMP traps supported by StarOS.

To configure the system to communicate with an alarm server:

**Step 1**  
Set SNMP parameters such as UDP port, and alarm server target by applying the example configuration in *Configuring SNMP and Alarm Server Parameters*.

**Step 2**  
To view your new SNMP configuration, follow the steps in *Verifying SNMP Parameters*.

**Step 3**  
Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.
Configuring SNMP and Alarm Server Parameters

Use the following example to set SNMP and alarm server parameters:

```
configure
    system contact contact_name
    system location location_name
    snmp authentication-failure-trap
    snmp community community_string
    snmp server port port_number
    snmp target name ip_address
    snmp engine-id local id_string
    snmp notif-threshold value low low_value period time_period
    snmp user user_name
    snmp mib mib_name
    snmp runtime-debug [ debug-tokens token_id token_id token_id...token_id
end
```

Notes:

- The **system contact** is the name of the person to contact when traps are generated that indicate an error condition.

- An **snmp community** string is a password that allows access to system management information bases (MIBs). The system can send SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices.

- The **snmp notif-threshold** command configures the number of SNMP notifications that need to be generated for a given event and the number of seconds in the monitoring window size (default = 300), before the notification is propagated to the SNMP users (default = 100).

- The **snmp engine-id local** command is optional. It is only required if your network requires SNMP v3 support. The engine ID uniquely identifies the SNMP engine and associated SNMP entities, thus providing a security association between the two for the sending and receiving of data.

- The **snmp user** name is for SNMP v3 and is optional. There are numerous keyword options associated with this command.

- Use the **snmp mib** command to enable other industry standard and Cisco MIBs. To see a list of supported MIBs, use the Exec mode **show snmp server** command.

- By default SNMP runtime debugging always runs and consumes CPU cycles for event logging. To control CPU usage you can set **no snmp runtime-debug** to disable runtime debugging. An option to this command allows you to specify SNMP token values that will locate and parse specified MIBs.
Verifying SNMP Parameters

Step 1 Run the `show snmp server` command to verify that the SNMP server information is correctly configured. The following displays a sample output of this command.

SNMP Server Configuration:

- Server State : enabled
- SNMP Port : 161
- sysLocation : chicago
- sysContact : admin
- authenticationFail traps : Enabled
- EngineID : 123456789
- Alert Threshold : 100 alerts in 300 seconds
- Alert Low Threshold : 20 alerts in 300 seconds

SNMP Agent Mib Configuration:

- STARENT-MIB : Enabled
- IF-MIB : Disabled
- ENTITY-MIB : Disabled
- ENTITY-STATE-MIB : Disabled
- ENTITY-SENSORE-MIB : Disabled
- HOST-RESOURCES-MIB : Disabled
- CISCO-MOBILE-WIRELESS-SERVICE-MIB : Disabled
- CISCO-ENTITY-DISPLAY-MIB : Disabled
- CISCO-ENTITY-FRU-CONTROL-MIB : Disabled
- CISCO-ENTITY-REDUNDANCY-MIB : Disabled
- CISCO-IP-LOCAL-POOL-MIB : Disabled
- CISCO-PROCESS-MIB : Disabled
- CISCO-FLASH-MIB : Disabled
- CISCO-IPSEC-FLOW-MONITOR-MIB : Disabled
- CISCO-ENHANCED-IPSEC-FLOW-MIB : Disabled
**Step 2**  Verify that the SNMP community(ies) were configured properly by entering the following command:

```
show snmp communities
```

The output of this command lists the configured SNMP communities and their corresponding access levels.

**Step 3**  Verify that the SNMP transports are configured properly by entering the following command:

```
show snmp transports
```

The following displays a sample output:

```
Target Name: rms1
IP Address: 192.168.1.200
Port: 162
Default: Default
Security Name: public
Version: 1
Security: 
View: 
Notif Type: traps
```
Controlling SNMP Trap Generation

The system uses SNMP traps (notifications) to indicate that certain events have occurred. By default, the system enables the generation of all traps. However, you can disable individual traps to allow only traps of a certain type or alarm level to be generated. This section provides instructions for disabling/enabling SNMP traps.

**Important:** Commands used in the configuration samples in this section provide base functionality. The most common commands and keyword options are presented. In many cases, other optional commands and keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

To configure SNMP trap generation:

**Step 1** Set parameters by applying the following example configuration:

```
configure

snmp trap suppress

snmp trap suppress trap_name1 trap_name2 ... trap_nameN
```

**Important:** If at a later time you wish to re-enable a trap that was previously suppressed, use the `snmp trap enable` command.

```
snmp trap enable trap_name1 trap_name2 ... trap_nameN target target-name
```

**Step 2** Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.
Chapter 6
Verifying and Saving Your Configuration

This chapter describes how to save the configuration files for VPC-VMS instances running on an ASR 9000 VSM. It includes the following sections:

- Verifying the Configuration
- Service Configuration
- Saving the Configuration
Verifying and Saving Your Configuration

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

**Important:** Each VPC-VSM instance (StarOS VM) is separately configured on a VSM (four VMs per VSM). You must separately configure and save each instance.

Feature Configuration

In many configurations, you have to set and verify specific features. An example includes IP address pool configuration. Using the example below, enter the listed commands to verify proper feature configuration.

Enter the `show connectedapps` command to display the StarOS oneP session configuration. The output from this command should look similar to the sample shown below.

```
Current connectedapps controller configuration:
    CA session usedid : vsm01
    CA session password : cisco123
    CA session name : wsg
    CA session IP address : 30.30.30.13
    RRI mode : ENABLED
    HA chassis mode : inter
    HA network mode : L3
    CA session Activation : YES
    CA session ID : 0
    CA SRP Status : INIT
    CA SRP State : INIT
```

**Important:** To configure features on the system, use the `show` commands specifically for these features. Refer to the **Exec Mode show Commands** chapter in the **Command Line Interface Reference** for more information.
Service Configuration

Verify that your service was created and configured properly by entering the following command:

```bash
show service_type name service_name
```

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a wsg-service called rav4 is configured.

Service name: rav4
Context: wsg
Bind: DONE
Max Sessions: 8000
IP address: 33.33.33.30  UDP Port: 500
MTU: 1400
Crypto template: rav4
deployment mode: 0

Context Configuration

Verify that your context was created and configured properly by entering the `show context name name` command.

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named wsg is configured.

<table>
<thead>
<tr>
<th>Context Name</th>
<th>ContextID</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>wsg</td>
<td>2</td>
<td>Active</td>
</tr>
</tbody>
</table>

System Configuration

Verify that your entire configuration file was created and configured properly by entering the `show configuration` command.

This command displays the entire configuration for the VPC-VSM instance, including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the `show configuration errors` command.
This command displays errors it finds within the configuration. For example, if you have created a service named “service1”, but entered it as “srv1” in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the section keyword and choose a section from the help menu as shown in the examples below.

    show configuration errors section wsg-service

If the configuration contains no errors, an output similar to the following is displayed:

    ####################################################################
    Displaying Global WSG system errors
    ####################################################################
    Total 0 error(s) in this section !
Saving the Configuration

save Command Syntax

These instructions assume that you are at the root prompt for the Exec mode of the target VPC-VSM instance:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [ obsolete-encryption | showsecrets | verbose ] [ -redundant ] [ -noconfirm ]
```

`url` specifies the location in which to store the configuration file. It may refer to a local or a remote file.

**Important:** Do not use the “/” (forward slash), “:” (colon) or “@” (at sign) characters when entering a string for the following URL fields: directory, filename, username, password, host or port#.

Refer to the Exec Mode Commands chapter of the Command Line Interface Reference for complete information about this command.

**Important:** To avoid the possibility of overwriting critical files, always assign a unique file name to each VPC-VSM instance running in the ASR 9000 chassis.

To save a configuration file called `vsm1-vm1.cfg` to a directory that was previously created in `/flash` memory called `cfgfiles`, enter the following command:

```
save configuration /flash/cfgfiles/vms1-vm1.cfg
```

To save a configuration file called `vsm1-vm1.cfg` to a directory called `host_name_configs`, using an FTP server with an IP address of `192.168.34.156`, on which you have an account with a username of `administrator` and a password of `secure`, use the following command:

```
save configuration sftp://administrator:secure@192.168.34.156/host_name_configs/vsm1-vm1.cfg
```

To save a configuration file called `vsm1-vm1.cfg` to the `root` directory of a TFTP server with a hostname of `config_server`, enter the following command:

```
save configuration tftp://config_server/vsm1-vm1.cfg
```

USB Devices

The USB ports on the VSM cannot be used to save configuration files.

The recommended procedure is to save VPC-VSM configurations to an external network device.
Chapter 7
Interfaces and Ports

This chapter describes how to create a context and configure interfaces and ports within the context for a VPC-VSM instance (StarOS VM). Before beginning these procedures, refer to the SecGW Administration Guide and ASR 9000 configuration guides for additional configuration information.

This chapter discusses the following topics:

- Contexts
- Ethernet Interfaces and Virtual Ports
- VLANs

**Important:** Interfaces and ports must be configured for each VPC-VSM instance running on an ASR 9000 VSM. One StarOS VM runs on each VSM CPU; there are four CPUs on each VSM.
Contexts

An operator can configure multiple StarOS contexts to perform specific functions. The contexts are all created using the same procedure.

Creating Contexts

Important: StarOS commands used in the configuration examples in this section represent the most common or likely commands and/or keyword options. In many cases, other commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

To create a context, apply the following example configuration:

```
configure
context ctx_name
end
```

Repeat to configure additional contexts.

Viewing and Verifying Contexts

Step 1  Verify that your contexts were successfully created by entering the following command:

```
show context all
```

The output is a two-column table similar to the example below. This example shows that two contexts were created: one named source and one named destination.

<table>
<thead>
<tr>
<th>Context Name</th>
<th>ContextID</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>1</td>
<td>Active</td>
</tr>
<tr>
<td>wsg</td>
<td>2</td>
<td>Active</td>
</tr>
<tr>
<td>srp</td>
<td>3</td>
<td>Active</td>
</tr>
</tbody>
</table>

The left column lists the contexts that are currently configured. The center column lists the corresponding context ID for each of the configured contexts. The third column lists the current state of the context.

Step 2  Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Step 3  Now that the context has been created, interfaces and specific functionality can be configured within the context. Proceed to other sections for instructions on configuring specific services and options.
Ethernet Interfaces and Virtual Ports

Regardless of the type of application interface, the procedure to create and configure it consists of the following:

**Step 1** Create an interface and assign an IP address and subnet mask to it by applying the example configuration in the Creating an Interface.

**Step 2** Assign a virtual port for use by the interface and bind the port to the interface by applying the example configuration in the Configuring a Virtual Port and Binding It to an Interface.

**Step 3** Optionally configure a static route for the interface by applying the example configuration in the Configuring a Static Route for an Interface.

**Step 4** Repeat the above steps for each interface to be configured.

---

**Important:** Interface configuration requires one-to-one mapping between the VPC-VSM virtual interfaces and the 10 Gbps (tengige) ports on the ASR 9000 RSP. This section provides the minimum instructions for configuring interfaces and ports to allow the system to communicate on the network. Commands that configure additional interface or port properties are described in the Ethernet Port Configuration Mode Commands and Ethernet Interface Configuration Mode Commands chapters in the Command Line Interface Reference.

---

**Caution:** To ensure that system line card and port-level redundancy mechanisms function properly, the Spanning Tree protocol must be disabled on devices connected directly to any port. Failure to turn off the Spanning Tree protocol may result in failures in the redundancy mechanisms or service outage.

For additional information, see Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router

### Creating an Interface

Use the following example to create a new interface in a context:

```
configure

context name

interface name

{ ip | ipv6 } address address subnetmask [ secondary ]

end
```

**Notes:**
- **Optional:** Add the `loopback` keyword option to the `interface name` command, to set the interface type as “loopback” which is always UP and not bound to any physical port.
• **Optional:** Add the `secondary` keyword to the `{ ip | ipv6 } address` command, to assign multiple IP addresses to the interface. IP addresses can be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

• **Optional:** In the interface config mode, add the `port-switch-on-L3-fail address` command, to configure the interface for switchover to the port on the redundant line card if connectivity to a specified IP address is lost. This IP address can be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### Configuring a Virtual Port and Binding It to an Interface

Use the following example configuration to configure and assign a port to an interface:

```bash
configure
  port ethernet slot#/port#
    description description
    no shutdown
    bind interface interface_name context_name
end
```

**Notes:**

- For `port ethernet slot#`, always use slot 1.
- For `port ethernet port#`, use ports 1 (mgmt) or 10 to 21 (traffic).
- Binding associates the port and all of its settings to the named interface.

### Configuring a Static Route for an Interface

Use the following example to configure a static route for an interface:

```bash
configure
  context name
    { ip | ipv6 } route ip_address netmask next-hop gw_address interface_name
end
```

**Notes:**

- `ip_address` and `netmask` are the IP address and subnet mask of the target network. This IP address can be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- `gw_address` is the IP address of the default gateway or next-hop route. This IP address can be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- To configure a route to the gateway router, use 0.0.0.0 for the network and mask variables.
- Repeat as needed. Multiple static routes can be configured to the same destination to provide an alternative means of communication in case the preferred route fails.
Viewing and Verifying Port Configuration

**Step 1** Verify that your interface configuration settings are correct by entering the following commands:

```
context context_name
show { ip | ipv6 } interface
```

`context_name` represents the name of the context in which the interface was created. The output from these commands should be similar to the following example.

In this example an interface named `clear` was configured in the local context.

```
Intf Name: clear
Intf Type: Broadcast
Description: 
VRF: None
IP State: UP (Bound to 1/11 untagged, ifIndex 285278209)
IP Address: 192.168.100.30 Subnet Mask: 255.255.255.0
Bcast Address: 192.168.100.255 MTU: 1500
Resoln Type: ARP ARP timeout: 60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
Total interface count: 0
```

**Step 2** Verify that your port configuration settings are correct by entering the following command:

```
show configuration port slot#/port#
```

`slot#` is the chassis slot number, always slot 1.

This command produces an output similar to that displayed in the following example that shows the configuration for port 11 in chassis slot 1.

In this example, the port is bound to an interface called `clear` configured in a context called `wsg`.

```
config

port ethernet 1/11
    description 11_clear
    no shutdown
    bind interface clear wsg
#end
```
Step 3  Verify that your static route(s) was configured properly by entering the following command:

```
show ip static-route
```

This command produces an output similar to that displayed in the following example that shows a static route to a gateway with an IP address of 192.168.250.1.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop</th>
<th>Protocol</th>
<th>Prec</th>
<th>Cost</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>192.168.250.1</td>
<td>Static</td>
<td>0</td>
<td>0</td>
<td>vNIC1</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>192.168.250.1</td>
<td>Static</td>
<td>0</td>
<td>0</td>
<td>clear wsg</td>
</tr>
</tbody>
</table>

Step 4  Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.
VLANs

Virtual LANs (VLANs) allow two logically separated networks to use the same physical medium. VLAN segmentation, also called 802.1q tagging, works by appending a tag identifying the VLAN ID to each Ethernet frame.

VLAN usage under KVM is an extension to bridge interface sharing. The difference lies in which interface participates in the bridge set. The physical interfaces (such as eth0, eth1) are bound to the bridge, which is used by each guest. These interfaces carry unmodified packets coming externally or being generated internally, with or without a VLAN ID tag.

For information on how to create VLANs to handle specific packet types, see the VLANs chapter.
Chapter 8
StarOS Security

This chapter describes the StarOS security features supported by VPC.

This chapter explores the following topics:

- Encrypted SNMP Community Strings
- Lawful Intercept Restrictions
- Adding Modifying and Removing Users
- Hidden Commands
Encrypted SNMP Community Strings

Simple Network Management Protocol (SNMP) uses community strings as passwords for network elements. Although these community strings are sent in clear-text in the SNMP PDUs, the values can be encrypted in the configuration file.

The `snmp community encrypted name` command enables the encryption of SNMP community strings. For additional information, see the *Global Configuration Mode Commands* chapter in the CLI Reference.
Lawful Intercept Restrictions

This section describes some of the security features associated with the provisioning of Lawful Intercept (LI). For additional information, refer to the Lawful Intercept Configuration Guide.

LI Server Addresses

An external authenticating agent (such as RADIUS or Diameter) sends a list of LI server addresses as part of access-accept. For any intercept that was already installed or will be installed for that subscriber, a security check is performed to match the LI server address with any of the LI-addresses that were received from the authenticating agent. Only those addresses that pass this criteria will get the intercepted information for that subscriber.

While configuring a campon trigger, the user will not be required to enter the destination LI server addresses. When a matching call for that campon trigger is detected, a security check is done with the list received from the authentication agent. The LI-related information is only forwarded if a matching address is found.

When an active-only intercept is configured, if a matching call is found, a security check is made for the LI address received from the authentication agent and the intercept configuration will be rejected.

If no information related to LI server addresses is received for that subscriber, LI server addresses will not be restricted.

**Important:** A maximum of five LI server addresses are supported via an authenticating agent.

Modifying Intercepts

One LI administrator can access and/or modify the intercepts created by another LI administrator. Whenever an intercept is added, removed or modified, an event log is displayed across LI administrators about the change. An SNMP trap is also generated.
Adding, Modifying and Removing Users

It is considered uncommon for a user to be added or removed from the VPC. Likewise, it is considered uncommon for a user's privileges to modified. However, if the system is compromised, it is common for attackers to add or remove a privileged user, raise their privileges or lower the privileges of others.

As a general rule, lower privileged users should not be allowed to increase their privileges or gain access to sensitive data, such as passwords, which were entered by higher privileged users.

**Important:** VPC can only detect changes in users and user attributes, such as privilege level, when these users are configured through VPC.

Notification of Users Being Added or Deleted

Users with low level authorization should not be able to create users with high level authorization. However, if a malicious actor were to be able to create a high level authorized user, they could then delete the other high level authorized users, thereby locking them out of the system.

The following SNMP traps notify an administrator when users are added or removed:
- `starLocalUserAdded` – indicates that a new local user account has been added to the system.
- `starLocalUserRemoved` – indicates that a local user account has been removed from the system.

Notification of Changes in Privilege Levels

Whenever a user's privilege level is increased or decreased, an SNMP notification will be sent out. A malicious actor may gain access to more privileged commands by somehow promoting their privileges. Once this is done, they could then “demote” the privileges of all the other users, thereby locking the proper administrators out of the system.

The `starLocalUserProfileChanged` trap indicates that a local user's privilege level has been changed.

User Access to Operating System Shell

The `starOsShellAccessed` trap indicates that a user has accessed the operating system shell.
Hidden Commands

A Security Administrator can set a plain-text or encrypted password for access to CLI test commands. The password value is stored in /flash along with the boot configuration information. The *show configuration* and *save configuration* commands will *never* output this value.

⚠️ **Caution:** VPC-VSM requires that **cli test-commands** mode be enabled. Use of cli test-commands other than those required to configure SecGW can slow system performance, drop subscribers, and/or render the system inoperable.

Enabling cli test-commands Mode

The Global Configuration mode command *tech-support test-commands [encrypted] password* password sets an encrypted or plain-text password for access to CLI test-commands.

When a test-commands password is enabled, the Global Configuration mode command *cli test-commands [encrypted] password password* requires the entry of the *password* keyword. If the *encrypted* keyword is specified, the *password* argument is interpreted as an encrypted string containing the password value. If the *encrypted* keyword is not specified, the *password* argument is interpreted as the actual plain text value.

⚠️ **Important:** If *tech-support test-commands password* is never configured, **cli-test commands** will always fail. If the *password* keyword is not entered for **cli test-commands**, the user is prompted (no-echo) to enter the password. Also, **cli hidden** must be enabled by a Security Administrator to access the CLI test-commands.

⚠️ **Important:** Low-level diagnostic and test commands/keywords will now be visible to a user with Administrator or higher privilege. There is no visual indication on the CLI that the test-commands mode has been enabled.

Enabling Password for Access to CLI-test commands

The Global Configuration mode command *tech-support test-commands [encrypted] password* password sets an encrypted or plain-text password for access to CLI test-commands.

This command sequence is shown below.

```
[local]host_name# config

[local]host_name(config)# tech-support test-commands [encrypted] password

[local]host_name(config)#
```
Exec Mode cli test-commands

**Important:** The cli hidden command must be enabled by a Security Administrator via Global Configuration mode to access the CLI test-commands form the Exec mode.

Exec mode commands are available to a privileged user who enters the command cli test-commands from Exec mode.

```
[local]host_name# cli test-commands [encrypted] password password
```

Warning: Test commands enables internal testing and debugging commands

USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION

**Important:** An SNMP trap (starTestModeEntered) is generated whenever a user enters CLI test-commands mode.

Configuration mode cli test-commands

Configuration commands which provided access to low-level software parameters are accessible only after a privileged user enters the command cli test-commands from Global Configuration mode.

```
[local]host_name# config
[local]host_name(config)# cli test-commands [encrypted] password password
```

Warning: Test commands enables internal testing and debugging commands

USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION

**Important:** An SNMP trap (starTestModeEntered) is generated whenever a user enters CLI test-commands mode.

List of Exec and Configuration Mode cli test-commands

CLI test-commands are not documented in the CLI Reference or other user documents. Lists of these Exec mode and Configuration mode commands/keywords is published in a separate document available through Cisco TAC. Detailed descriptions of the command/keyword functions are not provided. However, the user can refer to the CLI Help function for additional information.
Chapter 9
StarOS Management Operations

This chapter provides information about software management operations on the VPC. Software management sections include:

- Understanding the Local File System
- Maintaining the Local File System
- Configuring the Boot Stack
- Upgrading StarOS
- Performing Dynamic Software Updates
- Managing License Keys
- Managing Local-User Administrative Accounts
Understanding the Local File System

The local VPC file system is made up of files that are stored on the following:

- **/flash** – Flash memory allocated as vHDD-1 via the hypervisor is the default storage media for the StarOS image, CLI configuration, and crash log files used by the system.
- **/hd-raid** – This is the storage space allocated as vHDD-2 by the hypervisor. It is used to store CDRs (Charging Data Records) and UDRs (Usage Data Records).

File Types Used by the Local File System

The following file types can be located in the local file system:

- **Operating System Software Image File**: This binary file type is identified by its .bin extension. This file is StarOS and is loaded upon startup or reloading. This is an executable, read-only file that cannot be modified by end users.
- **CLI Configuration File**: This file type is identified by its .cfg extension. These are text files that contain CLI commands that work in conjunction with the StarOS image. They determine services to be provided, hardware and software configurations, and other functions performed by the system. The files are typically created by the end user. You can modify the files both on and off-line and use descriptive long filenames.
- **System File**: Only one file identified by a .sys extension is used by StarOS. The boot.sys file contains system-specific information, which describes how the system locates, and in what priority it loads, file groups (paired .bin and .cfg files) from its boot stack.
- **Abridged Crash Log**: The abridged crash log, identified by its crashlog filename, contains summary information about software or hardware failures that occur on the system. This file is located in the /flash/crsh2/ directory on the device. You can view the contents of this file through the CLI, but you cannot modify the file.

Understanding the boot.sys File

StarOS uses the boot.sys file to store the prioritized boot stack parameters and file groups the system uses during startup. Modify this file only through StarOS CLI commands and not through external means. Boot parameters contain information StarOS needs to locate the StarOS image file, including:

- **bootmode**: This setting is typically configured to normal, and identifies how StarOS starts.
- **boot stack information**: The boot stack is made up of prioritized file group entries that designate the StarOS image file and the CLI configuration file to load.

When VPC is started for the first time, the boot.sys file is configured to use the normal boot mode and load the StarOS image from the /flash directory.

There is no CLI configuration file contained on the local file system. This causes StarOS to automatically start its CLI-based Quick Setup Wizard upon the first successful boot. Refer to the Getting Started chapter for more information on using the Quick Setup Wizard.
Maintaining the Local File System

Use StarOS CLI commands to manage and maintain the devices that make up the local file system. Execute all the commands described in this section in the Exec Mode. Unless otherwise specified, you must have security administrator or administrator privileges to execute these commands.

File System Management Commands

Use the commands in this section to manage and organize the local file system.

Important: For complete information on the following commands, see the Exec Mode Commands chapter of the Command Line Interface Reference.

Creating Directories

Use the `mkdir` command to create a new directory on the specified local device. This directory can then be incorporated as part of the path name for any file located in the local file system.

```sh
[local]host_name# mkdir { /flash | /hd-raid } /dir_name
```

Use the following command to create a directory named `configs`:

```sh
[local]host_name# mkdir /flash/configs
```

Renaming Files and Directories

Use the `rename` command to change the name of a file from its original name to a different name. Remember to use the same file extension, if applicable, to ensure that the file type remains unchanged.

```sh
[local]host_name# rename { /flash | /hd-raid } /src_filename { /flash | /hd-raid } /dst_filename [-noconfirm]
```

Use the following command to rename the file `iot_test.cfg` to `iot_accept.cfg` on the /flash local device.

```sh
[local]host_name# rename /flash/iot_test.cfg /flash/iot_accept.cfg -noconfirm
```

Important: Use the `rename` command only within the same local device. You cannot rename a file and place it onto another local device at the same time. To move a renamed file, you must use the `copy` command.

Copying Files

These instructions assume that you are at the root prompt for the Exec mode:

```sh
[local]host_name#
```

To save your current configuration, enter the following command:
Maintaining the Local File System

[local]host_name# copy from_url to_url [ passive ] [ -noconfirm ]

To copy the configuration file system.cfg from the directory cfgfiles to the directory configs_old on /flash, enter the following command:

[local]host_name# copy /flash/cfgfiles/system.cfg /flash/configs_old/system_2011.cfg

To copy the configuration file simple_ip.cfg from the directory host_name_configs to an FTP server with an IP address of 192.168.34.156, on which you have an account with a username administrator and a password secure, use the following command:

[local]host_name# copy /flash/host_name_configs/simple_ip.cfg ftp://administrator:secure@192.168.34.156/host_name_configs/ simple_ip.cfg

To copy a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

[local]host_name# copy /flash/cfgfiles/init_config.cfg tftp://config_server/init_config.cfg

Deleting Files

The delete command removes a designated file from its specified location on the local file system.

**Important:** This command does **not** support wildcard entries; each filename must be specified in its entirety.

**Caution:** Do **not** delete the boot.sys file. If deleted, StarOS will not reboot on command and will be rendered inoperable.

[local]host_name# delete { /flash | /hd-raid }/filename [-noconfirm]

The following command deletes the file test.cfg from the /flash directory.

[local]host_name# delete /flash/test.cfg

Removing Directories

The rmdir command deletes a current directory on the specified local device. This directory can then be incorporated as part of the path name for any file located in the local file system.

**Important:** The directory you want to remove (delete) must be empty before executing the rmdir command. If the directory is not empty, the CLI displays a “Directory not empty” message and will not execute.

[local]host_name# rmdir url /dir_name

The following command deletes the empty directory configs in the /flash directory.
Important: Local devices that have been formatted using other methods such as NTFS or FAT32 may be used to store various StarOS, CLI configuration, and crash log files. However, when installing a new local device via the hypervisor for regular use, you should format the device prior to use. This ensures that the proper file allocation table format is used, preventing any possible discrepancies between other formats used with other operating systems.

Caution: The `filesystem format` command removes all files and information stored on the device.

To format a local device for use by the local file system, enter the following command:

```
[local]host_name# filesystem format { /flash | /hd-raid }
```

Applying Pre-existing CLI Configuration Files

A pre-existing CLI configuration file is any `.cfg` file created to provide utility functions (such as clearing all statistics during testing) or created off-line using a text editor. Pre-existing configuration files stored on the local file system can be applied to a running system at any time.

Caution: If a configuration file is applied to VPC currently running another StarOS CLI configuration, any like contexts, services, ports, IP address pools, or other configured items will be overwritten if the same command exists in the configuration file being applied. You must review the contents of the file being applied and understand the service ramifications if a currently running command is overwritten. Also note that changes will not be saved automatically.

A CLI configuration file, or script containing CLI commands, can be applied to a running system by entering the following command at the Exec mode prompt:

```
[local]host_name# configure url [ verbose ]
```

The following command applies the pre-existing CLI configuration file `clearcmds.cfg` in the `/flash` directory.

```
[local]host_name# configure /flash/clearcmds.cfg
```

Viewing Files on the Local File System

This section describes how to view a variety of files.

Viewing the Contents of a Local Device

The contents, usage information, and file system directory structure of any local device can be viewed by entering the following command at the Exec mode prompt:

```
[local]host_name# rmdir /flash/configs
```
Maintaining the Local File System

Importantly: The USB device must be pre-configuration via the hypervisor for the `usb1` keyword to work.

Viewing CLI Configuration and boot.sys Files

The contents of CLI configuration and boot.sys files, contained on the local file system, can be viewed off-line (without loading them into the OS) by entering the following command at the Exec mode prompt:

```bash
[local]host_name# show file url { /flash | /usb1 | /hd-raid } /filename
```

Where: `url` is the path name for the location of the file and `filename` is the name of the file, including any extension.

Important: The USB device must be pre-configuration via the hypervisor for the `usb1` keyword to work.

Important: Operator and inspector-level users can execute the `show file` command but cannot execute the `directory` command.

Validating an StarOS File

The StarOS image file, identified by its `.bin` extension, is a non-readable, non-editable file that executes on the system, creating its runtime operating system (OS).

It is important to verify a new StarOS image file before attempting to load it. To accomplish this, a proprietary checksum algorithm is used to create checksum values for each portion of the application stored within the `.bin` file during program compilation.

This information can be used to validate the actual file against the checksum values stored within the file during its compilation. If any portion of the image file has become corrupted (for example, the file was truncated or was transferred using ASCII mode instead of binary mode), then this information is reported and the file is deemed unusable.

To validate a StarOS image file, enter the following command at the Exec mode prompt:

```bash
[local]host_name# show version { /flash | /usb1 | /hd-raid } /directory /filename [all]
```

The output of this command displays the following information:

- Version number
- Image Description
- Image Date
- Boot Image

If an invalid file is found, the system displays a failure message similar to these:

```
Failure: Image /flash/image_version.bin CRC check failed!
```
Failure: /flash/image.bin, has a bad magic number
Configuring the Boot Stack

The boot stack consists of a prioritized listing of StarOS image-to-CLI configuration file associations. These associations determine which StarOS image and configuration file gets loaded during StarOS startup or upon a reload or reboot. Though multiple associations can be configured, StarOS uses the association with the highest priority.

In the event that there is an error processing this association (for example, one of the files cannot be located), StarOS attempts to use the association with the next highest priority. Priorities range from 1 to 100, with 1 being the highest priority. The maximum number of boot stack entries that may be configured in the boot.sys file is 10.

Boot stack information is contained in the boot.sys file, described in Understanding the bootsys File. In addition to boot stack entries, the boot.sys file contains any configuration commands required to define the system boot method as explained in the section that follows.

Local-Boot Method

The local-boot method uses the StarOS image and configuration files stored locally. Upon startup or reboot, StarOS looks on /flash or /hd-raid for the specific software image and accompanying configuration text file. When using the local-booting method, you only need to configure boot stack parameters.

Viewing the Current Boot Stack

To view the boot stack entries contained in the boot.sys file run the Exec mode show boot command.

**Important:** Operator and inspector-level users can execute the show boot command.

The example below shows the command output for a local booting configuration. Notice that in this example both the image file (operating system software) and configuration file (CLI commands) are located on the /flash device.

```
boot system priority 10 \\
  image /flash/staros.bin \\
  config /flash/system.cfg
```

To identify the boot image priority that was loaded at the initial boot time enter:

```
[local]host_name# show boot initial-config
```

The example below displays the output:

```
Initial (boot time) configuration:
  image tftp://192.168.1.161/tftpboot/image_filename.bin \\
  config /flash/system.cfg \\
  priority 1
```
Adding a New Boot Stack Entry

**Important:** Before performing this procedure, verify that there are less than 10 entries in the boot.sys file and that a higher priority entry is available (minimally there is no priority 1 entry in the boot stack). For more information, refer to Viewing the Current Boot Stack.

If priority 1 is in use, then you must renumber the existing entry(ies) to ensure that at least that priority is available. The maximum number of boot stack entries that can be contained in the boot.sys file is 10. If there are already 10 entries in the boot stack, you must delete at least one of these entries (typically, the lowest priority) and, if necessary, renumber some or all of the other entries before proceeding. For more information, see Deleting a Boot Stack Entry.

This procedure details how to add new boot stack entries to the boot.sys file. Make sure you are at the Exec mode prompt and enter the following commands:

```
configure
  boot system priority number image image_url config cfg_url
```

**Important:** If the URL is a USB device, the USB port must be pre-configured via the hypervisor for the `usb1` keyword to work.

The following command creates a new boot stack entry, using a boot priority of 3.

```
[local] host_name(config)# boot system priority 3 image /flash/image_filename.bin config /flash/general.cfg
```

**Important:** Boot stack changes saved to the boot.sys file are not executed until StarOS is rebooted.

Deleting a Boot Stack Entry

This procedure details how to remove an individual boot stack entry from the boot.sys file. Make sure you are at the Exec mode prompt and enter the following commands:

```
configure
  no boot system priority number
```

Where `number` specifies the boot priority used for the boot stack entry. This command removes that specific entry from the boot stack, causing the boot.sys file to be overwritten.
Upgrading StarOS

The following information is required prior to performing a StarOS upgrade:

- Current StarOS version
- New StarOS version
- Upgrade method

StarOS Release Version

StarOS can be configured to provide services and perform pre-defined functions through commands issued from the CLI.

The StarOS image is delivered as a single binary file (.bin file extension) and is loaded as a single instance.

Refer to the Release Notes supplied with the StarOS code drop for the binary file name.

Download the StarOS Image from the Support Site

Access to the Cisco support site and download facility is username and password controlled. You must have an active customer account to access the site and download the StarOS image.

Download the software image to a network location from which it can be uploaded to the /flash device.

Contact your Cisco representative or Cisco TAC for additional information.

Transfer the StarOS Image to /flash

Transfer the new operating system image file to the /flash using one of the following methods:

- Copy the file from a network location by entering the following command:

  ```
  [local]host_name# copy from_url to_url [-noconfirm]
  ```

- Transfer the file to the /flash device using an FTP client with access to the system.

  **Important:** Whenever transferring a StarOS image file using the file transfer protocol (FTP), the FTP client must be configured to transfer the file using binary mode. Failure to use binary transfer mode will make the transferred operating system image file unusable.

- Transfer the file to the /flash device using an SFTP client with access to the system.

Verify that the image file was successfully transferred to the /flash device by running the following Exec mode command:

  ```
  [local]host_name# directory /flash
  ```

The image filename should appear in the displayed output.

Run the `show version /flash/image_filename` command to verify the build information.
Saving a Copy of the Current Configuration File

Prior to upgrading to a new StarOS release, you should copy and rename the current configuration file to the /flash device and to an off-chassis location (external memory device or network URL). This renamed copy assures that you will have a fallback, loadable configuration file should a problem be encountered during the upgrade.

Off-line Software Upgrade

An off-line software upgrade can be performed for any VPC, upgrading from any version of StarOS to any other version, regardless of version number. This process is considered off-line because while many of the steps can be performed while the VPC is currently supporting sessions, the last step of this process requires a reload to actually apply the StarOS upgrade.

This procedure assumes that you have a CLI session established and are placing the new StarOS .bin image file onto the local file system. To begin, make sure you are at the Exec mode prompt.

Configure a Newcall Policy

Configure a newcall policy from the Exec mode to meet your service requirements. When enabled the policy redirects or rejects new calls in anticipation of the StarOS reload that completes the upgrade process. This reduces the amount of service disruption to subscribers caused by the system reload that completes the upgrade.

**Important:** Newcall policies are created on a per-service basis. If you have multiple services running on the VPC, you can configure multiple newcall policies.

The general syntax for newcall policies is described below:

\[
[\text{local}]\text{host\_name}\# \text{newcall policy service\_type \{ all | name service\_name \} reject}
\]

Keyword availability varies by service_type. For a complete description of the newcall policy command with all its associated keywords, see the Exec Mode Commands chapter of the Command Line Interface Reference.

Configure a Message of the Day Banner

*Optional:* Configure a “Message of the Day” banner informing other management users that the system will be rebooted by entering the following command from the Global Configuration mode prompt.

\[
[\text{local}]\text{host\_name(config)}\# \text{banner motd “banner\_text”}
\]

*banner_text* is the message that you would like to be displayed and can be up to 2048 alphanumeric characters. Note that *banner_text* must begin with and end in double quotation marks (“ “). For more information in entering CLI banner information, see the CLI Reference. The banner is displayed when an administrative user logs onto the CLI.

Back up the Current CLI Configuration File

Back up the current CLI configuration file by entering the following command:

\[
[\text{local}]\text{host\_name}\# \text{show version /flash/image\_filename.bin}
\]
Upgrading StarOS

[local]host_name# copy from_url to_url [-noconfirm]

This creates a mirror-image of the CLI configuration file linked to the operating system defined in the current boot stack entry.

The following command example creates a backup copy of the file general.cfg located on the /flash device to the file general_3652.cfg:

[local]host_name# copy /flash/general.cfg /flash/general_3652.cfg

Create a New Boot Stack Entry

Create a new boot stack entry for the new file group, consisting of the new operating system image file and the currently used CLI configuration file by entering the following Global Configuration command:

[local]host_name(config)# boot system priority number image image_url
 /flash/filename config cfg_url /flash/filename

Assign the next highest priority to this entry, by using the N-1 method, wherein you assign a priority number that is one number less than your current highest priority.

Important: Run the Exec mode show boot command to verify that there are less than 10 entries in the boot.sys file and that a higher priority entry is available (minimally there is no priority 1 entry in the boot stack).

If priority 1 is in use, you must renumber the existing entries to ensure that at least that priority is available.

The maximum number of boot stack entries that can be contained in the boot.sys file is 10. If there are already 10 entries in the boot stack, you must delete at least one of these entries (typically, the lowest priority) and, if necessary, renumber some or all of the other entries before proceeding. Use the no boot system priority command to delete a book stack entry.

[local]host_name# configure

[local]host_name(config)# no boot system priority number

To add new boot stack entries to the boot.sys file enter the following commands:

[local]host_name# configure

[local]host_name(config)# boot system priority number image image_url config
cfg_url

For information on using the boot system priority command, refer to Adding a New Boot Stack Entry.

Save the Running Configuration

Save the currently running, upgraded configuration prior to rebooting StarOS.

To save the running configuration to the current configuration file:

[local]host_name# save configuration /flash
Reboot StarOS

Reboot StarOS by entering the following command:

```
[local]host_name# reload [-noconfirm]
```

As StarOS reboots, it loads the new StarOS image and its corresponding CLI configuration file using the new boot stack entry configured earlier.

After the reboot is completed, establish a CLI session and enter the `show version` command to verify that the active software version is correct.

Verify the Running Software Version

After StarOS has successfully booted, verify that the new StarOS version is running by executing the Exec mode `show version` command.

```
[local]host_name# show version
```

Restoring the Previous Software Image

If for some reason you need to undo the upgrade, perform the upgrade again except:

- Specify the locations of the upgrade software image and configuration files.
  then
- Specify the locations of the original software image and configuration files.

Upgrading ICSR

The procedure for upgrading primary and backup ICSR instances is described in the `Interchassis Session Recovery` chapter. Essentially the procedure requires upgrading the primary and standby VPCs using the off-line method while each is in standby mode.
Performing Dynamic Software Updates

StarOS allows the runtime loading of plugins. All StarOS builds include a “default” baseline plugin.

This feature is currently used to dynamically update the detection logic used to filter P2P applications via the Application Detection and Control (ADC) feature.

Patching is the process used to install a plugin as an incremental update to a StarOS release. One plugin can be provided to multiple, compatible, concurrent product releases. A plugin is distributed in the form of a compressed distribution kit via the internet or by other means (USB stick, CD, etc.).

A plugin is a functional software entity that provides incremental updates to a pre-existing StarOS software component. Plugins have the characteristic of being dynamically loadable at runtime and do not require a system restart. A plugin has a name and one or more versions. All plugin names are known to the system at product release.

For complete information on the Dynamic Software Update process, refer to the ADC Administration Guide.
Managing License Keys

License keys define capacity limits (number of allowed subscriber sessions) and available features on VPC. Adding new license keys allows you to increase capacity and add new features as your subscriber base grows.

New System License Keys

New StarOS images are delivered with no license keys installed. In most cases, you receive the license key in electronic format (usually through e-mail).

When StarOS boots with no license key installed, a default set of restricted session use and feature licenses is installed. The following Exec Mode command lists the license information:

```
[local]host_name# show license information
```

Session Use and Feature Use Licenses

Session use and feature use licenses are software mechanisms that provide session limit controls and enable special features within StarOS. These electronic licenses are stored in the StarOS configuration file that is loaded each time VPC is initialized or restarted.

- Session use licenses limit the number of concurrent sessions that a VPC is capable of supporting per service type and are acquired on an as-needed basis. This allows carriers to pay only for what they are using and easily increase capacity as their subscriber base grows.

- Feature use licenses enable specific features/functionality within StarOS and are distributed based on the total number of sessions supported by VPC.

Installing New License Keys

Use the instructions below to install a new license key.

Cutting and Pasting the Key

If you have a copy of the license, use the following configuration to cut and paste just the license key part:

**Step 1** From the Exec mode, enter the following:

```
configure
license key license
exit
```

*license* is the license key string. The license can be an alphanumeric string of 1 through 1023 characters that is case sensitive. Copy the license key as shown in the example below, including the "\" (double-quote slash). Please note: this is not a functional license.

"\"
Managing License Keys

Step 2 Verify that the license key just entered was accepted by entering the following command at the Exec mode prompt:

```
show license key
```

The new license key should be displayed. If it is not, return to the Global configuration mode and re-enter the key using the license key command.

Step 3 Verify that the license key enabled the correct functionality by entering the following command:

```
[local] host_name# show license information
```

All license keys and the new session capacity or functionality enabled should be listed. If the functionality or session capacity enabled by the new key is incorrect, please contact your service representative.

Step 4 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

---

**Caution:** Failure to save the new license key configuration in the current CLI configuration file will result in the loss of any of the new features enabled by the license key once the system is reloaded.

Adding License Keys to Configuration Files

License keys can be added to a new or existing configuration file.

1. **Open the configuration file to which the new license key commands are to be copied.**

2. **Copy the license as shown in the example, including the “\” (double-quote slash). Please note: this is not a functional license.**

```
""

VER=1|C1M=000-0000-00|C1S=03290231803|C2M=11-1111-11-
1|C2S=\STCB21M82003R80411A4|DO1=00000000000|DOE=00000000|ISS=1|NUM=13459|0000000000
0000|LSF=000000|LSH=000000|LSG=500000|LSL=500000\|FIS=Y|FR4=Y|FPF=Y|FCS=Y|FTC=Y|F
MG=Y|FCR=Y|FSR=Y|FPM=Y|FID=Y|SIG=MCwCF\Esng6Bsx/XdmyfLe7rHcD4sVP2bzAhQ3iEHDoyyd638
8jHsHD99sg36SG267gshssja77

end
```

3. **Paste the license key into the configuration**
Important: Paste the license key information at the beginning of the configuration file to ensure the system has the expected capacity and features before it configures contexts.

Step 4  Save your configuration as described in the Verifying and Saving Your Configuration chapter.

License Expiration Behavior

When a license expires, there is a built-in grace period of 30 days that allows normal use of the licensed session use and feature use licenses. This allows you to obtain a new license without any interruption of service.

The following Exec mode command lists the license information including the date the grace period is set to expire:

```
[local]host_name# show license information
```

Requesting License Keys

License keys for the system can be obtained through your Cisco account representative. Specific information is required before a license key may be generated:

- Sales Order or Purchase Order information
- Desired session capacity
- Desired functionality

Viewing License Information

To see the license detail, enter the following command from the Exec mode:

```
[local]host_name# show license information [ full | key [ full ] ]
```

Deleting a License Key

Use the procedure below to delete the session and feature use license key from a configuration. You must be a security administrator or administrator.

```
configure

no license key

exit

[local]host_name# show license key
```

The output of this command should display: “No license key installed”.
Managing Local-User Administrative Accounts

Unlike context-level administrative accounts which are configured via a configuration file, information for local-user administrative accounts is maintained in a separate file in flash memory and managed through the software’s Shared Configuration Task (SCT). Because local-user accounts were designed to be compliant with ANSI T1.276-2003, the system provides a number of mechanisms for managing these types of administrative user accounts.

Configuring Local-User Password Properties

Local-user account password properties are configured globally and apply to all local-user accounts. The system supports the configuration of the following password properties:

- **Complexity**: Password complexity can be forced to be compliant with ANSI T1.276-2003.
- **History length**: How many previous password versions should be tracked by the system.
- **Maximum age**: How long a user can use the same password.
- **Minimum number of characters to change**: How many characters must be changed in the password during a reset.
- **Minimum change interval**: How often a user can change their password.
- **Minimum length**: The minimum number of characters a valid password must contain.

Refer to the `local-user password` command in *Global Configuration Mode Commands* in the Command Line Interface Reference for details on each of the above parameters.

Configuring Local-User Account Management Properties

Local-user account management includes configuring account lockouts and user suspensions.

Local-User Account Lockouts

Local-user accounts can be administratively locked for the following reasons:

- **Login failures**: The configured maximum login failure threshold has been reached. Refer to the `local-user max-failed-logins` command in *Global Configuration Mode Commands* in the Command Line Interface Reference for details.

- **Password Aging**: The configured maximum password age has been reached. Refer to the `local-user password` command in *Global Configuration Mode Commands* in the Command Line Interface Reference for details.

Accounts that are locked out are inaccessible to the user until either the configured lockout time is reached (refer to the `local-user lockout-time` command in *Global Configuration Mode Commands* in the Command Line Interface Reference) or a security administrator clears the lockout (refer to the `clear local-user` command in *Exec Mode Commands* in the Command Line Interface Reference).

**Important**: Local-user administrative user accounts could be configured to enforce or reject lockouts. Refer to the `local-user username` command in *Global Configuration Mode Commands* in the Command Line Interface Reference for details.
Local-User Account Suspensions

Local-user accounts can be suspended as follows:

```
configure

suspend local-user name
```

A suspension can be removed by entering:

```
configure

no suspend local-user name
```

Changing Local-User Passwords

Local-user administrative users can change their passwords using the `password change` command in the Exec mode. Users are prompted to enter their current and new passwords.

Security administrators can reset passwords for local-users by entering the following command from the root prompt in the Exec mode:

```
[local]host_name# password change username name
```

`name` is the name of the local-user account for which the password is to be changed. When a security administrator resets a local-user’s password, the system prompts the user to change their password the next time they login.

All new passwords must adhere to the password properties configured for the system.
Chapter 10
Monitoring VPC

This chapter provides information for monitoring VPC status and performance using the `show` commands found in the StarOS Command Line Interface (CLI). These command and their keywords provide useful information on all aspects of VPC ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter provides the most useful and in-depth information for monitoring the system. For additional information on these and other `show` command keywords, refer to *Exec Mode show Commands* in the *Command Line Interface Reference*.

This chapter includes the following sections:

- StarOS SNMP Notifications
- Monitoring VPC Status and Performance
- Clearing Statistics and Counters

**Important:** VPC has no knowledge of the hypervisor under which it is running or the commercial off-the-shelf (COTS) server. To monitor the status of the hypervisor and COTS server, refer to the user documentation supplied with these components of this system.
StarOS SNMP Notifications

In addition to the CLI, StarOS supports Simple Network Management Protocol (SNMP) notifications that indicate status and alarm conditions.

Use the `show snmp server` command to display the list of supported Management Information Bases (MIBs). Enable support for a MIB via the Global Configuration mode `snmp mib` command. By default only the STARENT-MIB is enabled.

**Important:** STARENT-MIB OIDs specific to card events will generally not apply. Hardware specific items will also not apply (such as, temperature and fans).

Refer to the *SNMP MIB Reference* for a detailed listing of these notifications.

For complete descriptions of SNMP-related commands, refer to the *Exec Mode show Commands* and *Global Configuration Mode Commands* chapters of the *Command Line Interface Reference*. 
Monitoring VPC Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components within VPC. Output descriptions for most of the commands are located in the Statistics and Counters Reference.

Table 4. Status and Performance Monitoring Commands

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Administrative Information</td>
<td></td>
</tr>
<tr>
<td>View a list of all administrative users currently logged on the system</td>
<td>show administrators</td>
</tr>
<tr>
<td>View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number</td>
<td>show administrators session id</td>
</tr>
<tr>
<td>View information pertaining to local-user administrative accounts configured for the system</td>
<td>show local-user verbose</td>
</tr>
<tr>
<td>View statistics for local-user administrative accounts</td>
<td>show local-user statistics verbose</td>
</tr>
<tr>
<td>View information pertaining to your CLI session</td>
<td>show cli</td>
</tr>
<tr>
<td>Determining System Uptime</td>
<td></td>
</tr>
<tr>
<td>View system uptime (time since last reboot)</td>
<td>show system uptime</td>
</tr>
<tr>
<td>View NTP Server Status</td>
<td></td>
</tr>
<tr>
<td>View NTP servers status</td>
<td>show ntp status</td>
</tr>
<tr>
<td>View System Resources</td>
<td></td>
</tr>
<tr>
<td>View all system resources such as CPU resources and number of managers created</td>
<td>show resources [ cpu ]</td>
</tr>
<tr>
<td>View System Alarms</td>
<td></td>
</tr>
<tr>
<td>View information about all currently outstanding alarms</td>
<td>show alarm outstanding all verbose</td>
</tr>
<tr>
<td>View system alarm statistics</td>
<td>show alarm statistics</td>
</tr>
<tr>
<td>View Congestion-Control Statistics</td>
<td></td>
</tr>
<tr>
<td>View Congestion-Control Statistics</td>
<td>show congestion-control statistics</td>
</tr>
<tr>
<td>View Remote Management Statistics</td>
<td></td>
</tr>
<tr>
<td>View SNMP notification statistics</td>
<td>show snmp notifies</td>
</tr>
<tr>
<td>View SNMP access statistics</td>
<td>show snmp accesses</td>
</tr>
<tr>
<td>View SNMP trap history</td>
<td>show snmp trap history</td>
</tr>
<tr>
<td>View SNMP Trap Statistics</td>
<td>show snmp trap statistics</td>
</tr>
</tbody>
</table>
## Monitoring VPC Status and Performance

To do this: | Enter this command:
---|---
View System Information and Network Interfaces | show hardware
View information about system components, storage devices and network interfaces | show hardware

View Card Information and Statistics | show card diag
View card-level diagnostics (slot 1 only) | show card diag
View information about the virtual card in slot 1 | show card info
View card operating status for slot 1. | show card table

View Port Information and Counters | show port table
View information about a specific port | show port datalink counters 1/port#
View NPU counters for a specific port | show port npu counters 1/port#
View administrative and operating status of all ports | show port table
View per port utilization in Mbps | show port utilization table

---

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s). Some commands have different outputs depending on the platform type.
Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping.

Statistics and counters can be cleared using the CLI `clear` command. Refer to *Exec Mode Commands* in the *Command Line Interface Reference* for detailed information on using this command.
Chapter 11
Bulk Statistics

This chapter provides configuration information for:

- Configuring Communication with the Collection Server
- Viewing Collected Bulk Statistics Data
- Manually Gathering and Transferring Bulk Statistics
- Clearing Bulk Statistics Counters and Information
- Bulk Statistics Event Log Messages
Configuring Communication with the Collection Server

Two configuration methods are available for defining how bulk statistics are collected and managed. A “standard” configuration allows the system to automatically assign a number to the bulk statistics file. Optionally, a number can be specified by an administrator in the optional configuration method. Command details and descriptions of keywords and variables for commands in this chapter are located in the Bulk Statistics Configuration Mode Commands and Bulk Statistics File Configuration Mode Commands chapters in the Command Line Interface Reference.

Configuring Standard Settings

The configuration example in this section defines basic operation of the bulk statistics feature. Use the following example configuration to set up the system to communicate with the statistic collection server:

```
configure
  bulkstats mode
    schema name format format_string
    sample-interval time_interval
    transfer-interval xmit_time_interval
    limit mem_limit
  exit
  bulkstats collection
end
```

Configuring Optional Settings

This section describes optional commands that can be used within the Bulk Statistics Configuration mode. Specifically, bulk statistic “files” under which to group the bulk statistic configuration are configured using commands in this section. “Files” are used to group bulk statistic schema, delivery options, and receiver configuration. Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers.

```
configure
  bulkstats mode
    file number
      receiver ip_address { primary | secondary } [ mechanism { { ftp | sftp
      } login user_name [ encrypted ] password pwd } | tftp } ] ]
      receiver mode { redundant | secondary-on-failure }
```
Configuring Bulk Statistic Schemas

In each configuration example described in Configuring Standard Settings and Configuring Optional Settings, the following is the primary command used to configure the type of schema and the statistics collected:

```
name schema format format_string
```

Refer to the Bulk Statistics Configuration Mode Commands and Bulk Statistics File Configuration Mode Commands chapters in the Command Line Interface Reference for more information regarding supported schemas, available statistics, and proper command syntax.

Verifying Your Configuration

After configuring support for bulk statistics on the system, you can check your settings prior to saving them. Follow the instructions in this section to verify your bulk statistic settings. These instructions assume that you are at the root prompt for the Exec mode.

Check your collection server communication and schema settings by entering the following command:

```
show bulkstats schemas
```

The following is an example command output:

```
Bulk Statistics Server Configuration:
Server State: Enabled
File Limit: 6000 KB
Sample Interval: 15 minutes (0D 0H 15M)
```
Transfer Interval: 480 minutes (0D 0H 15M)
Collection Mode: Cumulative
Receiver Mode: Secondary-on-failure
Local File Storage: None

Bulk Statistics Server Statistics:
Records awaiting transmission: 114
Bytes awaiting transmission: 8092
Total records collected: 59926
Total bytes collected: 4190178
Total records transmitted: 59812
Total bytes transmitted: 4188512
Total records discarded: 0
Total bytes discarded: 0
Last collection time required: 2 second(s)
Last transfer time required: 0 second(s)
Last successful transfer: Wednesday December 7 12:14:30 EDT 2011
Last successful tx recs: 190
Last successful tx bytes: 13507
Last attempted transfer: Wednesday December 7 12:14:30 EDT 2011

File 1
Remote File Format: /users/ems/server/data/chicago/bulkstat%date%%time%.txt
File Header: "CHI_test %time%"
File Footer: 

Bulkstats Receivers:
Primary: 192.168.0.100 using FTP with username administrator
Records awaiting transmission: 0
Bytes awaiting transmission: 0
Total records collected: 0
Total bytes collected: 0
Total records transmitted: 0
Total bytes transmitted: 0
Total records discarded: 0
Total bytes discarded: 0
Last transfer time required: 0 second(s)
No successful data transfers
No attempted data transfers

File 2 not configured

File 3 not configured

File 4 not configured

**Saving Your Configuration**

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.
Viewing Collected Bulk Statistics Data

The system provides a mechanism for viewing data that has been collected but has not been transferred. This data is referred to as “pending data”.

View pending bulk statistics data per schema by entering the following:

```
show bulkstats data
```

The above command also shows the statistics of remote files, if configured as described in Configuring Optional Settings.

The following is a sample output:

```
Bulk Statistics Server Statistics:
  Records awaiting transmission: 1800
  Bytes awaiting transmission: 163687
  Total records collected: 1800
  Total bytes collected: 163687
  Total records transmitted: 0
  Total bytes transmitted: 0
  Total records discarded: 0
  Total bytes discarded: 0
  Last collection time required: 2 second(s)
  Last transfer time required: 0 second(s)
  No successful data transfers
  Last attempted transfer: Monday February 14 15:12:30 EST 2011

File 1
  Remote File Format: %date%%time%
  File Header: "Format 4.5.3.0"
  File Footer: ""
  Bulkstats Receivers:
    Primary: 192.168.1.200 using FTP with username root

File Statistics:
```
Records awaiting transmission: 1800
Bytes awaiting transmission: 163687
Total records collected: 1800
Total bytes collected: 163687
Total records transmitted: 0
Total bytes transmitted: 0
Total records discarded: 0
Total bytes discarded: 0
Last transfer time required: 0 second(s)
No successful data transfers
Last attempted transfer: Monday February 14 15:12:30 EST 2011

File 2 not configured

File 3 not configured

File 4 not configured
Manually Gathering and Transferring Bulk Statistics

There may be times where it is necessary to gather and transfer bulk statistics outside of the scheduled intervals. The system provides commands that allow you to manually initiate the gathering and transferring of bulk statistics. These commands are issued from the Exec mode.

To manually initiate the gathering of bulk statistics outside of the configured sampling interval, enter the following command:

```
bulkstats force gather
```

To manually initiate the transferring of bulk statistics prior to reaching the maximum configured storage limit, enter the following command:

```
bulkstats force transfer
```
Clearing Bulk Statistics Counters and Information

It may be necessary to periodically clear counters pertaining to bulk statistics in order to gather new information or to remove bulk statistics information that has already been collected. The following command can be used to perform either of these functions:

`clear bulkstats { counters | data }

The `clear bulkstats data` command clears any accumulated data that has not been transferred. This includes any "completed" files that have not been successfully transferred.
Bulk Statistics Event Log Messages

The stat logging facility captures several events that can be useful for diagnosing errors that could occur with either the creation or writing of a bulk statistic data set to a particular location.

The following table displays information pertaining to these events.

Table 5. Logging Events Pertaining to Bulk Statistics

<table>
<thead>
<tr>
<th>Event</th>
<th>Event ID</th>
<th>Severity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local File Open Error</td>
<td>31002</td>
<td>Warning</td>
<td>&quot;Unable to open local file filename for storing bulkstats data&quot;</td>
</tr>
<tr>
<td>Receiver Open Error</td>
<td>31018</td>
<td>Warning</td>
<td>&quot;Unable to open url filename for storing bulkstats data&quot;</td>
</tr>
<tr>
<td>Receiver Write Error</td>
<td>31019</td>
<td>Warning</td>
<td>&quot;Unable to write to url filename while storing bulkstats data&quot;</td>
</tr>
<tr>
<td>Receiver Close Error</td>
<td>31020</td>
<td>Warning</td>
<td>&quot;Unable to close url filename while storing bulkstats data&quot;</td>
</tr>
</tbody>
</table>
This chapter describes how to configure parameters related to the various types of logging and how to viewing their content. It includes the following sections:

- Configuring Event Logging Parameters
- Configuring Active Logs
- Specifying Facilities
- Configuring Trace Logging
- Configuring Monitor Logs
- Viewing Logging Configuration and Statistics
- Viewing Event Logs Using the CLI
- Configuring and Viewing Crash Logs
- Saving Log Files
- Event ID Overview
System Log Types

There are five types of logs that can be configured and viewed on the system:

- **Event**: Event logging can be used to determine system status and capture important information pertaining to protocols and tasks in use by the system. This is a global function that will be applied to all contexts, sessions, and processes.

- **Active**: Active logs are operator configurable on a CLI instance-by-CLI instance basis. Active logs configured by an administrative user in one CLI instance cannot be viewed by an administrative user in a different CLI instance. Each active log can be configured with filter and display properties that are independent of those configured globally for the system. Active logs are displayed in real time as events are generated.

- **Trace**: Trace logging can be used to quickly isolate issues that may arise for a particular connected subscriber session. Traces can be taken for a specific call identification (callid) number, IP address, mobile station identification (MSID) number, or username.

- **Monitor**: Monitor logging records all activity associated with a particular session. This functionality is available in order to comply with law enforcement agency requirements for monitoring capabilities of particular subscribers. Monitors can be performed based on a subscriber’s MSID or username.

- **Crash**: Crash logging stores useful information pertaining to system software crashes. This information is useful in determining the cause of the crash.

---

**Important**: Not all Event Logs can be configured on all products. Configurability depends on the hardware platform and licenses in use.
Configuring Event Logging Parameters

The system can be configured to generate logs based on user-defined filters. The filters specify the facilities (system tasks or protocols) that the system is to monitor and severity levels at which to trigger the generation of the event entries.

Event logs are stored in system memory and can be viewed via the CLI. There are two memory buffers that store event logging information. The first buffer stores the active log information. The second buffer stores inactive logging information. The inactive buffer is used as a temporary repository to allow you to view logs without having data be overwritten. Logs are copied to the inactive buffer only through manual intervention.

Each buffer can store up to 50,000 events. Once these buffers reach their capacity, the oldest information is removed to make room for the newest.

To prevent the loss of log data, the system can be configured to transmit logs to a syslog server over a network interface.

**Important:** For releases after 15.0 MR4, TACACS+ accounting (CLI event logging) will not be generated for Lawful Intercept users (priv-level 15 and 13).

Configuring Event Log Filters

Follow the example below to configure run time event logging parameters for the system:

```shell
configure

logging filter runtime facility facility level report_level

logging display { event-verbosity | pdu-data | pdu-verbosity }

end
```

Notes:

- Configure the logging filter that determines which system facilities should be logged and at what levels. For detailed information, see Specifying Facilities and Event Severities.
- Repeat for every facility that you would like to log.
- Optional: Configure event ID restrictions by adding the `logging disable eventid` command. The system provides the ability to restrict the sending of a specific event ID or a range of event IDs to minimize the amount of data logged to that which is most useful. Repeat to disable logging for additional event IDs or event ID ranges.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.

Configuring syslog Servers

Information generated by the run time event logging filters can be transmitted to a syslog server for permanent storage.

**Important:** The data transmitted to the syslog server is meant to be used for informational purposes. Functions such as billing and performance monitoring should not be based on syslogs.
**Important:** Although the system provides the flexibility to configure syslog servers on a context-by-context basis, it is recommended that all servers be configured in the local context in order to isolate the log traffic from the network traffic.

Use the following example to configure syslog servers:

```
configure
  context local
  logging syslog ip_address
end
```

Notes:

- `ip_address` specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- A number of keyword options/variables are available for the `logging syslog` command. Refer to the Context Configuration Mode Commands chapter in the Command Line Interface Reference for more information.

- Repeat as needed to configure additional syslog servers. There is no limit to the number of syslog servers that can be configured.

Save the configuration as described in the Verifying and Saving Your Configuration chapter.
Configuring Active Logs

Active logs are event logs that are operator configurable on a CLI instance-by-CLI instance basis. Active logs configured by an administrative user in one CLI instance are not displayed to an administrative user in a different CLI instance. Each active log can be configured with filter and display properties that are independent of those configured globally for the system. Active logs are displayed in real time as they are generated.

Active logs are not written to the active memory buffer by default. To write active logs to the active memory buffer execute the following command in the Global Configuration mode:

```
[local]host_name(config)# logging runtime buffer store all-events
```

When active logs are written to the active memory buffer, they are available to all users in all CLI instances.

Use the following example to configure active logging in Global Configuration mode:

```
[local]host_name(config)# logging filter runtime facility facility level report_level
```

Notes:

- Configure the logging filter that determines which system facilities should be logged and at what levels. For detailed information, see Specifying Facilities and Event Severities.

- Repeat for every facility that you would like to log.

- Optional: Configure event ID restrictions by adding the logging disable eventid command. The system provides the ability to restrict the sending of a specific event ID or a range of event IDs to minimize the amount of data logged to that which is most useful. Repeat to disable logging for additional event IDs or event ID ranges.

- A number of keyword options/variables are available for the Exec mode logging active command. Refer to the Exec Mode Commands chapter in the Command Line Interface Reference for more information.

Once all of the necessary information has been gathered, the Active log display can be stopped by entering the following command in the Exec mode:

```
no logging active
```
Specifying Facilities

**Important:** The actual facilities available for logging vary by platform type, StarOS version and installed product licenses.

The following facilities can be configured for logging event data:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- cli: Command Line Interface (CLI) logging facility
- cmp: Certificate Management Protocol (IPSec) logging facility
- connectedapps: SecGW ASR 9000 oneP communication protocol
- connproxy: Controller Proxy logging facility
- credit-control: Credit Control (CC) facility
- cscf: IMS/MMD Call Session Control Function (CSCF)
- cscfcpmgr: CSCFCPMGR logging facility
- cscfmgr: SIP CSCF Manager facility
- cscfnpdb: CSCF Number Portability Database (NPDB) logging facility
- cscfrrtp: IMS/MMD CSCF RTCP log facility
- cscfrtp: IMS/MMD CSCF RTP log facility
- cscfttmgr: SIP CSCF Tunnel and Transport Manager facility
- csp: Card/Slot/Port controller facility
- css: Content Service Selection (CSS) facility
- css-sig: CSS RADIUS Signaling facility
- cx-diameter: Cx Diameter Messages facility [CSCF <--> HSS]
- data-mgr: Data Manager Framework logging facility
- dcardctrl: IPSec Daughter Card Controller logging facility
- dcardmgr: IPSec Daughter Card Manager logging facility
- demuxmgr: Demux Manager API facility
- dgmbmgr: Diameter Gmb Application Manager logging facility
- dhcp: Dynamic Host Configuration Protocol (DHCP) logging facility
- dhcpv6: DHCPv6
- dhost: Distributed Host logging facility
- diabase: Diabase messages facility
- diactrl: Diameter Controller proclet logging facility
- diameter: Diameter endpoint logging facility
- diameter acct: Diameter Accounting
- diameter-auth: Diameter Authentication
- diameter-dns: Diameter DNS subsystem
- diameter-ees: ACS Diameter signaling facility
- diameter-engine: Diameter version2 engine logging facility
- diameter-hdd: Diameter Horizontal Directional Drilling (HDD) Interface facility
- diameter-svc: Diameter Service
- diamproxy: DiamProxy logging facility
- dpath: IPSec Data Path facility
- drvctrl: Driver Controller facility
Specify Facilities

- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtp**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **embms**: evolved Multimedia Broadcast Multicast Services Gateway facility
- **egtpu**: eGTP-U logging facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**: For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility
- **henbgw**: HENB-GW facility
- **henbgw-pws**: HENB-GW Public Warning System logging facility
- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
- **henbgw-sctp-nw**: HENBGW network SCTP facility
- **henbgwdemux**: HENB-GW Demux facility
- **henbgwmg**: HENB-GW Manager facility
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNB-GW Demux Manager logging facility
- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authoriztn**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ips**: IP Service Gateway interface logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Precool (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
Specifying Facilities

- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-driv**: NPUMGR DRIV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rrri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppeo**: PPP over Ethernet logging facility
- **proclet-map-frwk**: Proclet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBC protocol logging facility
- **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: Session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipse**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacsplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **tectrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **user tcp-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• **vmgctrl**: Virtual Media Gateway (VMG) controller facility
• **vmgctrl**: VMG Content Manager facility
• **vpn**: Virtual Private Network logging facility
• **wimax-data**: WiMAX DATA
• **wimax-r6**: WiMAX R6
• **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
• **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
• **x2gw-demux**: X2GW demux task logging facility
Configuring Trace Logging

Trace logging is useful for quickly resolving issues for specific sessions that are currently active. They are temporary filters that are generated based on a qualifier that is independent of the global event log filter configured using the `logging filter` command in the Exec mode. Like event logs, however, the information generated by the logs is stored in the active memory buffer.

All debug level events associated with the selected call are stored.

**Important:** Trace logs impact session processing. They should be implemented for debug purposes only.

Use the following example to configure trace logs in the Exec mode:

```
[local]host_name#logging trace { callid call_id | ipaddr ip_address | msid ms_id | username username }
```

Once all of the necessary information has been gathered, the trace log can be deleted by entering the following command:

```
[local]host_name#no logging trace { callid call_id | ipaddr ip_address | msid ms_id | username username }
```
Configuring Monitor Logs

Monitor logging records all activity associated with all of a particular subscriber’s sessions. This functionality is available in compliance with law enforcement agency requirements for monitoring capabilities of particular subscribers.

Monitors can be performed based on a subscriber’s MSID or username, and are only intended to be used for finite periods of time as dictated by the law enforcement agency. Therefore, they should be terminated immediately after the required monitoring period.

This section provides instructions for enabling and disabling monitor logs.

Enabling Monitor Logs

Use the following example to configure monitor log targets:

```
configure

logging monitor { ip_addr | IPv6_addr | msid id | username name }

end
```

Repeat to configure additional monitor log targets.

Disabling Monitor Logs

Use the following example to disable monitor logs:

```
configure

no logging monitor { ip_addr | IPv6_addr | msid id | username name }

end
```
Viewing Logging Configuration and Statistics

Logging configuration and statistics can be verified by entering the following command from the Exec mode:

```
[local]host_name# show logging [ active | verbose ]
```

When no keyword is specified, the global filter configuration is displayed as well as information about any other type of logging that is enabled.

The following table provides information and descriptions of the statistics that are displayed when the `verbose` keyword is used.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Logging Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Total events received</td>
<td>Displays the total number of events generated by the system.</td>
</tr>
<tr>
<td>Number of applications</td>
<td>Displays the number of applications receiving the events.</td>
</tr>
<tr>
<td>receiving events</td>
<td></td>
</tr>
<tr>
<td><strong>Logging Source Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Event sequence ids by</td>
<td>Displays a list of system processes that have generated events and the</td>
</tr>
<tr>
<td>process</td>
<td>reference identification number of the event that was generated.</td>
</tr>
<tr>
<td>Msg backlog stat with total</td>
<td>Displays the number of event messages that have been back logged in</td>
</tr>
<tr>
<td>cnt</td>
<td>comparison to the total number of events generated.</td>
</tr>
<tr>
<td>LS L2 filter drop rate</td>
<td>Displays the percentage of logging source (LS) layer 2 (L2) event drops.</td>
</tr>
<tr>
<td>Abnormal Log Source Statistics</td>
<td>Displays abnormal logging source (LS) statistics, if any.</td>
</tr>
<tr>
<td><strong>Runtime Logging Buffer Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Active buffer</td>
<td>Displays the number of events currently logged in the active memory buffer as</td>
</tr>
<tr>
<td></td>
<td>well as a date/time timestamp for the oldest and most recent entries in the</td>
</tr>
<tr>
<td></td>
<td>buffer.</td>
</tr>
<tr>
<td>Inactive buffer</td>
<td>Displays the number of events currently logged in the inactive memory buffer.</td>
</tr>
</tbody>
</table>

---

**Table 6. Logging Configuration and Statistics Commands**
Viewing Event Logs Using the CLI

Event logs generated by the system can be viewed in one of the following ways:

- **From the syslog server:** If the system is configured to send logs to a syslog server, the logs can be viewed directly on the syslog server.
- **From the system CLI:** Logs stored in the system memory buffers can be viewed directly from the CLI.
- **From the console port:** By default, the system automatically displays events over the console interface to a terminal provided that there is no CLI session active.

This section provides instructions for viewing event logs using the CLI. These instructions assume that you are at the root prompt for the Exec mode.

**Step 1**
Copy the active log memory buffer to the inactive log memory buffer.

When the active log memory buffer is copied to the inactive log memory buffer, existing information in the inactive log memory buffer is deleted.

Both active and inactive event log memory buffers can be viewed using the CLI in Exec mode. However, it is preferable to view the inactive log in order to prevent any data from being over-written. The information from the active log buffer can be copied to the inactive log buffer by entering the following command:

```
[local]host_name# logs checkpoint
```

**Step 2**
View the logs by entering the following command:

```
[local]host_name# show logs
```

**Important:** A number of optional keywords/variables are available for the `show logs` command. Refer to the *Exec Mode Show Commands* chapter in the *Command Line Interface Reference* for more information.
Configuring and Viewing Crash Logs

In the unlikely even of a software crash, the system stores information that could be useful in determining the reason for the crash. This information can be maintained in system memory or it can be transferred and stored on a network server.

The system supports the generation of the following two types of logs:

- **Crash log**: Crash logs record all possible information pertaining to a software crash (full core dump). Due to their size, they can not be stored in system memory. Therefore, these logs are only generated if the system is configured with a Universal Resource Locator (URL) pointing to a local device or a network server where the log can be stored.

- **Abridged crash log**: Crash event records are automatically generated when a software crash occurs and are stored in flash memory on management cards. The abridged crash log contains a list crash event records along with associated dump files. This log allows you to view event records and dump files via CLI commands.

Crash Logging Architecture

The crash log is a persistent repository of crash event information. Each event is numbered and contains text associated with a CPU (minicore), NPU or kernel crash. The logged events are recorded into fixed length records and stored in /flash/crashlog2.

Whenever a crash occurs, the following crash information is stored:

1. The event record is stored in /flash/crashlog2 file (the crash log).
2. The associated minicore, NPU or kernel dump file is stored in the /flash/crsh2 directory.
3. A full core dump is stored in a user configured directory.

**Important**: The crashlog2 file along with associated minicore, NPU and kernel dumps are automatically synchronized across redundant management cards (SMC, MIO/UMIO). Full core dumps are not synchronized across management cards.

The following behaviors apply to the crash logging process.

- When a crash event arrives on an active management card, the event record is stored in its crashlog2 file along with the minicore, NPU, or kernel dump file in /flash/crsh2. The crash event and dump file are also automatically stored in the same locations on the standby management card.

- When a crash log entry is deleted via CLI command, it is deleted on both the active and standby management cards.

- When a management card is added or replaced, active and standby cards will automatically synchronize crash logs and dump files.

- When a crash event is received and the crash log file is full, the oldest entry in the crash log and its related dump file will be replaced with the latest arrived event and dump file on both management cards. Information for a maximum of 120 crash events can be stored on management cards.

- Duplicate crash events bump the count of hits in the existing record and update the new record with the old crash record. Additions to the count use the timestamp for the first time the event happened.
Configuring Software Crash Log Destinations

The system can be configured to store software crash log information to any of the following locations:

- **On the ASR 5000:**
  - **CompactFlash™:** Installed on the SMC [abridged crash log and associated dump files only]
  - **PCMCIA Flash Card:** Installed in the PCMCIA1 slot on the SMC
- **On the ASR 5500:**
  - **Flash memory:** Installed on the active MIO/UMIO [abridged crash log and associated dump files only]
  - **USB memory stick:** Installed in the USB slot on the active MIO/UMIO
- **On VPC**
  - **Flash memory:** Accessible by the virtual machine
  - **USB memory stick:** Installed in the USB slot of the platform (USB slot has been enabled via the hypervisor)
- **Network Server:** Any workstation or server on the network that the system can access using the Trivial File Transfer Protocol (TFTP), the File Transfer Protocol (FTP), the Secure File Transfer Protocol (SFTP), or the Hyper-Text Transfer Protocol (HTTP); this is recommended for large network deployments in which multiple systems require the same configuration

Crash log files (full core dumps) are written with unique names as they occur to the specified location. The name format is crash-card-cpu-time-core. Where card is the card slot, cpu is the number of the CPU on the card, and time is the Portable Operating System Interface (POSIX) timestamp in hexadecimal notation.

Use the following example to configure a software crash log destination in the Global Configuration mode:

```plaintext
configure
  crash enable [ encrypted ] url crash_url
end
```

Notes:

- Refer to the *Global Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.
- Repeat to configure additional software crash log destinations. There is no limit to the number of destinations that can be configured.

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Viewing Abridged Crash Log Information Using the CLI

You can view abridged crash information that is stored as a set of event records in flash memory on management cards (/flash/crashlog2). Each crash event record has an associated dump file (minicore, NPU or kernel) that can also be displayed (/flash/crsh2)

Follow the instructions in this section to view software crash events that have occurred on the system. These instructions assume that you are at the root prompt for the Exec mode.

**Step 1** View a list of software crash events by entering the following Exec mode command:
Configuring and Viewing Crash Logs

```
[local]host_name# show crash { all | list | number crash_num }
```

Notes:
- Run `show crash list` to obtain the number for a specific crash event.
- Run `show crash number crash_num` to display the output for the target crash event.

**Important:** Information about similar crash events is suppressed in the output of this command.

**Step 2**
View the dump file associated with a specific crash event.

The information contained in the dump file helps identify and diagnose any internal or external factors causing the software to crash.

- **Crash #** – unique number assigned by StarOS when logging the crash event
- **SW Version** – StarOS build release in format: RR.n(bbbbb)
- **Similar Crash Count** – number of similar crashes
- **Time of first crash** – timestamp when first crash occurred in format: YYY-MM-DD+hh:mm:ss
- **Failure message** – text of event message
- **Function** – code identifier
- **Process** – where the crash occurred (Card, CPU, PID, etc.)
- **Crash time** – timestamp for when the crash occurred in the format: YYY-MM-DD+hh:mm:ss time zone
- **Recent errno** – text of most recent error number.
- **Stack** – memory stack information
- **Last Bounce** – information about the messaging received prior to the crash
- **Registers** – memory register contents
- **Current inbound message** – hexadecimal information for the current inbound message
- **Address Map**
- **Recent heap activity** (oldest first)
- **Recent events** (oldest first)
- **Profile depth**

**Important:** The informational content of each crash log entry varies based on the type of crash and the StarOS release.
Saving Log Files

Log files can be saved to a file in a local or remote location specified by a URL. Use the following Exec mode command to save log files:

```
save logs { url } [active] [inactive] [callid call_id] [event-verbosity evt_verbosity] [facility facility] [level severity_level] [pdu-data pdu_format] [pdu-verbosity pdu_verbosity] [since from_date_time[until to_date_time] ] [ | { grep grep_options | more } ]
```

For detailed information on the `save logs` command, see the Exec Mode Commands chapter in the Command Line Interface Reference.
Event ID Overview

**Important:** The use of event IDs depends on the platform type and the licenses running on the platform.

Identification numbers (IDs) are used to reference events as they occur when logging is enabled on the system. As described previously, logs are collected on a per facility basis. Each facility possesses its own range of event IDs as indicated in the following table.

**Table 7. System Facilities and Event ID Ranges**

<table>
<thead>
<tr>
<th>Facility</th>
<th>Description</th>
<th>Event ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>a10</td>
<td>A10 Protocol Facility</td>
<td>28000-28999</td>
</tr>
<tr>
<td>a11</td>
<td>A11 Protocol Facility</td>
<td>29000-29999</td>
</tr>
<tr>
<td>a11mgr</td>
<td>A11 Manager Facility</td>
<td>90000-9999</td>
</tr>
<tr>
<td>aaa-client</td>
<td>AAA Client Facility</td>
<td>6000-6999</td>
</tr>
<tr>
<td>aaamgr</td>
<td>AAA Manager Facility</td>
<td>36000-36999</td>
</tr>
<tr>
<td>aaaproxy</td>
<td>AAA Proxy Facility</td>
<td>64000-64999</td>
</tr>
<tr>
<td>aal2</td>
<td>AAL2 Protocol Facility</td>
<td>173200-173299</td>
</tr>
<tr>
<td>acl-log</td>
<td>IP Access Control List (ACL) Facility</td>
<td>21000-21999</td>
</tr>
<tr>
<td>acsctrl</td>
<td>Active Charging Service Controller (ACSCtrl) Facility</td>
<td>90000-90999</td>
</tr>
<tr>
<td>acsmgr</td>
<td>Active Charging Service Manager (ACSMgr) Facility</td>
<td>91000-91999</td>
</tr>
<tr>
<td>afctrl</td>
<td>Ares Fabric Controller (ASR 5500 only)</td>
<td>186000-186999</td>
</tr>
<tr>
<td>afmgr</td>
<td>Ares Fabric Manager (ASR 5500 only)</td>
<td>187000-187999</td>
</tr>
<tr>
<td>alarmctrl</td>
<td>Alarm Controller Facility</td>
<td>65000-65999</td>
</tr>
<tr>
<td>alcap</td>
<td>Access Link Control Application Part (ALCAP) Protocol Facility</td>
<td>160900-161399</td>
</tr>
<tr>
<td>alcapmgr</td>
<td>ALCAP Manager Facility</td>
<td>160500-160899</td>
</tr>
<tr>
<td>asf</td>
<td>ASF Facility</td>
<td>73000-73999</td>
</tr>
<tr>
<td>asfprt</td>
<td>ASFPRT Facility</td>
<td>59000-59999</td>
</tr>
<tr>
<td>asngwmgm</td>
<td>Access Service Network (ASN) Gateway Manager Facility</td>
<td>100000-100499</td>
</tr>
<tr>
<td>asnpcmgr</td>
<td>ASN Paging/Location-Registry Manager Facility</td>
<td>100500-100999</td>
</tr>
<tr>
<td>bcmcs</td>
<td>Broadcast/Multicast Service (BCMCS) Facility</td>
<td>109000-109999</td>
</tr>
<tr>
<td>bfd</td>
<td>Bidirectional Forwarding Detection (BFD) Protocol Facility</td>
<td>170500-170999</td>
</tr>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol (BGP) Facility</td>
<td>85000-85999</td>
</tr>
<tr>
<td>bindmux</td>
<td>BindMux Manager Facility [Intelligent Policy Control Function (IPCF)]</td>
<td>158200-158999</td>
</tr>
<tr>
<td>Facility</td>
<td>Description</td>
<td>Event ID Range</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>bngmgr</td>
<td>Broadband Network Gateway (BNG) Manager Facility</td>
<td>182000-182999</td>
</tr>
<tr>
<td>bssap</td>
<td>Base Station System Application Part+ (BSSAP+) Service Facilities</td>
<td>131000-131199</td>
</tr>
<tr>
<td>bssgp</td>
<td>Base Station System GPRS Protocol (BSSGP) Facility</td>
<td>115050-115099</td>
</tr>
<tr>
<td>callhome</td>
<td>Call Home Facility</td>
<td>173600-173999</td>
</tr>
<tr>
<td>cap</td>
<td>CAMEL Application Part (CAP) Facility</td>
<td>87900-88099</td>
</tr>
<tr>
<td>chatconf</td>
<td>CHATCONF Facility</td>
<td>74000-74999</td>
</tr>
<tr>
<td>cli</td>
<td>Command Line Interface (CLI) Facility</td>
<td>30000-30999</td>
</tr>
<tr>
<td>connproxy</td>
<td>Connection Line Interface (CLI) Facility</td>
<td>190000-190999</td>
</tr>
<tr>
<td>crdt-ctl</td>
<td>Credit Control Facility</td>
<td>127000-127999</td>
</tr>
<tr>
<td>cscf</td>
<td>Call Session Control Function (CSCF) Facility</td>
<td>105000-108924</td>
</tr>
<tr>
<td>cscfcpmgr</td>
<td>CSCF CP Manager Facility</td>
<td>197000-197999</td>
</tr>
<tr>
<td>cscfmgm</td>
<td>CSCF FM Manager Facility</td>
<td>101000-101999</td>
</tr>
<tr>
<td>cscfnpdb</td>
<td>CSCF NPDB Facility</td>
<td>108925-108949</td>
</tr>
<tr>
<td>cscfrtcp</td>
<td>CSCF RTCP Facility</td>
<td>108976-108999</td>
</tr>
<tr>
<td>cscfrtp</td>
<td>CSCF RTP Facility</td>
<td>108950-108975</td>
</tr>
<tr>
<td>cscfttmgr</td>
<td>CSCF TT Manager Facility</td>
<td>163000-163499</td>
</tr>
<tr>
<td>csg</td>
<td>Closed Subscriber Groups (CSG) Facility</td>
<td>188000-188999</td>
</tr>
<tr>
<td>csg-acl</td>
<td>CSG Access Control List (ACL) Facility</td>
<td>189000-189999</td>
</tr>
<tr>
<td>csp</td>
<td>Card/Slot/Port (CSP) Facility</td>
<td>7000-7999</td>
</tr>
<tr>
<td>css</td>
<td>Content Steering Service (CSS) Facility [ESC]</td>
<td>77000-77499</td>
</tr>
<tr>
<td>css-sig</td>
<td>Content Service Selection (CSS) RADIUS Signaling Facility</td>
<td>77500-77599</td>
</tr>
<tr>
<td>cx-diameter</td>
<td>Cx Diameter Message Facility</td>
<td>92840-92849</td>
</tr>
<tr>
<td>dcardctrl</td>
<td>Daughter Card Controller Facility</td>
<td>62000-62999</td>
</tr>
<tr>
<td>dcardmgr</td>
<td>Daughter Card Manager Facility</td>
<td>57000-57999</td>
</tr>
<tr>
<td>demuxmgr</td>
<td>Demux Manager Facility</td>
<td>110000-110999</td>
</tr>
<tr>
<td>dgmbmgr</td>
<td>Diameter Gmb (DGMB) Application Manager Facility</td>
<td>126000-126999</td>
</tr>
<tr>
<td>dhcp</td>
<td>DHCP Facility</td>
<td>53000-53999</td>
</tr>
<tr>
<td>dhcpv6</td>
<td>DHCPv6 Protocol Facility</td>
<td>123000-123999</td>
</tr>
<tr>
<td>dhost</td>
<td>Distributed Host Manager Facility</td>
<td>83000-83999</td>
</tr>
<tr>
<td>diameter</td>
<td>Diameter Endpoint Facility</td>
<td>92000-92599</td>
</tr>
<tr>
<td>diabase</td>
<td>Diabase Message Facility</td>
<td>92800-92809</td>
</tr>
<tr>
<td>Facility</td>
<td>Description</td>
<td>Event ID Range</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>diameter-acct</td>
<td>Diameter Accounting Protocol Facility</td>
<td>112000-112999</td>
</tr>
<tr>
<td>diameter-auth</td>
<td>Diameter Authentication Protocol Facility</td>
<td>111000-111999</td>
</tr>
<tr>
<td>diameter-dns</td>
<td>Diameter DNS Subsystem Facility</td>
<td>92600-92699</td>
</tr>
<tr>
<td>diameter-ecs</td>
<td>ECS Diameter Signaling Facility</td>
<td>81990-81999</td>
</tr>
<tr>
<td>diameter-hdd</td>
<td>Diameter Horizontal Directional Drilling (HDD) Interface Facility</td>
<td>92700-92799</td>
</tr>
<tr>
<td>diameter-svc</td>
<td>Diameter Service Facility</td>
<td>121200-121999</td>
</tr>
<tr>
<td>diamproxy</td>
<td>Diameter Proxy Facility</td>
<td>119000-119999</td>
</tr>
<tr>
<td>dpath</td>
<td>Data Path for IPSec Facility</td>
<td>54000-54999</td>
</tr>
<tr>
<td>drvctrl</td>
<td>Driver Controller Facility</td>
<td>39000-39999</td>
</tr>
<tr>
<td>ds3mgr</td>
<td>DS3 and DS3/E Line Card Manager Facility (part of NPU Manager Controller Facility)</td>
<td>40000-40999</td>
</tr>
<tr>
<td>eap-diameter</td>
<td>Extensible Authentication Protocol (EAP) Diameter Facility</td>
<td>92870-92879</td>
</tr>
<tr>
<td>eap-ipsec</td>
<td>EAP IPSec Facility</td>
<td>118000-118999</td>
</tr>
<tr>
<td>ecs-css</td>
<td>ACS Session Manager (ACSMgr) Signalling Interface Facility</td>
<td>97000-97099</td>
</tr>
<tr>
<td>edr</td>
<td>Event Data Record (EDR) Facility</td>
<td>80000-80999</td>
</tr>
<tr>
<td>egtpc</td>
<td>eGTP-C Facility</td>
<td>141000-141999</td>
</tr>
<tr>
<td>egtpmgr</td>
<td>eGTP Manager Facility</td>
<td>143000-143999</td>
</tr>
<tr>
<td>egtpu</td>
<td>eGTP-U Facility</td>
<td>142000-142999</td>
</tr>
<tr>
<td>epdg</td>
<td>Evolved Packet Data Gateway (ePDG) Facility</td>
<td>178000-178999</td>
</tr>
<tr>
<td>evlog</td>
<td>Event Log Facility</td>
<td>2000-2999</td>
</tr>
<tr>
<td>famgr</td>
<td>Foreign Agent (FA) Manager Facility</td>
<td>33000-33999</td>
</tr>
<tr>
<td>firewall</td>
<td>Firewall Facility</td>
<td>96000-96999</td>
</tr>
<tr>
<td>fng</td>
<td>Femto Network Gateway (FNG) Facility</td>
<td>149000-149999</td>
</tr>
<tr>
<td>gbrmgr</td>
<td>Gb-Manager Facility</td>
<td>201900-202699</td>
</tr>
<tr>
<td>gcdr</td>
<td>GGSN-Charging Data Record (G-CDR) Facility</td>
<td>66000-66999</td>
</tr>
<tr>
<td>gmm</td>
<td>GPRS Mobility Management (GMM) Facility</td>
<td>88100-88299</td>
</tr>
<tr>
<td>gprs-app</td>
<td>General Packet Radio Service (GPRS) Application Facility</td>
<td>115100-115399</td>
</tr>
<tr>
<td>gprs-ns</td>
<td>GPRS-NS Protocol Facility</td>
<td>115000-115049</td>
</tr>
<tr>
<td>gq-rx-tx-diameter</td>
<td>Gq/Rx/Tx Diameter Messages Facility</td>
<td>92830-92839</td>
</tr>
<tr>
<td>gss-gcdr</td>
<td>GTPP Storage Server GCDDR Facility</td>
<td>98000-98099</td>
</tr>
<tr>
<td>gtpc</td>
<td>GTPC Protocol Facility</td>
<td>47000-47999</td>
</tr>
<tr>
<td>gtpcmgr</td>
<td>GTPC Signaling Demultiplexer Manager Facility</td>
<td>46000-46999</td>
</tr>
<tr>
<td>Facility</td>
<td>Description</td>
<td>Event ID Range</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>gtp</td>
<td>GTP-PRIME Protocol Facility</td>
<td>52000-52999</td>
</tr>
<tr>
<td>gtpu</td>
<td>GTPU Protocol Facility</td>
<td>45000-45999</td>
</tr>
<tr>
<td>gtpumgr</td>
<td>GTPU Manager Facility</td>
<td>157200-157999</td>
</tr>
<tr>
<td>gx-ty-diameter</td>
<td>Gx/Ty Diameter Messages Facility</td>
<td>92820-92829</td>
</tr>
<tr>
<td>gy-diameter</td>
<td>Gy Diameter Messages Facility</td>
<td>92810-92819</td>
</tr>
<tr>
<td>h248pRT</td>
<td>H.248 Protocol Facility</td>
<td>42000-42999</td>
</tr>
<tr>
<td>hamgr</td>
<td>Home Agent (HA) Manager Facility</td>
<td>34000-34999</td>
</tr>
<tr>
<td>hat</td>
<td>High Availability Task (HAT) Facility</td>
<td>3000-3999</td>
</tr>
<tr>
<td>hddctrl</td>
<td>Hard Disk (HD) Controller Facility</td>
<td>132000-132999</td>
</tr>
<tr>
<td>hddshare</td>
<td>HDD Share Facility</td>
<td>184000-184999</td>
</tr>
<tr>
<td>henb-gw</td>
<td>Home eNodeB-GW Facility</td>
<td>195000-195999</td>
</tr>
<tr>
<td>henbapp</td>
<td>Home eNodeB Application Facility</td>
<td>196000-196999</td>
</tr>
<tr>
<td>henbgwdemux</td>
<td>Home eNodeB-GW Demux Facility</td>
<td>194000-194999</td>
</tr>
<tr>
<td>henbgwmgr</td>
<td>Home eNodeB-GW Manager Facility</td>
<td>193000, 193999</td>
</tr>
<tr>
<td>hnb-gw</td>
<td>Home NodeB (HNB) Gateway Facility</td>
<td>151000-151999</td>
</tr>
<tr>
<td>hnbmgr</td>
<td>HNB Manager Facility</td>
<td>158000-158199</td>
</tr>
<tr>
<td>hss-peer-service</td>
<td>Home Subscriber Server (HSS) Facility [MME]</td>
<td>138000-138999</td>
</tr>
<tr>
<td>igmp</td>
<td>Internet Group Management Protocol (IGMP) Facility</td>
<td>113000-113999</td>
</tr>
<tr>
<td>ikev2</td>
<td>IKEv2 Facility</td>
<td>122000-122999</td>
</tr>
<tr>
<td>ims-authoriztn</td>
<td>IMS Authorization Service Library Facility</td>
<td>98100-98999</td>
</tr>
<tr>
<td>ims-sh</td>
<td>IMS SH Library Facility</td>
<td>124000-124999</td>
</tr>
<tr>
<td>imsimgr</td>
<td>International Mobile Subscriber Identity (IMSI) Manager Facility</td>
<td>114000-114999</td>
</tr>
<tr>
<td>imsue</td>
<td>IMS User Equipment (IMSUE) Facility</td>
<td>144000-145999</td>
</tr>
<tr>
<td>ip-arp</td>
<td>IP Address Resolution Protocol (ARP) Facility</td>
<td>19000-19999</td>
</tr>
<tr>
<td>ip-interface</td>
<td>IP Interface Facility</td>
<td>18000-18999</td>
</tr>
<tr>
<td>ip-route</td>
<td>IP Route Facility</td>
<td>20000-20999</td>
</tr>
<tr>
<td>ipms</td>
<td>Intelligent Packet Monitoring System (IPMS) Facility</td>
<td>134000-134999</td>
</tr>
<tr>
<td>ipne</td>
<td>IP Network Enabler (IPNE) Facility</td>
<td>192000-192999</td>
</tr>
<tr>
<td>ipsec</td>
<td>IPSec Protocol Facility</td>
<td>55000-56998</td>
</tr>
<tr>
<td>ipsg</td>
<td>IP Services Gateway (IPSG) Facility</td>
<td>128000-128999</td>
</tr>
<tr>
<td>ipsgmgr</td>
<td>IPSG Manager (IPSGMgr) Facility</td>
<td>99000-99999</td>
</tr>
<tr>
<td>Facility</td>
<td>Description</td>
<td>Event ID Range</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ipsp</td>
<td>IP Pool Sharing Protocol (IPSP) Facility</td>
<td>68000-68999</td>
</tr>
<tr>
<td>kvstore</td>
<td>Key/Value Store (KVSTORE) Facility</td>
<td>125000-125999</td>
</tr>
<tr>
<td>l2tp-control</td>
<td>L2TP Control PDU Protocol Facility</td>
<td>50000-50999</td>
</tr>
<tr>
<td>l2tp-data</td>
<td>L2TP Data PDU Protocol Facility</td>
<td>49000-49999</td>
</tr>
<tr>
<td>l2tpdemux</td>
<td>L2TP Demux Facility</td>
<td>63000-63999</td>
</tr>
<tr>
<td>l2tpmgr</td>
<td>L2TP Manager Facility</td>
<td>48000-48999</td>
</tr>
<tr>
<td>lagmgr</td>
<td>Link Aggregation Group (LAG) Manager Facility</td>
<td>179000-179999</td>
</tr>
<tr>
<td>ldap</td>
<td>Lightweight Directory Access Protocol (LDAP) Request Facility</td>
<td>160000-160499</td>
</tr>
<tr>
<td>li</td>
<td>Lawful Intercept (LI) Log Facility</td>
<td>69000-69999</td>
</tr>
<tr>
<td>linkmgr</td>
<td>Link Manager Facility</td>
<td>89500-89999</td>
</tr>
<tr>
<td>llc</td>
<td>Logical Link-Control (LLC) Layer Facility (GPRS)</td>
<td>115700-115799</td>
</tr>
<tr>
<td>local-policy</td>
<td>Local Policy Configuration Facility</td>
<td>161400-162399</td>
</tr>
<tr>
<td>m3ua</td>
<td>MTP Level 3 (M3UA) Protocol Facility [SIGTRAN]</td>
<td>87500-87699</td>
</tr>
<tr>
<td>magmgr</td>
<td>Mobile Access Gateway (MAG) Manager Facility</td>
<td>137500-137999</td>
</tr>
<tr>
<td>map</td>
<td>Mobile Application Part (MAP) Protocol Facility [SS7]</td>
<td>87100-87299</td>
</tr>
<tr>
<td>megadianmgr</td>
<td>MegaDiameter Manager Facility</td>
<td>121000-121199</td>
</tr>
<tr>
<td>mme-app</td>
<td>Mobility Management Entity (MME) Application Facility</td>
<td>147000-147999</td>
</tr>
<tr>
<td>mme-misc</td>
<td>MME Miscellaneous Facility</td>
<td>155800-156199</td>
</tr>
<tr>
<td>mmedemux</td>
<td>MME Demux Manager Facility</td>
<td>154000-154999</td>
</tr>
<tr>
<td>mmemgr</td>
<td>MME Manager Facility</td>
<td>137000-137499</td>
</tr>
<tr>
<td>mmgr</td>
<td>Master Manager (MMGR) Facility</td>
<td>86000-86399</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>Mobile IP (MIP) Protocol Facility</td>
<td>26000-26999</td>
</tr>
<tr>
<td>mobile-ip-data</td>
<td>MIP Tunneled Data Facility</td>
<td>27000-27999</td>
</tr>
<tr>
<td>mobile-ipv6</td>
<td>Mobile IPv6 Facility</td>
<td>129000-129999</td>
</tr>
<tr>
<td>mpls</td>
<td>Multiprotocol Label Switching (MPLS) Facility</td>
<td>163500-163999</td>
</tr>
<tr>
<td>mseg-app</td>
<td>Mobile Services Edge Gateway (MSEG) Application Facility</td>
<td>172300-172999</td>
</tr>
<tr>
<td>mseg-gtpc</td>
<td>MSEG GTPC Application Facility</td>
<td>172000-172199</td>
</tr>
<tr>
<td>mseg-gtpu</td>
<td>MSEG GTPU Application Facility</td>
<td>172200-172299</td>
</tr>
<tr>
<td>msegmgr</td>
<td>MSEG Manager Facility</td>
<td>171000-171999</td>
</tr>
</tbody>
</table>

Not supported in this release.
<table>
<thead>
<tr>
<th>Facility</th>
<th>Description</th>
<th>Event ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtp2</td>
<td>Message Transfer Part 2 (MTP2) Service Facility [SS7]</td>
<td>116900-116999</td>
</tr>
<tr>
<td>mtp3</td>
<td>Message Transfer Part 3 (MTP3) Service Facility [SS7]</td>
<td>115600-115699</td>
</tr>
<tr>
<td>multicast-proxy</td>
<td>Multicast Proxy Facility</td>
<td>94000-94999</td>
</tr>
<tr>
<td>nas</td>
<td>Network Access Signaling (NAS) Facility</td>
<td>153000-153999</td>
</tr>
<tr>
<td>netwstrg</td>
<td>Network Storage Facility</td>
<td>78000-78999</td>
</tr>
<tr>
<td>npucrtl</td>
<td>Network Processing Unit (NPU) Control Facility</td>
<td>16000-16999</td>
</tr>
<tr>
<td>npudrv</td>
<td>NPU Driver Facility</td>
<td>191000-191999</td>
</tr>
<tr>
<td>npumgr</td>
<td>NPU Manager (NPUMGR) Facility</td>
<td>17000-17999</td>
</tr>
<tr>
<td>npumgr-acl</td>
<td>NPUMGR ACL Facility</td>
<td>169000-169999</td>
</tr>
<tr>
<td>npumgr-driv</td>
<td>NPUMGR Driver Facility</td>
<td>185000-185999</td>
</tr>
<tr>
<td>npumgr-flow</td>
<td>NPUMGR Flow Facility</td>
<td>167000-167999</td>
</tr>
<tr>
<td>npumgr-fwd</td>
<td>NPUMGR Forwarding Facility</td>
<td>168000-168999</td>
</tr>
<tr>
<td>npumgr-init</td>
<td>NPUMGR Initialization Facility</td>
<td>164000-164999</td>
</tr>
<tr>
<td>npumgr-lc</td>
<td>NPUMGR LC Facility</td>
<td>180000-180999</td>
</tr>
<tr>
<td>npumgr-port</td>
<td>NPUMGR Port Facility</td>
<td>166000-166999</td>
</tr>
<tr>
<td>npumgr-recovery</td>
<td>NPUMGR Recovery Facility</td>
<td>165000-165999</td>
</tr>
<tr>
<td>npumgr-vpn</td>
<td>NPUMGR VPN Facility</td>
<td>181000-181999</td>
</tr>
<tr>
<td>npusim</td>
<td>NPUSIM Facility</td>
<td>176000-176999</td>
</tr>
<tr>
<td>ntfy-intf</td>
<td>Event Notification Interface Facility</td>
<td>170000-170499</td>
</tr>
<tr>
<td>orbs</td>
<td>Object Request Broker (ORB) System Facility</td>
<td>15000-15999</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF) Protocol Facility</td>
<td>38000-38999</td>
</tr>
<tr>
<td>ospfv3</td>
<td>OSPFv3 Protocol Facility</td>
<td>150000-150999</td>
</tr>
<tr>
<td>p2p</td>
<td>Peer-to-Peer (P2P) Facility</td>
<td>146000-146999</td>
</tr>
<tr>
<td>pccmgr</td>
<td>Policy Charging and Control (PCC) Manager Facility</td>
<td>159000-159499</td>
</tr>
<tr>
<td>pdg</td>
<td>Packet Data Gateway (PDG) Facility</td>
<td>152010-152999</td>
</tr>
<tr>
<td>pdgdmgmgr</td>
<td>PDG TCP Demux Manager (pdgdmgmr) Facility (this is a customer-specific facility)</td>
<td>162400-162999</td>
</tr>
<tr>
<td>pdif</td>
<td>Packet Data Interworking Function (PDIF) Facility</td>
<td>120000-120999</td>
</tr>
<tr>
<td>pgw</td>
<td>Packet Data Network Gateway (PGW) Facility</td>
<td>139000-139999</td>
</tr>
<tr>
<td>pmm-app</td>
<td>Packet Mobility Management (PMM) Application Facility [SGSN]</td>
<td>89200-89499</td>
</tr>
<tr>
<td>ppp</td>
<td>Point-To-Point Protocol (PPP) Facility</td>
<td>25000-25999</td>
</tr>
<tr>
<td>pppoe</td>
<td>Point-To-Point Protocol over Ethernet (PPPoE) Facility</td>
<td>183000-183999</td>
</tr>
</tbody>
</table>
## Event ID Overview

<table>
<thead>
<tr>
<th>Facility</th>
<th>Description</th>
<th>Event ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptt</td>
<td>PTT Facility</td>
<td>76000-76999</td>
</tr>
<tr>
<td>push</td>
<td>PUSH (VPNMgr CDR Push) Facility</td>
<td>133000-133999</td>
</tr>
<tr>
<td>radius-acct</td>
<td>RADIUS Accounting Protocol Facility</td>
<td>24000-24999</td>
</tr>
<tr>
<td>radius-auth</td>
<td>RADIUS Authentication Protocol Facility</td>
<td>23000-23999</td>
</tr>
<tr>
<td>radius-coa</td>
<td>RADIUS Change of Authorization (CoA) and Disconnect Facility</td>
<td>70000-70999</td>
</tr>
<tr>
<td>ranap</td>
<td>Radio Access Network Application Part (RANAP) Facility</td>
<td>87700-87899</td>
</tr>
<tr>
<td>rct</td>
<td>Recovery Control Task (RCT) Facility</td>
<td>13000-13999</td>
</tr>
<tr>
<td>rdt</td>
<td>Redirector Task (RDT) Facility</td>
<td>67000-67999</td>
</tr>
<tr>
<td>resmgr</td>
<td>Resource Manager (RM) Facility</td>
<td>14000-14999</td>
</tr>
<tr>
<td>rf-diameter</td>
<td>Rf Diameter Messages Facility</td>
<td>92860-92869</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP) Facility</td>
<td>35000-35999</td>
</tr>
<tr>
<td>rohc</td>
<td>Robust Header Compression (ROHC) Protocol Facility</td>
<td>103000-103999</td>
</tr>
<tr>
<td>rsvp</td>
<td>RSVP Protocol Facility</td>
<td>93000-93999</td>
</tr>
<tr>
<td>rau</td>
<td>RANAP User Adaptation (RUA) Protocol Facility</td>
<td>152000-152009</td>
</tr>
<tr>
<td>s1ap</td>
<td>S1 Application Protocol (S1AP) Facility</td>
<td>155200-155799</td>
</tr>
<tr>
<td>saegw</td>
<td>System Architecture Evolution Gateway Facility</td>
<td>191000-191999</td>
</tr>
<tr>
<td>sct</td>
<td>Shared Configuration Task (SCT) Facility</td>
<td>32000-32099</td>
</tr>
<tr>
<td>scsp</td>
<td>Stream Control Transmission Protocol (SCTP) Protocol Facility</td>
<td>87300-87499</td>
</tr>
<tr>
<td>sess-gr</td>
<td>SESS-GR Facility</td>
<td>77600-77999</td>
</tr>
<tr>
<td>sessctl</td>
<td>Session Controller Facility</td>
<td>8000-8999</td>
</tr>
<tr>
<td>sessmgr</td>
<td>Session Manager Facility</td>
<td>10000-12999</td>
</tr>
<tr>
<td>sess alcoholic</td>
<td>Session Trace Facility</td>
<td>155000-155199</td>
</tr>
<tr>
<td>sft</td>
<td>Switch Fabric Task (SFT) Facility</td>
<td>58000-58999</td>
</tr>
<tr>
<td>sgs</td>
<td>SGs Interface Protocol Facility [MME]</td>
<td>173000-173199</td>
</tr>
<tr>
<td>sgsn-app</td>
<td>SGSN Application Interface Facility</td>
<td>115900-115999</td>
</tr>
<tr>
<td>sgsn-failures</td>
<td>SGSN Call Failures Facility</td>
<td>89100-89199</td>
</tr>
<tr>
<td>sgsn-gtpc</td>
<td>SGSN GTP-C Protocol Facility</td>
<td>116000-116599</td>
</tr>
<tr>
<td>sgsn-gtpu</td>
<td>SGSN GTP-U Protocol Facility</td>
<td>86900-87099</td>
</tr>
<tr>
<td>sgsn-mbms-bearer</td>
<td>SGSN MBMS Bearer Application (SMGR) Facility</td>
<td>116600-116799</td>
</tr>
<tr>
<td>sgsn-misc</td>
<td>SGSN Miscellaneous Facility</td>
<td>88800-89099</td>
</tr>
<tr>
<td>Facility</td>
<td>Description</td>
<td>Event ID Range</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>sgsn-system</td>
<td>SGSN System Components Facility</td>
<td>86400-86499</td>
</tr>
<tr>
<td>sgsn-test</td>
<td>SGSN Tests Facility</td>
<td>88700-88799</td>
</tr>
<tr>
<td>sgsn2</td>
<td>SGSN2 Facility</td>
<td>114000-117999</td>
</tr>
<tr>
<td>sgtpcmrg</td>
<td>SGSN GTP-C (SGTPC) Manager Facility</td>
<td>117000-117999</td>
</tr>
<tr>
<td>sgw</td>
<td>Serving Gateway (SGW) Facility</td>
<td>140000-140999</td>
</tr>
<tr>
<td>sh-diameter</td>
<td>Sh Diameter Messages Facility</td>
<td>92850-92859</td>
</tr>
<tr>
<td>sipdprt</td>
<td>SIPCDPRT Facility</td>
<td>95000-95999</td>
</tr>
<tr>
<td>sitmain</td>
<td>System Initiation Task (SIT) Main Facility</td>
<td>4000-4999</td>
</tr>
<tr>
<td>sm-app</td>
<td>Short Message Service (SMS) Facility</td>
<td>88300-88499</td>
</tr>
<tr>
<td>sms</td>
<td>SMS Service Facility</td>
<td>116800-116899</td>
</tr>
<tr>
<td>sndcp</td>
<td>Sub Network Dependent Convergence Protocol (SNDCP) Facility</td>
<td>115800-115899</td>
</tr>
<tr>
<td>snmp</td>
<td>Simple Network Management Protocol (SNMP) Facility</td>
<td>22000-22999</td>
</tr>
<tr>
<td>sprmgr</td>
<td>Subscriber Policy Register (SPR) Manager Facility</td>
<td>159500-159999</td>
</tr>
<tr>
<td>srdb</td>
<td>Static Rating Database Facility</td>
<td>102000-102999</td>
</tr>
<tr>
<td>srp</td>
<td>Service Redundancy Protocol (SRP) Facility</td>
<td>84000-84999</td>
</tr>
<tr>
<td>ssclfnni</td>
<td>SSCFNNI Protocol Facility [ATM]</td>
<td>115500-115599</td>
</tr>
<tr>
<td>sscop</td>
<td>SSCOP Protocol Facility [ATM]</td>
<td>115400-115499</td>
</tr>
<tr>
<td>ssh-ipsec</td>
<td>SSH IP Security Facility</td>
<td>56999-56999</td>
</tr>
<tr>
<td>ssl</td>
<td>SSL Facility (this is a customer-specific facility)</td>
<td>156200-157199</td>
</tr>
<tr>
<td>stat</td>
<td>Statistics Facility</td>
<td>31000-31999</td>
</tr>
<tr>
<td>system</td>
<td>System Facility</td>
<td>1000-1999</td>
</tr>
<tr>
<td>tacacs+</td>
<td>TACACS+ Protocol Facility</td>
<td>37000-37999</td>
</tr>
<tr>
<td>taclcp</td>
<td>TACLCP Facility</td>
<td>44000-44999</td>
</tr>
<tr>
<td>testctrl</td>
<td>Test Controller Facility</td>
<td>174000-174999</td>
</tr>
<tr>
<td>testmgr</td>
<td>Test Manager Facility</td>
<td>175000-175999</td>
</tr>
<tr>
<td>threshold</td>
<td>Threshold Facility</td>
<td>61000-61999</td>
</tr>
<tr>
<td>ttg</td>
<td>Tunnel Termination Gateway (TTG) Facility</td>
<td>130000-130999</td>
</tr>
<tr>
<td>tucl</td>
<td>TCP/UDP Convergence Layer (TUCL) Facility [SS7]</td>
<td>88500-88699</td>
</tr>
<tr>
<td>udr</td>
<td>User Data Record (UDR) Facility</td>
<td>79000-79999</td>
</tr>
<tr>
<td>user-data</td>
<td>User-Data Facility</td>
<td>51000-51999</td>
</tr>
</tbody>
</table>
### Event ID Overview

The system provides the flexibility to configure the level of information that is displayed when logging is enabled. The following levels are supported:

- **critical**: Logs only those events indicating a serious error has occurred that is causing the system or a system component to cease functioning. This is the highest severity level.
- **error**: Logs events that indicate an error has occurred that is causing the system or a system component to operate in a degraded state. This level also logs events with a higher severity level.
- **warning**: Logs events that may indicate a potential problem. This level also logs events with a higher severity level.
- **unusual**: Logs events that are very unusual and may need to be investigated. This level also logs events with a higher severity level.
- **info**: Logs informational events and events with a higher severity level.
- **trace**: Logs events useful for tracing and events with a higher severity level.
- **debug**: Logs all events regardless of the severity.

Each of the above levels correspond to the “severity” level of the event ID. Therefore, only those event IDs with a “severity” level equal to the logging level are displayed.

## Event Severities

### Understanding Event ID Information in Logged Output

This section explains the event information that is displayed when logging is enabled.

The following displays a sample output for an event that was logged.

```
2011-Dec-11+5:18:41.993 [cli 30005 info] [8/0/609 cli:8000609 _commands_cli.c:1290] [software internal system] CLI session ended for Security Administrator admin on device /dev/pts/2
```

The following table describes the elements of contained in the sample output.
### Table 8. Event Element Descriptions

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-Dec-11+5:18:41.993</td>
<td>Date/Timestamp indicating when the event was generated</td>
</tr>
</tbody>
</table>
| [cli 30005 info] | Information about the event including:  
  - The facility the event belongs to  
  - The event ID  
  - The event’s severity level  
  In this example, the event belongs to the CLI facility, has an ID of 3005, and a severity level of “info”. |
| [8/0/609 cli:800609 _commands_cli.c:1290] | Information about the specific CLI instance. |
| [software internal system] | Indicates that the event was generated because of system operation. |
| CLI session ended for Security Administrator admin on device /dev/pts/2 | The event’s details. Event details may, or may not include variables that are specific to the occurrence of the event. |
Chapter 13
Troubleshooting

This chapter provides information and instructions for using the StarOS command line interface (CLI) for troubleshooting any issues that may arise during VPC-VSM operation.

The following topics are included:

- Monitoring StarOS VPC-VSM
- Verifying StarOS Network Connectivity
- Using StarOS Diagnostic Utilities

**Important:** Each VPC-VSM instance (StarOS VM) requires separate troubleshooting using the techniques described in this chapter. Up to four StarOS VMs can be running on a single VSM. You must be logged into the CLI of the target VM to use the commands described in this chapter.
Monitoring StarOS VPC-VSM

Basic tools and procedures for monitoring the VPC-VSM are described in the Monitoring the VPC-VSM chapter. VPC-VSM also provides diagnostic tools that are briefly described in the remaining sections of this chapter.

- Verifying StarOS Network Connectivity
  - Using the ping or ping6 Command
  - Using the traceroute or traceroute6 Command
  - Viewing IP Routes
  - Viewing the Address Resolution Protocol Table
- Using StarOS Diagnostic Utilities
  - Using the Monitor Utility
  - Using the Protocol Monitor
Verifying StarOS Network Connectivity

There are multiple StarOS commands to verify and/or troubleshoot network connectivity of the target VPC-VSM instance. Note that network connectivity can only be tested only after VM interfaces and ports have been configured and bound.

The commands specified in this section should be issued on a context-by-context basis. Contexts act like virtual private networks (VPNs) that operate independently of other contexts. Ports, interfaces, and routes configured in one context cannot be tested from another context without additional configuration.

To switch between contexts enter the following command at the root prompt for the Exec mode:

```
context context_name
```

`context_name` is the name of the context to which you wish to switch. The following prompt appears:

```
[context_name]host_name#
```

Using the ping or ping6 Command

The `ping` or `ping6` command verifies the system’s ability to communicate with a remote node in the network by passing data packets between and measuring the response. This command is useful in verifying network routing and if a remote node is able to respond at the IP layer.

Syntax

The `ping` command has the following syntax:

```
ping host_ipv4_address [ count num_packets ] [ flood ] [ pattern packet_pattern ]
[ size octet_count ] [ src { src_host_name | src_host_ipv4_address } ] [ vrf vrf_nam ]
```

The `ping6` command has the following syntax:

```
ping6 host_ipv6_address [ count num_packets ] [ flood ] [ pattern packet_pattern ]
[ size octet_count ] [ src { src_host_name | src_host_ipv6_address } ] [ vrf vrf_nam ]
```

For complete information regarding the above commands, see the `Exec Mode Commands` chapter of the Command line Interface Reference.

The following displays a sample of a successful `ping` (IPV4) response.

```
PING 192.29.96.1 (192.29.96.1) 56(84) bytes of data.
64 bytes from 192.29.96.1: icmp_seq=1 ttl=255 time=0.624 ms
64 bytes from 192.29.96.1: icmp_seq=2 ttl=255 time=0.606 ms
64 bytes from 192.29.96.1: icmp_seq=3 ttl=255 time=0.612 ms
64 bytes from 192.29.96.1: icmp_seq=4 ttl=255 time=3.78 ms
64 bytes from 192.29.96.1: icmp_seq=5 ttl=255 time=4.83 ms
```
Troubleshooting

If no response is received from the target follow these troubleshooting procedures:

- Verify that the correct IP address was entered.
- Attempt to ping a different device on the same network. If the ping was successful then it is likely that your system configuration is correct. Verify that the device you are attempting to ping is powered and functioning properly.
- Verify the port is operational.
- Verify that the configuration of the ports and interfaces within the context are correct.
- If the configuration is correct and you have access to the device that you’re attempting to ping, ping the system from that device.
- If there is still no response, it is likely that the packets are getting discarded by a network device. Use the `traceroute` or `traceroute6` and `show ip static-route` commands discussed in this segment to further troubleshoot the issue.

Using the `traceroute` or `traceroute6` Command

The traceroute or traceroute6 command collects information on the route data will take to a specified host. This is a useful troubleshooting command that can be used to identify the source of significant packet delays or packet loss on the network. This command can also be used to identify bottle necks in the routing of data over the network.

**traceroute – IPv4**

The `traceroute` command has the following syntax:

```
traceroute { host_name | host_ipv4_address } [ count packets ] [ df ] [ maxttl max_ttl ] [ minttl min_ttl ] [ port port_number ] [ size octet_count ] [ src { src_host_name | src_host_ipv4_address } ] [ timeout seconds ] [ vrf vrf_name ]
```

For complete information regarding the above command, see the `Exec Mode Commands` chapter of the Command line Interface Reference.

The following displays a sample output.

```
traceroute to 192.168.250.1 (192.168.250.1), 30 hops max, 40 byte packets

1 192.168.250.1 (192.168.250.1) 0.446 ms 0.235 ms 0.178 ms
```
**traceroute6 – IPv6**

The **traceroute6** command has the following syntax:

```
traceroute6 { host_name | host_ipv6_address } [ count packets ] [ maxttl max_ttl ] [ port port_number ] [ size octet_count ] [ src { src_host_name | src_host_ipv6_address } ] [ timeout seconds ] [ vrf vrf_name ]
```

For complete information regarding the above command, see the *Exec Mode Commands* chapter of the *Command line Interface Reference*.

The following displays a sample output.

```
traceroute6 to 2001:4A2B::1f3F (2001:4A2B::1f3F), 30 hops max, 40 byte packets
1 2001:4A2B::1f3F (2001:4A2B::1f3F)  0.446 ms  0.235 ms  0.178 ms
```

**Viewing IP Routes**

The system provides a mechanism for viewing route information to a specific node or for an entire context. This information can be used to verify network connectivity and to ensure the efficiency of the network connection. The command has the following syntax:

```
show ip route [ route_ip_address ]

show ipv6 route [ route_ipv6_address ]
```

For complete information regarding the above commands, see the *Exec Mode Commands* chapter of the *Command line Interface Reference*.

If no keywords are specified, all IP routes within the context’s routing table are displayed.

The following displays a sample of this command’s output showing a context IPv4 routing table.

```
"*" indicates the Best or Used route.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop</th>
<th>Protocol</th>
<th>Prec</th>
<th>Cost</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0.0.0.0/0</td>
<td>192.29.96.1</td>
<td>static</td>
<td>1</td>
<td>0</td>
<td>LOCAL1</td>
</tr>
<tr>
<td>*192.29.96.0/24</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td>LOCAL1</td>
</tr>
<tr>
<td>*192.29.96.202/32</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td>LOCAL1</td>
</tr>
</tbody>
</table>

Total route count : 3
Unique route count: 3
Connected: 2 Static: 1
Verifying StarOS Network Connectivity

Viewing the Address Resolution Protocol Table

The system provides a mechanism for viewing Address Resolution Protocol (ARP) table information to a specific node or for an entire context. This information can be used to verify that when the system sends an ARP packet, it receives valid responses from other network nodes. The command has the following syntax:

```
show ip arp [ arp_ip_address ]
```

`arp_ip_address` specifies a specific network node for which to display ARP information. The address can be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. If this keyword is not specified, all entries within the context’s ARP table are displayed.

**Important:** Restarting the VPN Manager removes all interfaces from the kernel which in turn removes all ARP entries. However, the NPU still retains all of the ARP entries so that there is no traffic disruption. From a user point of view, `show ip arp` is broken since this command gathers information from the kernel and not the NPU.

The following displays a sample of this command’s output showing a context’s ARP table.

Flags codes:

- I - Incomplete
- R - Reachable
- M - Permanent
- S - Stale
- D - Delay
- P - Probe
- F - Failed

<table>
<thead>
<tr>
<th>Address</th>
<th>Link Type</th>
<th>Link Address</th>
<th>Flags</th>
<th>Mask</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.29.96.1</td>
<td>ether</td>
<td>00:23:05:C6:68:43</td>
<td>R</td>
<td>LOCAL1</td>
<td></td>
</tr>
<tr>
<td>192.29.96.9</td>
<td>ether</td>
<td>00:0C:29:8E:1D:56</td>
<td>R</td>
<td>LOCAL1</td>
<td></td>
</tr>
</tbody>
</table>

Total number of arps: 2
Using StarOS Diagnostic Utilities

StarOS provides protocol monitor and test utilities that are useful when troubleshooting or verifying configurations. The information generated by these utilities can help identify the root cause of a software or network configuration issue. This section describes how to use these utilities.

**Important:** Only an administrator with Operator or higher privilege can run the diagnostic utilities described in this section.

**Using the Monitor Utility**

For troubleshooting purposes, the system provides a protocol monitoring utility. This tool displays protocol information for a particular subscriber session or for every session being processed via the VPC-VSM instance.

**Caution:** The monitor tool may cause session processing delays and/or data loss. Therefore, it should be used only when troubleshooting.

**Using the Protocol Monitor**

The protocol monitor displays information for every session that is currently being processed. Depending on the number of protocols monitored, and the number of sessions in progress, a significant amount of data is generated. It is highly recommended that logging be enabled on your terminal client in order to capture all of the information that is generated. The protocol monitor is also used to capture packets over a particular interface.

Follow the instructions below to invoke and configure the protocol monitoring tool.

**Step 1** Invoke the protocol monitor from the Exec mode by entering the `monitor protocol` command.

An output listing all the currently available protocols, each with an assigned number, is displayed.

**Step 2** Choose the protocol that you wish to monitor by entering the associated number at the `Select:` prompt. A right arrow (>) appears next to the protocol you selected.

**Step 3** Repeat step 2 as needed to choose multiple protocols.

**Step 4** Press B to begin the protocol monitor.

```
WARNING!!! You have selected options that can DISRUPT USER SERVICE
Existing CALLS MAY BE DROPPED and/or new CALLS MAY FAIL!!!
(Under heavy call load, some debugging output may not be displayed)
Proceed? - Select (Y)es or (N)o
```

**Step 5** Enter Y to proceed with the monitor or N to go back to the previous menu.

```
C - Control Events (ON )
```
|
|---|
| **D** - Data Events | (ON ) |
| **E** - EventID Info | (ON ) |
| **H** - Display ethernet | (ON ) |
| **I** - Inbound Events | (ON ) |
| **O** - Outbound Events | (ON ) |
| **S** - Sender Info | (OFF) |
| **T** - Timestamps | (ON ) |
| **X** - PDU Hexdump | (OFF) |
| **A** - PDU Hex/Ascii | (OFF) |
| **+/-** Verbosity Level | ( 1) |
| **L** - Limit Context | (OFF) |
| **M** - Match Newcalls | (ON ) |
| **R** - RADIUS Dict | (no-override) |
| **G** - GTPP Dict | (no-override) |
| **Y** - Multi-Call Trace | (OFF)) |

(Q)uit,  <ESC> Prev Menu,  <SPACE> Pause,  <ENTER> Re-Display Options

**Step 6**  Configure the amount of information that is displayed by the monitor. To enable or disable options, enter the letter associated with that option (C, D, E, etc.). To increase or decrease the verbosity, use the plus (+) or minus (-) keys. The current state, ON (enabled) or OFF (disabled), is shown to the right of each option.

**Step 7**  Press the **Enter** key to refresh the screen and begin monitoring.
The monitor remains active until disabled. To quit the protocol monitor and return to the prompt, press **q**.
Chapter 14
Access Control Lists

This chapter describes system support for access control lists and explains how they are configured. The product administration guides provide examples and procedures for configuration of basic services on the system. You should select the configuration example that best meets your service model before using the procedures described below.

Important: You do not require a license to configure ACLs. However, the number of ACLs configured may impact performance significantly.

This chapter contains the following sections:

- Understanding ACLs
- Configuring ACLs on the System
- Applying IP ACLs

Important: Not all commands and keywords/variables may be available. Availability depends on the platform type.
Overview

IP access lists, commonly known as access control lists (ACLs), control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

Separate ACLs may be created for IPv4 and IPv6 access routes.
Understanding ACLs

This section discusses the two main aspects to ACLs on the system:

- Rule(s)
- Rule Order

**Important:** Refer to *ACL Configuration Mode Commands* and the *IPv6 ACL Configuration Mode Commands* chapter in the *Command Line Interface Reference* for the full command syntax.

### Rule(s)

A single ACL consists of one or more ACL rules. Each rule is a filter configured to take a specific action when packets matching specific criteria. Up to 128 rules can be configured per ACL.

**Important:** Configured ACLs consisting of no rules imply a “deny any” rule. The *deny* action and *any* criteria are discussed later in this section. This is the default behavior for an empty ACL.

Each rule specifies the action to take when a packet matches the specified criteria. This section discusses the rule actions and criteria supported by the system.

### Actions

ACLs specify that one of the following actions can be taken on a packet that matches the specified criteria:

- **Permit:** The packet is accepted and processed.
- **Deny:** The packet is rejected.
- **Redirect:** The packet is forwarded to the specified next-hop address through a specific system interface or to the specified context for processing.

**Important:** Redirect rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context, or APN for UMTS subscribers.

### Criteria

Each ACL consists of one or more rules specifying the criteria that packets will be compared against. The following criteria are supported:

- **Any:** Filters all packets
- **Host:** Filters packets based on the source host IP address
- **ICMP:** Filters Internet Control Message Protocol (ICMP) packets
- **IP:** Filters Internet Protocol (IP) packets
- **Source IP Address:** Filter packets based on one or more source IP addresses
- **TCP**: Filters Transport Control Protocol (TCP) packets
- **UDP**: Filters User Datagram Protocol (UDP) packets

Each of the above criteria are described in detail in the sections that follow.

**Important**: The following sections contain basic ACL rule syntax information. Refer to the *ACL Configuration Mode Commands* and *IPv6 ACL Configuration Mode Commands* chapters in the *Command Line Interface Reference* for the full command syntax.

- **Any**: The rule applies to all packets.
- **Host**: The rule applies to a specific host as determined by its IP address.
- **ICMP**: The rule applies to specific Internet Control Message Protocol (ICMP) packets, Types, or Codes. ICMP type and code definitions can be found at [www.iana.org](http://www.iana.org) (RFC 3232).
- **IP**: The rule applies to specific Internet Protocol (IP) packets or fragments.
- **IP Packet Size Identification Algorithm**: The rule applies to specific Internet Protocol (IP) packets identification for fragmentation during forwarding.

  This configuration is related to the “IP Identification field” assignment algorithm used by the system, when subscriber packets are being encapsulated (such as Mobile IP and other tunneling encapsulation). Within the system, subscriber packet encapsulation is done in a distributed way and a 16-bit IP identification space is divided and distributed to each entity which does the encapsulation, so that unique IP identification value can be assigned for IP headers during encapsulation.

  Since this distributed IP Identification space is small, a non-zero unique identification will be assigned only for those packets which may potentially be fragmented during forwarding (since the IP identification field is only used for reassembly of the fragmented packet). The total size of the IP packet is used to determine the possibility of that packet getting fragmented.

- **Source IP Address**: The rule applies to specific packets originating from a specific source address or a group of source addresses.
- **TCP**: The rule applies to any Transport Control Protocol (TCP) traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. TCP port numbers definitions can be found at [www.iana.org](http://www.iana.org)
- **UDP**: The rule applies to any User Datagram Protocol (UDP) traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. UDP port numbers definitions can be found at [www.iana.org](http://www.iana.org).

### Rule Order

A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Additional rules can be added to an existing ACL and properly ordered using either of the following options:

- **Before**
- **After**

Using these placement options requires the specification of an existing rule in the ACL and the configuration of the new rule as demonstrated by the following flow:

```
[ before | after ] { existing_rule }
```
Configuring ACLs on the System

This section describes how to configure ACLs.

**Important:** This section provides the minimum instruction set for configuring access control list on the system. For more information on commands that configure additional parameters and options, refer to the *ACL Configuration Mode Commands* and *IPv6 ACL Configuration Mode Commands* chapters in the *Command Line Interface Reference*.

To configure the system to provide an access control list facility to subscribers:

**Step 1** Create the access control list by following the example configuration in *Creating ACLs*.

**Step 2** Specify the rules and criteria for action in the ACL list by following the example configuration in *Configuring Action and Criteria for Subscriber Traffic*.

**Step 3** Optional. The system provides an “undefined” ACL that acts as a default filter for all packets into the context. The default action is to “permit all”. Modify the default configuration for “unidentified” ACLs for by following the example configuration in *Configuring an Undefined ACL*.

**Step 4** Verify your ACL configuration by following the steps in *Verifying the ACL Configuration*.

**Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode `save configuration` command. For additional information refer to the *Verifying and Saving Your Configuration* chapter.

Creating ACLs

To create an ACL, enter the following command sequence from the Exec mode of the system CLI:

```
configure
context acl_ctxt_name [ -noconfirm ]
{ ip | ipv6 } access-list acl_list_name
end
```

Notes:

- The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task. Typically, the maximum is less than 200.

Configuring Action and Criteria for Subscriber Traffic

To create rules to deny/permit the subscriber traffic and apply the rules after or before action, enter the following command sequence from the Exec mode of the system CLI:

```
configure
context acl_ctxt_name [ -noconfirm ]
```
Access Control Lists

Configuring ACLs on the System

VPC-VSM System Administration Guide, StarOS Release 19

{ ip | ipv6 } access-list acl_list_name

deny { ip_address | any | host | icmp | ip | log | tcp | udp }
permit { ip_address | any | host | icmp | ip | log | tcp | udp }

after { deny | permit | readdress | redirect }
before { deny | permit | readdress | redirect }
end

Notes:

⚠️ Caution: The system does not apply a “deny any” rule, unless it is specified in the ACL. This behavior can be changed by adding a “deny any” rule at the end of the ACL.

- The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules chapter.

- Use the information provided in the Actions and Criteria to configure the rules that comprise the ACL. For more information, refer to the ACL Configuration Mode Commands and IPv6 ACL Configuration Mode Commands chapters in the Command Line Interface Reference.

Configuring an Undefined ACL

As discussed previously the system uses an “undefined” ACL mechanism for filtering the packet(s) in the event that an ACL that has been applied is not present. This scenario is likely the result of a mis-configuration such as the ACL name being mis-typed during the configuration process.

For these scenarios, the system provides an “undefined” ACL that acts as a default filter for all packets into the context. The default action is to “permit all”.

To modify the default behavior for unidentified ACLs, use the following configuration:

```
configure

custom acl_ctxt_name [-noconfirm]

access-list undefined { deny-all | permit-all }

end
```

Notes:

- Context name is the name of the context containing the “undefined” ACL to be modified. For more information, refer to the Context Configuration Mode Commands chapter in the Command Line Interface Reference.

Verifying the ACL Configuration

To verify the ACL configuration, enter the Exec mode `show { ip | ipv6 } access-list` command.

The following is a sample output of this command. In this example, an ACL named `acl_1` was configured.
ip access list acl_1
  deny host 10.2.3.4
  deny ip any host 10.2.3.4
  permit any 10.2.4.4
1 ip access-lists are configured.
Applying IP ACLs

Once an ACL is configured, it must be applied to take effect.

**Important:** All ACLs should be configured and verified according to the instructions in the Configuring ACLs on the System prior to beginning these procedures. The procedures described below also assume that the subscribers have been previously configured.

As discussed earlier, you can apply an ACL to any of the following:

- Applying an ACL to an Individual Interface
- Applying an ACL to All Traffic Within a Context (known as a policy ACL)
- Applying an ACL to an Individual Subscriber
- Applying a Single ACL to Multiple Subscribers
- Applying a Single ACL to Multiple Subscribers via APNs (for 3GPP subscribers only)

**Important:** ACLs must be configured in the same context in which the subscribers and/or interfaces to which they are to be applied. Similarly, ACLs to be applied to a context must be configured in that context.

If ACLs are applied at multiple levels within a single context (such as an ACL is applied to an interface within the context and another ACL is applied to the entire context), they will be processed as shown in the following figure and table.

**Figure 3. ACL Processing Order**

**Table 9. ACL Processing Order Descriptions**

<table>
<thead>
<tr>
<th>Order</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An inbound ACL configured for the receiving interface in the Source Context is applied to the tunneled data (such as the outer IP header). The packet is then forwarded to the Destination Context.</td>
</tr>
<tr>
<td>2</td>
<td>An inbound ACL configured for the subscriber (either the specific subscriber or for any subscriber facilitated by the context) is applied.</td>
</tr>
</tbody>
</table>
Applying IP ACLs

<table>
<thead>
<tr>
<th>Order</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An inbound ACL configured for the receiving interface configured in the Destination Context is applied.</td>
</tr>
<tr>
<td>2</td>
<td>An outbound ACL configured for the subscriber (either the specific subscriber or for any subscriber facilitated by the context) is applied. The packet is then forwarded to the Source Context.</td>
</tr>
<tr>
<td>3</td>
<td>A context ACL (policy ACL) configured in the Source Context is applied prior to forwarding.</td>
</tr>
<tr>
<td>4</td>
<td>An outbound ACL configured on the interface in the Source Context through which the packet is being forwarded, is applied to the tunneled data (such as the outer IP header).</td>
</tr>
</tbody>
</table>

In the event that an IP ACL is applied that has not been configured (for example, the name of the applied ACL was configured incorrectly), the system uses an “undefined” ACL mechanism for filtering the packet(s).

This section provides information and instructions for applying ACLs and for configuring an “undefined” ACL.

Applying an ACL to an Individual Interface

This section provides information and instructions for applying one or more ACLs to an individual interface configured on the system.

Important: This section provides the minimum instruction set for applying the ACL list to an interface on the system. For more information on commands that configure additional parameters and options, refer to the Ethernet Interface Configuration Mode Commands chapter in the Command Line Interface Reference.

To configure the system to provide ACL facility to subscribers:

Step 1 Apply the configured access control list by following the example configuration in Applying the ACL to an Interface.

Step 2 Verify that ACL is applied properly on interface by following the steps in Verifying the ACL Configuration on an Interface.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode save configuration command. For additional information refer to the Verifying and Saving Your Configuration chapter.

Applying the ACL to an Interface

To apply the ACL to an interface, use the following configuration:

```
configure
c

context acl_ctxt_name [ -noconfirm ]

interface interface_name
```
Applying IP ACLs

{ ip | ipv6 } access-group acl_list_name { in | out } [ preference ]
end

Notes:
- The context name is the name of the ACL context containing the interface to which the ACL is to be applied.
- The ACL to be applied must be configured in the context specified by this command.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Verifying the ACL Configuration on an Interface

This section describes how to verify the ACL configuration.

Step 1  In the Exec Mode, enter the following command:

[local]host_name# show configuration context context_name

context_name is the name of the context containing the interface to which the ACL(s) was/were applied.

The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

configure
context context_name
  ip access-list acl_name
  deny host ip_address
  deny ip any host ip_address
  exit
  ip access-group access_group_name
  service-redundancy-protocol
  exit
  interface interface_name
    ip address ip_address/mask
    exit
  subscriber default
  exit
  aaa group default
  exit
Applying an ACL to All Traffic Within a Context

This section provides information and instructions for applying one or more ACLs to a context configured within a specific context on the system. The applied ACLs, known as policy ACLs, contain rules that apply to all traffic facilitated by the context.

**Important:** This section provides the minimum instruction set for applying the ACL list to all traffic within a context. For more information on commands that configure additional parameters and options, refer to the **Context Configuration Mode Commands** chapter in the **Command Line Interface Reference**.

To configure the system to provide access control list facility to subscribers:

**Step 1** Apply the configured ACL as described in **Applying the ACL to a Context**.

**Step 2** Verify that ACL is applied properly on interface as described in **Verifying the ACL Configuration in a Context**.

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode `save configuration` command. For additional information refer to the **Verifying and Saving Your Configuration** chapter.

Applying the ACL to a Context

To apply the ACLs to a context, use the following configuration:

```plaintext
configure
  context acl_ctxt_name [ -noconfirm ]
    { ip | ipv6 } access-group acl_list_name [ in | out ] [ preference ]
  end
```

**Notes:**

- The context name is the name of the ACL context containing the interface to which the ACL is to be applied.
- The context-level ACL is applied to outgoing packets. This applies to incoming packets also if the flow match criteria fails and forwarded again.

The `in` and `out` keywords are deprecated and are only present for backward compatibility.

Context ACL will be applied in the following cases:

- Outgoing packets to an external source.
- Incoming packets that fail flow match and are forwarded again. In this case, the context ACL applies first and only if it passes are packets forwarded.

        During forwarding, if an ACL rule is added with a destination address as a loopback address, the context ACL is also applied. This is because StarOS handles packets destined to the kernel by going
Applying IP ACLs

through a forwarding lookup for them. To apply ACL rules to incoming packets, the interface ACL must be used instead of the context ACL.

- The ACL to be applied must be configured in the context specified by this command.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Verifying the ACL Configuration in a Context

To verify the ACL configuration:

Step 1 Verify that your ACL lists were applied properly by entering the following command in Exec Mode:

```
[local]host_name# show configuration context context_name
```

`context_name` is the name of the context to which the ACL(s) was/were applied.

The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

```
configure

context context_name

ip access-list acl_name

deny host ip_address

deny ip any host ip_address

exit

ip access-group access_group_name

service-redundancy-protocol

exit

interface interface_name

ip address ip_address/mask

exit

subscriber default

exit

aaa group default

exit

gtpp group default

end
```
Applying an ACL to a RADIUS-based Subscriber

IP ACLs are applied to subscribers via attributes in their profile. The subscriber profile could be configured locally on the system or remotely on a RADIUS server.

To apply an ACL to a RADIUS-based subscriber, use the `Filter-Id` attribute.

For more details on this attribute, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

This section provides information and instructions for applying an ACL to an individual subscriber whose profile is configured locally on the system.

---

**Important:** This section provides the minimum instruction set for applying the ACL list to all traffic within a context. For more information on commands that configure additional parameters and options, refer to the *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to provide access control list facility to subscribers:

1. **Step 1** Apply the configured access control list by following the example configuration in Applying an ACL to an Individual Subscriber.
2. **Step 2** Verify that ACL is applied properly on interface by following the steps in Verifying the ACL Configuration to an Individual Subscriber.
3. **Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode `save configuration` command. For additional information refer to the *Verifying and Saving Your Configuration* chapter.

---

**Applying an ACL to an Individual Subscriber**

To apply the ACL to an individual subscriber, use the following configuration:

```
configure

context acl_ctxt_name [ -noconfirm ]

subscriber name subs_name

{ ip | ipv6 } access-group acl_list_name [ in | out ]

end
```

**Notes:**

- The context name is the name of the ACL context containing the interface to which the ACL is to be applied.
- If neither the `in` nor the `out` keyword is specified, the ACL will be applied to all inbound and outbound packets.
- The ACL to be applied must be configured in the context specified by this command.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.
Verifying the ACL Configuration to an Individual Subscriber

These instructions are used to verify the ACL configuration.

**Step 1**  Verify that your ACL lists were applied properly by entering the following command in Exec Mode:

```
[local]host_name# show configuration context context_name
```

`context_name` is the name of the context containing the subscriber `subs1` to which the ACL(s) was/were applied.

The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

```
configure

context context_name

ip access-list acl_name

deny host ip_address

deny ip any host ip_address
exit

ip access-group access_group_name

service-redundancy-protocol
exit

interface interface

ip address ip_address/mask
exit

subscriber default
exit

subscriber name subscriber_name

ip access-group access_group_name in

ip access-group access_group_name out
exit

aaa group default
exit

gtpp group default
exit
```
Applying a Single ACL to Multiple Subscribers

As mentioned in the previous section, IP ACLs are applied to subscribers via attributes in their profile. The subscriber profile could be configured locally on the system or remotely on a RADIUS server.

The system provides for the configuration of subscriber functions that serve as default values when specific attributes are not contained in the individual subscriber’s profile. The following table describes these functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber named</td>
<td>Within each context, the system creates a subscriber called default. The profile for the subscriber named default provides a configuration template of attribute values for subscribers authenticated in that context. Any subscriber attributes that are not included in a RADIUS-based subscriber profile is configured according to the values for those attributes as defined for the subscriber named default. <strong>NOTE:</strong> The profile for the subscriber named default is not used to provide missing information for subscribers configured locally.</td>
</tr>
<tr>
<td>default subscriber</td>
<td>This command in the PDSN, FA, and HA service Configuration modes specifies a profile from a subscriber named something other than default to use a configuration template of attribute values for subscribers authenticated in that context. This command allows multiple services to draw “default” subscriber information from multiple profiles.</td>
</tr>
</tbody>
</table>

When configured properly, the functions described in the table above could be used to apply an ACL to:

- All subscribers facilitated within a specific context by applying the ACL to the profile of the subscriber named default.
- All subscribers facilitated by specific services by applying the ACL to a subscriber profile and then using the default subscriber command to configure the service to use that subscriber as the “default” profile.

Applying an ACL to the Subscriber Named default

This section provides information and instructions for applying an ACL to the subscriber named default.

**Important:** This section provides the minimum instruction set for applying the ACL list to all traffic within a context. For more information on commands that configure additional parameters and options, refer to Subscriber Configuration Mode Commands in the Command Line Interface Reference.

To configure the system to provide access control list facility to subscribers:

**Step 1** Apply the configured access control list by following the example configuration in Applying an ACL to the Subscriber Named default.
Step 2  Verify that ACL is applied properly on interface by following the steps in Applying an ACL to the Subscriber Named default.

Step 3  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode save configuration command. For additional information refer to the Verifying and Saving Your Configuration chapter.

Applying an ACL to the Subscriber Named default

To apply the ACL to the subscriber named default, use the following configuration:

```
configure

context acl_ctxt_name [ -noconfirm ]

subscriber name subs_name

{ ip | ipv6 } access-group acl_list_name [ in | out ]

end
```

Notes:

- The context name is the name of the ACL context containing the interface to which the ACL is to be applied.
- If neither the in nor the out keyword is specified, the ACL will be applied to all inbound and outbound packets.
- The ACL to be applied must be configured in the context specified by this command.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Verifying the ACL Configuration to the Subscriber Named default

These instructions are used to verify the ACL configuration.

Step 1  Verify that your ACL lists were applied properly by entering the following command in Exec Mode:

```
[local]host_name# show configuration context context_name
```

`context_name` is the name of the context containing the subscriber default to which the ACL(s) was/were applied. The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

```
configure

context context_name

ip access-list acl_name

deny host ip_address

deny ip any host ip_address

exit

ip access-group access_group_name
```
Applying an ACL to Service-specified Default Subscriber

This section provides information and instructions for applying an ACL to the subscriber to be used as the “default” profile by various system services.

Important: This section provides the minimum instruction set for applying the ACL list to all traffic within a context. For more information on commands that configure additional parameters and options, refer to the Subscriber Configuration Mode Commands chapter in the Command Line Interface Reference.

To configure the system to provide access control list facility to subscribers:

Step 1 Apply the configured access control list by following the example configuration in Applying an ACL to Service-specified Default Subscriber.

Step 2 Verify that the ACL is applied properly on interface by following the steps in Verifying the ACL Configuration to Service-specified Default Subscriber.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode save configuration command. For additional information refer to the Verifying and Saving Your Configuration chapter.
Applying an ACL to Service-specified Default Subscriber

To apply the ACL to a service-specified Default subscriber, use the following configuration:

```
configure

context acl_ctxt_name [ -noconfirm ]

{ pdsn-service | fa-service | ha-service } service_name

default subscriber svc_default_subs_name

exit

subscriber name svc_default_subs_name

{ ip | ipv6 } access-group acl_list_name [ in | out ]

end
```

Notes:
- The context name is the name of the ACL context containing the interface to which the ACL is to be applied.
- If neither the `in` nor the `out` keyword is specified, the ACL will be applied to all inbound and outbound packets.
- The ACL to be applied must be configured in the context specified by this command.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Verifying the ACL Configuration to Service-specified Default Subscriber

To verify the ACL configuration.

Step 1  Verify that your ACL lists were applied properly by entering the following command in Exec Mode:

```
[local]host_name# show configuration context context_name
```

`context_name` is the name of the context containing the service with the default subscriber to which the ACL(s) was/were applied.

The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

```
configure

context context_name

ip access-list acl_name

deny host ip_address

deny ip any host ip_address

exit

ip access-group access_group_name
```
Applying an ACL to Multiple Subscriber via APNs

If IP ACLs are applied to subscribers via attributes in their profile, the subscriber profile could be configured locally on the system or remotely on a RADIUS server.

To reduce configuration time, ACLs can alternatively be applied to APN templates for GGSN subscribers. When configured, any subscriber packets facilitated by the APN template would then have the associated ACL applied.

This section provides information and instructions for applying an ACL to an APN template.

Important: This section provides the minimum instruction set for applying the ACL list to all traffic within a context. For more information on commands that configure additional parameters and options, refer to the Subscriber Configuration Mode Commands chapter in the Command Line Interface Reference.

To configure the system to provide access control list facility to subscribers:

Step 1  Apply the configured access control list by following the example configuration in Applying an ACL to Multiple Subscriber via APNs.

Step 2  Verify that ACL is applied properly on interface by following the steps in Verifying the ACL Configuration to APNs.

Step 3  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode save configuration command. For additional information refer to the Verifying and Saving Your Configuration chapter.

Applying an ACL to Multiple Subscriber via APNs

To apply the ACL to multiple subscribers via APN, use the following configuration:

```
configure

context dest_context_name [-noconfirm]
```
Access Control Lists

Applying IP ACLs

VPC-VSM System Administration Guide, StarOS Release 19

```
apn apn_name

   { ip | ipv6 } access-group acl_list_name [ in | out ]

end
```

Notes:
- The ACL to be applied must be in the destination context of the APN (which can be different from the context where the APN is configured).
- If neither the `in` nor the `out` keyword is specified, the ACL will be applied to all inbound and outbound packets.
- Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Verifying the ACL Configuration to APNs

To verify the ACL configuration:

**Step 1** Verify that your ACL lists were applied properly by entering the following command in Exec Mode:

```
show configuration context context_name
```

*context_name* is the name of the context containing the APN *apn1* having *default* subscriber to which the ACL(s) was/were applied.

The output of this command displays the configuration of the entire context. Examine the output for the commands pertaining to interface configuration. The commands display the ACL(s) applied using this procedure.

```
count

   context context_name
       ip access-list acl_name
           deny host ip_address
           deny ip any host ip_address
       exit
   ip access-group access_group_name
   interface interface
       ip address ip_address/mask
       exit
   subscriber default
   exit
apn apn_name
    ip access-group access_group_name in
```
ip access-group access_group_name out
end
Chapter 15
Congestion Control

This chapter describes the Congestion Control feature. It covers the following topics:

- Overview
- Configuring Congestion Control
Overview

Congestion Control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system’s ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds**: Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap (starCongestion) are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

- **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.

- **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

- **Service Congestion Policies**: Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

---

*Important*: This section provides the minimum instruction set for configuring congestion control. Commands that configure additional interface or port properties are provided in Subscriber Configuration Mode in the Command Line Interface Reference. Always refer to the Administration Guides for all of the licensed products running on this platform for additional configuration information with respect to congestion control. Congestion control functionality varies based on product and StarOS version.

For the MME three levels of congestion control thresholds are supported – critical, major and minor. By default only the critical threshold is supported for other products. SNMP traps also support major and minor congestion control thresholds. A set of congestion-action-profile commands allows an operator to establish additional actions to be taken for specific thresholds and threshold levels.
Configuring Congestion Control

To configure Congestion Control functionality:

**Step 1** Configure congestion control thresholds as described in Configuring the Congestion Control Threshold.

**Step 2** Configure service congestion policies as described in Configuring Service Congestion Policies.

**Step 3** Enable redirect overload policies as described in Enabling Congestion Control Redirect Overload Policy.

**Step 4** Configure disconnecting subscribers based on call or inactivity time as described in Disconnecting Subscribers Based on Call or Inactivity Time.

**Step 5** Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Configuring the Congestion Control Threshold

To configure congestion control threshold, apply the following example configuration in the Global Configuration mode of the CLI:

```
configure

congestion-control threshold max-sessions-per-service-utilization percent

congestion-control threshold tolerance percent

end
```

Notes:
- There are numerous threshold parameters. See Global Configuration Mode Commands in the Command Line Interface Reference for more information.
- The tolerance is the percentage under a configured threshold that dictates the point at which the condition is cleared.
- Multiple levels of congestion thresholds – critical, major and minor – are supported for various types of congestion control thresholds. If a threshold level is not specified, the default is critical. Currently, major and minor thresholds are only supported for the MME. The **congestion-action-profile** command under **lte-policy** defines the action to be taken when thresholds are exceeded. See Global Configuration Mode Commands, LTE Policy Configuration Mode Commands and Congestion Action Profile Configuration Mode Commands in the Command Line Interface Reference for more information.
- Repeat this configuration as needed for additional thresholds.

Configuring Service Congestion Policies

To create a congestion control policy, apply the following example configuration in the Global Configuration mode of the CLI:

```
configure
```
Configuring Congestion Control

### Notes:
- When the redirect action occurs for PDSN services, the PDSN responds to the PCF with a reply code of 136, “unknown PDSN address” along with the IP address of an alternate PDSN.
- **redirect** is not available for PDIF. The default action for PDIF is “none.”
- When the redirect action occurs for HA services, the system responds to the FA with a reply code of 136, “unknown home agent address”.
- **redirect** cannot be used in conjunction with GGSN services.
- **redirect** is not available for the Local Mobility Anchor (LMA) service.
- When setting the action to **reject**, the reply code is 130, “insufficient resources”.
- For the GGSN, the reply code is 199, “no resources available”.
- For the SaMOG, MME, **redirect** is not available.
- For the MME, create action profiles for optional major and minor thresholds using the `congestion-action-profile` command under **lte-policy** in the Global Configuration mode.
- For the MME, you can specify `service` as **critical**, **major** or **minor** to set a policy and associate an action-profile for the respective threshold. See **Global Configuration Mode Commands** in the **Command Line Interface Reference** for more information.

### Configuring Overload Reporting on the MME

When an overload condition is detected on an MME and the report-overload keyword is enabled in the **congestion-control policy** command, the system reports the condition to a specified percentage of eNodeBs and proceeds to take the configured action on incoming sessions. To create a congestion control policy with overload reporting, apply the following example configuration:

```plaintext
configure

congestion-control policy mme-service action report-overload reject-new-sessions enodeb-percentage percentage

end
```

### Notes:
- Other overload actions include **permit-emergency-sessions** and **reject-non-emergency-sessions**.

### Enabling Congestion Control Redirect Overload Policy

To create a congestion control policy and configure a redirect overload policy for the service, apply the following example configuration:

```plaintext
configure

congestion-control
```
Congestion Control

Configuring Congestion Control

```context context_name

{service_configuration_mode}

   policy overload redirect address

end
```

Notes:

- **Optional:** If the congestion control policy action was configured to `redirect`, then a redirect overload policy must be configured for the service(s) that are affected.
- There are several service configuration modes that you can configure. See the *Command Line Interface Reference* for a complete list of modes.
- You can set various options for redirection. See the *Command Line Interface Reference* for more information.
- Repeat this configuration example to configure overload policies for additional services configured in the same context.

**Verify the Service Overload Policies**

To verify that the service overload policies were properly configured enter the following command in the Exec Mode:

```
[local]host_name# show service_type name service_name
```

This command lists the entire service configuration. Verify that the information displayed for the “Overload Policy” is accurate.

Repeat this configuration example to configure additional services in other contexts.

**Verify the Congestion Control Configuration**

To verify Congestion Control Configuration enter the following `show` command in the Exec Mode.

```
[local]host_name# show congestion-control configuration
```

The following output is a concise listing of all threshold and policy configurations showing multi-level Critical, Major and Minor threshold parameters:

```
Congestion-control: enabled

Congestion-control Critical threshold parameters

  system cpu utilization:  80%
  service control cpu utilization:  80%
  system memory utilization:  80%
  message queue utilization:  80%
  message queue wait time:  10 seconds
```
Configuring Congestion Control

Port rx utilization: 80%
Port tx utilization: 80%
License utilization: 100%
Max-session-per-service utilization: 100%
Tolerance limit: 10%

Congestion-control Critical threshold parameters

System cpu utilization: 80%
Service control cpu utilization: 80%
System memory utilization: 80%
Message queue utilization: 80%
Message queue wait time: 10 seconds
Port rx utilization: 80%
Port tx utilization: 80%
License utilization: 100%
Max-session-per-service utilization: 100%
Tolerance limit: 10%

Congestion-control Major threshold parameters

System cpu utilization: 0%
Service control cpu utilization: 0%
System memory utilization: 0%
Message queue utilization: 0%
Message queue wait time: 0 seconds
Port rx utilization: 0%
Port tx utilization: 0%
License utilization: 0%
Max-session-per-service utilization: 0%
Tolerance limit: 0%

Congestion-control Minor threshold parameters

System cpu utilization: 0%
service control cpu utilization: 0%
system memory utilization: 0%
message queue utilization: 0%
message queue wait time: 0 seconds
port rx utilization: 0%
port tx utilization: 0%
license utilization: 0%
max-session-per-service utilization: 0%
tolerance limit: 0%
Overload-disconnect: disabled

Overload-disconnect threshold parameters
license utilization: 80%
max-session-per-service utilization: 80%
tolerance: 10%
session disconnect percent: 5%
iterations-per-stage: 8

Congestion-control Policy
pdsn-service: none
hsgw-service: none
ha-service: none
ggsn-service: none
closedrp-service: none
lns-service: none
cscf-service: reject
pdif-service: none
wsg-service: none
pdg-service: none
fng-service: none
sgsn-service: none
mme-service: drop
henbgw-network-service: none
asngw-service: none
asnpc-service: none
phsgw-service: none
phspc-service: none
mipv6ha-service: none
lma-service: none
saegw-service: none
sgw-service: none
pgw-service: none
hnbgw-service: none
pcc-policy-service: none
pcc-quota-service: none
pcc-af-service: none
ipsg-service: none
samog-service: none

The primary threshold to observe is license utilization. This threshold is defaulted to 80%. Overload controls on the system enables the Congestion-control Policy when the system has only 80% of the licenses used. The overload condition will not clear until the utilization drops below the tolerance limit setting. The tolerance limit is defaulted to 10%. If the system goes into overload due to license utilization (threshold at 80%), the overload condition will not clear until the license utilization reaches 70%.

The system may go into overload if threshold settings are set too low and congestion control is enabled. You will need to review all threshold values and become familiar with the settings.

Since the recommendation for license utilization overload threshold is 100%, you should enable a license threshold alarm at 80%. An alarm is then triggered when the license utilization hits 80%. When the congestion-control policy setting is set to drop, the system drops incoming packets containing new session requests.

**Important:** For additional information on configuring the alarm threshold, refer to the Threshold Configuration Guide.

### Verify MME Congestion Action Profiles

To verify MME multilevel congestion action profiles, run the following Exec mode command:
Disabling Subscribers Based on Call or Inactivity Time

During periods of heavy system load, it may be necessary to disconnect subscribers in order to maintain an acceptable level of system performance. You can establish thresholds to select subscribers to disconnect based on the length of time that a call has been connected or inactive.

To enable overload disconnect for the currently selected subscriber, use the following configuration example:

```plaintext
configure
  context context_name
    subscriber name subscriber_name
      default overload-disconnect threshold inactivity-time dur_thresh
      default overload-disconnect threshold connect-time dur_thresh
    end
end
```

To disable the overload disconnect feature for this subscriber, use the following configuration example:

```plaintext
configure
  context context_name
    subscriber subscriber_name
      no overload-disconnect { [threshold inactivity-time] | [threshold connect-time] }
    end
end
```

Notes:
- **overload-disconnect** is not supported for the Call Session Control Function (CSCF) service.
Chapter 16
Routing

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuring basic services on the system. You should select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures described below.

This chapter includes the following sections:

- Routing Policies
- Static Routing
- OSPF Routing
- OSPFv3 Routing
- Equal Cost Multiple Path ECMP
- BGP4 Routing
- Bidirectional Forwarding Detection
- Viewing Routing Information
Routing Policies

This section describes how to configure the elements needed to define routing policies. Routing policies modify and redirect routes to and from the system to satisfy specific network deployment requirements.

Use the following building blocks to configure routing policies:

- **Route Access Lists** – The basic building block of a routing policy. Route access lists filter routes based on a range of IP addresses.
- **IP Prefix Lists** – A more advanced element of a routing policy. An IP Prefix list filters routes based on IP prefixes.
- **AS Path Access Lists** – A basic building block used for Border Gateway Protocol (BGP) routing. These lists filter Autonomous System (AS) paths.
- **Route Maps** – Route-maps provide detailed control over routes during route selection or route advertisement by a routing protocol, and in route redistribution between routing protocols. For this level of control you use IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System paths.

Creating IP Prefix Lists

Use the following configuration example to create IP Prefix Lists:

```
config

   context context_name

   ip prefix-list name list_name { deny | permit } network_address/net_mask
```

Notes:

- Set the IP prefix list to deny, permit or match any prefix.
- IPv4 dotted-decimal and IPv6 colon-separated-hexadecimal addresses are supported.
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Creating Route Access Lists

Use the following procedure to create a Route Access List:

```
config

   context context_name

   route-access-list { extended identifier } { deny | permit } [ ip address
   ip_address ]

   route-access-list named list_name { deny | permit } { ip_address/mask | any
   } [ exact-match ]
```
route-access-list standard identifier { permit | deny } { ip_address wildcard_mask | any | network_address }

Notes:
- A maximum of 64 access lists are supported per context.
- A maximum of 16 entries can defined for each route-access-list.
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Creating AS Path Access Lists

Use the following procedure to create an AS Path Access List:

```
config
  context context_name
  ip as-path access-list list_name [ { deny | permit } reg_expr ]
```

Notes:
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Creating Route Maps

Use the following configuration example to create a Route Map:

```
config
  context context_name
  route-map map_name { deny | permit } seq_number
```

Notes:
- Use the `match` and `set` commands in Route Map Configuration mode to configure the route map. Refer to the Command Line Interface Reference for more information on these commands.
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Sample Configuration

The example below shows a configuration that creates two route access lists, applies them to a route map, and uses that route map for a BGP router neighbor.

```
config
  context isp1
```
route-access-list named RACLin1a permit 88.151.1.0/30
route-access-list named RACLin1a permit 88.151.1.4/30
route-access-list named RACAny permit any

route-map RMnet1 deny 100
    match ip address route-access-list RACLin1a
    #exit
route-map RMnet1 deny 200
    match ip address route-access-list RACLin1b
    #exit

route-map RMnet1 permit 1000
    match ip address route-access-list RACAny
    #exit

router bgp 1
    neighbor 152.20.1.99 as-path 101
    neighbor 152.20.1.99 route-map RMnet1
Static Routing

The system supports static network route configuration on a per context basis. Define network routes by specifying the:

- IP address and mask for the route
- Name of the interface in the current context that the route must use
- Next hop IP address

Adding Static Routes to a Context

To add static routes to a context configuration, you must know the names of the interfaces that are configured in the current context. Use the `show ip interface` command to list the interfaces in the current context (Exec mode). Information for all interfaces configured in the current context is displayed as shown in the following example.

```
[local]host_name# show ip interface
Intf Name: Egress 1
Description:
IP State: Up (Bound to slot/port untagged ifIndex 402718721)
IP Address: 192.168.231.5
Subnet Mask: 255.255.255.0
Bcast Address: 192.168.231.255
MTU: 1500
Resoln Type: ARP       ARP timeout: 3600 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
Total interface count: 1
```

The first line of information for each interface lists the interface name for the current context as shown in the example output. In this example, there is one interface with the name `Egress 1`.

```
config

context context_name

   ip route { ip_address [ ip_mask ] | ip_addr_mask_combo } { next-hop
   next_hop_address | egress_name [ precedence precedence [ cost cost ] }
```

Notes:

- You can configure a maximum of 1,200 static routes per context. Save your configuration as described in the Verifying and Saving Your Configuration chapter.
Deleting Static Routes From a Context

Use the following configuration example to remove static routes from a context’s configuration:

```config
context context_name
  no ip route { ip_address ip_mask | ip_addr_mask_combo } next_hop_address
  egress_name [ precedence precedence ] [ cost cost ]
```

Notes:
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
OSPF Routing

This section gives an overview of Open Shortest Path First (OSPF) routing and its implementation in the system. It also describes how to enable the base OSPF functionality and lists the commands that are available for more complex configurations.

You must purchase and install a license key before you can use this feature. Contact your Cisco account representative for more information on licenses.

**Important:** During system task recovery, it is possible for a dynamically-learned forwarding entry to incorrectly remain in the system forwarding table if that forwarding entry has been removed from the dynamic routing protocol during the recovery.

### OSPF Version 2 Overview

OSPF is a link-state routing protocol that employs an interior gateway protocol (IGP) to route IP packets using the shortest path first based solely on the destination IP address in the IP packet header. OSPF routed IP packets are not encapsulated in any additional protocol headers as they transit the network.

An Autonomous System (AS), or Domain, is defined as a group of networks within a common routing infrastructure. OSPF is a dynamic routing protocol that quickly detects topological changes in the AS (such as router interface failures) and calculates new loop-free routes after a period of convergence. This period of convergence is short and involves a minimum of routing traffic.

In a link-state routing protocol, each router maintains a database, referred to as the link-state database, that describes the Autonomous System's topology. Each participating router has an identical database. Each entry in this database is a particular router's local state (for example, the router's usable interfaces and reachable neighbors). The router distributes its local state throughout the AS by flooding.

All routers run the same algorithm in parallel. From the link-state database, each router constructs a tree of shortest paths with itself as root to each destination in the AS. Externally derived routing information appears on the tree as leaves. The cost of a route is described by a single dimensionless metric.

OSPF allows sets of networks to be grouped together. Such a grouping is called an area. The topology of this area is hidden from the rest of the AS, which enables a significant reduction in routing traffic. Also, routing within the area is determined only by the area’s own topology, lending the area protection from bad routing data. An area is a generalization of an IP subnetted network.

OSPF enables the flexible configuration of IP subnets so that each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different sizes (that is, different masks). This is commonly referred to as variable-length subnetting. A packet is routed to the best (longest or most specific) match. Host routes are considered to be subnets whose masks are “all ones” (0xffffffff).

OSPF traffic can be authenticated or non-authenticated, or can use no authentication, simple/clear text passwords, or MD5-based passwords. This means that only trusted routers can participate in the AS routing. You can specify a variety of authentication schemes and, in fact, you can configure separate authentication schemes for each IP subnet.

Externally derived routing data (for example, routes learned from an exterior protocol such as BGP) is advertised throughout the AS. This externally derived data is kept separate from the OSPF link state data.

Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.
OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations.

**Basic OSPFv2 Configuration**

This section describes how to implement basic OSPF routing.

**Enabling OSPF Routing For a Specific Context**

Use the following configuration example to enable OSPF Routing for a specific context:

```config
context context_name
    router ospf
end
```

**Notes:**
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

**Enabling OSPF Over a Specific Interface**

After you enable OSPF, specify the networks on which it will run. Use the following command to enable OSPF:

```network
network network_ip_address/network_mask area { area_id | area_ip_address }
```

**Important:** The default cost for OSPF on the system is 10. To change the cost, refer to the `ip ospf cost` command in the *Ethernet Interface Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

**Notes:**
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

**Redistributing Routes Into OSPF (Optional)**

Redistributing routes into OSPF means any routes from another protocol that meet specified criteria, such as route type, metric, or rule within a route-map, are redistributed using the OSPFv2 protocol to all OSPF areas. This is an optional configuration.

```config
context context_name
    router ospf
        redistribute { connected | static }
end
```
Notes:
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

### Confirming OSPF Configuration Parameters

To confirm the OSPF router configuration, use the following command and look for the section labeled `router ospf` in the screen output:

```
show config context ctxt_name [ verbose ]
```
OSPFv3 Routing

This section gives an overview of Open Shortest Path First Version 3 (OSPFv3) routing and its implementation in the system. It also describes how to enable the base OSPFv3 functionality and lists the commands that are available for more complex configurations.

OSPFv3 Overview

Much of OSPF version 3 is the same as OSPF version 2. OSPFv3 expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses. OSPFv3 dynamically learns and advertises (reistributes) IPv6 routes within an OSPFv3 routing domain.

In OSPFv3, a routing process does not need to be explicitly created. Enabling OSPFv3 on an interface will cause a routing process and its associated configuration to be created.

Basic OSPFv3 Configuration

This section describes how to implement basic OSPF routing.

Enabling OSPFv3 Routing For a Specific Context

Use the following configuration example to enable OSPF Routing for a specific context:

```
config
  context context_name
    router ospfv3
end
```

Notes:
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Enabling OSPFv3 Over a Specific Interface

After you enable OSPFv3 specify the area in which it will run. Use the following command to enable OSPFv3:

```
area { area_id | area_ip_address } [ default-cost dflt-cost ] [ stub stub-area ]
[ virtual-link vl-neighbor-ipv4address ]
```

**Important:** The default cost for OSPFv3 on the system is 10. To change the cost, refer to the `ipv6 ospf cost` command in the Ethernet Interface Configuration Mode Commands chapter of the Command Line Interface Reference.

Notes:
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.
Redistributing Routes Into OSPFv3 (Optional)

Redistributing routes into OSPFv3 means any routes from another protocol that meet specified criteria, such as route type, metric, or rule within a route-map, are redistributed using the OSPFv3 protocol to all OSPF areas. This is an optional configuration.

```
config

  context context_name

  router ospf3

    redistribute { connected | static }

  end
```

Notes:
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Confirming OSPFv3 Configuration Parameters

To confirm the OSPF router configuration, use the following command and look for the section labeled `router ipv6 ospf` in the screen output:

```
[local]host_name# show config context ctxt_name [ verbose ]
```
Equal Cost Multiple Path (ECMP)

The system supports ECMP for routing protocols. ECMP distributes traffic across multiple routes that have the same cost to lessen the burden on any one route.

The following command configures the maximum number of equal cost paths that can be submitted by a routing protocol:

```
config

context context_name

ip routing maximum-paths [ max_num ]
```

Notes:

- `max_num` is an integer from 1 through 10 (releases prior to 18.2) or 1 through 32 (release 18.2+).
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
BGP-4 Routing

The Border Gateway Protocol 4 (BGP-4) routing protocol is supported through a BGP router process that is implemented at the context level.

The Border Gateway Protocol (BGP) is an inter-AS routing protocol. An Autonomous System (AS) is a set of routers under a single technical administration that use an interior gateway protocol and common metrics to route packets within the AS. The set of routers uses an exterior gateway protocol to route packets to other autonomous systems.

BGP runs over TCP. This eliminates the need for the BGP protocol to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing information. Any authentication scheme used by TCP may be used in addition to BGP’s own authentication mechanisms.

BGP routers exchange network reachability information with other BGP routers. This information builds a picture of AS connectivity from which routes are filtered and AS-level policy decisions are enforced.

BGP-4 provides classless inter-domain routing. This includes support for advertising an IP prefix and eliminates the concept of network class within BGP. BGP-4 also allows the aggregation of routes, including the aggregation of AS paths.

Overview of BGP Support

Mobile devices communicate to the Internet through Home Agents (HAs). HAs assign IP addresses to the mobile node from a configured pool of addresses. These addresses are also advertised to Internet routers through an IP routing protocol to ensure dynamic routing. The BGP-4 protocol is used as a monitoring mechanism between an HA and Internet router with routing to support Interchassis Session Recovery (ICSR). (Refer to Interchassis Session Recovery for more information.).

The objective of BGP-4 protocol support is to satisfy routing requirements and monitor communications with Internet routers. BGP-4 may trigger an active to standby switchover to keep subscriber services from being interrupted.

The following BGP-4 features are supported:

- Exterior Border Gateway Protocol (EBGP) multi-hop
- Route Filtering for inbound and outbound routes
- Route redistribution and route-maps
- Support for BGP communities and extended communities in route maps
- Local preference for IPv4 and IPv6 (IBGP peers)

IP pool routes and loopback routes are advertised in the BGP domain in the following ways:

- Through BGP Configuration Mode redistribution commands, all or some of the connected routes are redistributed into the BGP domain. (IP pool and loopback routes are present in the IP routing table as connected routes.) The network routemap command provides the flexibility to change many BGP attributes.
- Through the BGP Configuration Mode network commands, connected routes are explicitly configured for advertisement into the BGP domain. The network routemap command provides the flexibility to change many BGP attributes. Refer to the Border Gateway Protocol Configuration Mode Commands chapter of the Command Line Interface Reference for details on these commands.
**Important:** If a BGP task restarts because of a processing card failure, a migration, a crash, or the removal of a processing card, all peering session and route information is lost.

### Configuring BGP

This section describes how to configure and enable basic BGP routing support in the system.

```config
context context_name
router bgp AS_number
    neighbor ip_address remote-as AS_num
```

Notes:
- A maximum of 64 BGP peers are supported per context.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

### Redistributing Routes Into BGP (Optional)

Redistributing routes into BGP simply means that any routes from another protocol that meet a specified criterion, such as a route type, or a rule within a route-map, are redistributed through the BGP protocol to all BGP areas. This is an optional configuration.

```config
context context_name
router bgp as_number
    redistribute bgp { bgp | connected | static } [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
```

Notes:
- The redistribution options are connected, ospf, rip, or static. Refer to the *Border Gateway Protocol Configuration Mode Commands* chapter of the *Command Line Interface Reference* for details on the redistribute command.
- A maximum of 64 route-maps are supported per context.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

### BGP Communities and Extended Communities

Route filtering based on a BGP community or extended community (route target) via CLI Route Map Configuration mode commands.
BGP Communities

Configuring a BGP Community

A BGP community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators define to which communities a destination belongs.

You configure a BGP community via a Context Configuration mode command.

```
config

context context_name

ip community-list { named named_list | standard identifier } { deny | permit } { internet | local-AS | no-advertise | no-export | value AS-community_number AS-community_number AS-community_number ...}

{ internet | local-AS | no-advertise | no-export | value AS-community_number AS-community_number AS-community_number ...}

{ internet | local-AS | no-advertise | no-export | value AS-community_number AS-community_number AS-community_number ...}
```

You can permit or deny the following BGP community destinations.

- **internet** – Advertise this route to the internet community, and any router that belongs to it.
- **local-AS** – Use in confederation scenarios to prevent sending packets outside the local autonomous system (AS).
- **no-advertise** – Do not advertise this route to any BGP peer, internal or external.
- **no-export** – Do not advertise to external BGP (eBGP) peers. Keep this route within an AS.
- **value AS-community_number** – Specifies a community string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters).

You can enter multiple destinations and AS community numbers for each community. For additional information, see the Command Line Interface Reference.

Multiple community-list entries can be attached to a community-list by adding multiple permit or deny clauses for various community strings. Up to 64 community-lists can be configured in a context.

Setting the Community Attribute

You set the BGP community attribute via a `set community` command in a route map.

```
config

context context_name

route-map map_name { deny | permit } sequence_number

set community [additive]{ internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ...}

{ internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ... }
```
Routing

{ internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ... }

The additive option allows you to enter multiple destinations and AS community numbers. For additional information, see the Command Line Interface Reference.

Filtering via a BGP Community

To filter routes based on a BGP community, you configure a match clause in a route map. The command sequence follows below.

```plaintext
config
  context context_name
  route-map map_name { deny | permit } sequence_number
  match community { named named_list | standard identifier }
```

BGP Extended Communities

Configuring a BGP Extended Community (Route Target)

A BGP extended community defines a route target. MPLS VPNs use a 64-bit Extended Community attribute called a Route Target (RT). An RT enables distribution of reachability information to the correct information table.

You configure a BGP extended community via a Context Configuration mode command.

```plaintext
config
  context context_name
  ip extcommunity-list { named named_list | standard identifier } { deny | permit } rt rt_number rt_number rt_number ...
```

`rt_number` specifies a Route Target as a string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters). You can add multiple route numbers to an IP extcommunity list.

Multiple extended community-list entries can be attached to an extended community-list by adding multiple permit or deny clauses for various extended community strings. Up to 64 extended community-lists can be configured in a context.

Setting the Extended Community Attribute

You set the BGP extended community attribute via a set extcommunity command in a route map.

```plaintext
config
  context context_name
  route-map map_name { deny | permit } sequence_number
  set extcommunity rt rt_number rt_number rt_number ...
```
rt_number specifies a Route Target as a string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters). You can add multiple route numbers to an IP extcommunity list.

Filtering via a BGP Extended Community

To filter routes based on a BGP extended community (route target), you configure a match clause in a route map. The command sequence follows below.

```
config
  context context_name
  route-map map_name { deny | permit }
  [no] match extcommunity { named named_list | standard identifier }
```

BGP Local Preference

The BGP local preference attribute is sent by BGP speaker only to IBGP peers. It is set in a route map via the following command sequence:

```
config
  context context_name
  route-map map_name { deny | permit }
  set local-preference pref_number
```

There is no match clause corresponding to local preference in the route-map because local-preference is directly used in the route selection algorithm.

ICSR and SRP Groups

BGP is employed with Interchassis Session Recovery (ICSR) configurations linked via Service Redundancy Protocol (SRP). By default an ICSR failover is triggered when all BGP peers within a context are down.

Optionally, you can configure SRP peer groups within a context. ICSR failover would then occur if all peers within a group fail. This option is useful in deployments in which a combination of IPv4 and IPv6 peers are spread across multiple paired VLANs, and IPv4 or IPv6 connectivity is lost by all members of a peer group.

For additional information refer to Interchassis Session Recovery in this guide and the description of the monitor bgp, monitor diameter and monitor authentication-probe commands in the Service Redundancy Protocol Configuration Mode Commands chapter of the Command Line Interface Reference.

Advertising BGP Routes from a Standby ICSR Chassis

An SRP Configuration mode command enables advertising BGP routes from an ICSR chassis in standby state. This command and its keywords allow an operator to take advantage of faster network convergence accrued from deploying BGP Prefix Independent Convergence (PIC) in the Optical Transport Network Generation Next (OTNGN).
BGP PIC is intended to improve network convergence which will safely allow for setting aggressive ICSR failure detection timers.

```plaintext
configure

context context_name

  service-redundancy-protocol

    advertise-routes-in-standby-state [ hold-off-time hold-off-time ] [ reset-bfd-nbhrs bfd-down-time ]

end
```

Notes:

- `hold-off-time hold-off-time` delays advertising the BGP routes until the timer expires. Specify `hold-off-time` in seconds as an integer from 1 to 300.
- After resetting BFD, `reset-bfd-nbhrs bfd-down-time` keeps the BFD sessions down for the configured number of milliseconds to improve network convergence. Specify `bfd-down-time` as an integer from 50 to 120000.

### Configurable BGP Route Advertisement Interval for ICSR

By default, the MinRtAdvInterval is set for each peer with a value of 5 seconds for an iBGP peer and 30 seconds for an eBGP peer. An operator can use the `neighbor identifier advertisement-interval` command to globally change the default interval.

The BGP advertisement-interval can also be separately set for each address family. If configured, this value over-rides the peer's default advertisement-interval for that address-family only. BGP will send route update-message for each AFI/SAFI based on the advertisement-interval configured for that AFI/SAFI. If no AFI/SAFI advertisement-interval is configured, the peer-based default advertisement-interval is used.

In ICSR configurations, this feature can be used to speed route advertisements and improve network convergence times.

The `timers bgp icsr-aggr-advertisement-interval` command is available in both the BGP Address-Family (VPNv4/VPNv6) Configuration and BGP Address-Family (VRF) Configuration modes.

```plaintext
configure

  context context_name

  router bgp as_number

    address-family { ipv4 | ipv6 | vpnv4 | vpnv6 }

      timers bgp icsr-aggr-advertisement-interval seconds
```

Notes:

- `seconds` – sets the number of seconds as an integer from 0 to 30. Default: 0.
Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between two forwarding engines connected by a link. BFD establishes a session between two endpoints over a particular link. If more than one link exists between two systems, multiple BFD sessions may be established to monitor each one of them. The session is established with a three-way handshake, and is torn down the same way. Authentication may be enabled on the session. A choice of simple password, MD5 or SHA1 authentication is available.

Overview of BFD Support

BFD does not have a discovery mechanism; sessions must be explicitly configured between endpoints. BFD may be used on many different underlying transport mechanisms and layers, and operates independently of all of these. Therefore, it needs to be encapsulated by whatever transport it uses.

Protocols that support some form of adjacency setup, such as OSPF or IS-IS, may also be used to bootstrap a BFD session. These protocols may then use BFD to receive faster notification of failing links than would normally be possible using the protocol's own keepalive mechanism.

In asynchronous mode, both endpoints periodically send Hello packets to each other. If a number of those packets are not received, the session is considered down.

When Echo is active, a stream of Echo packets is sent to the other endpoint which then forwards these back to the sender. Echo can be globally enabled via the `bfd-protocol` command, and/or individually enabled/disabled per interface. This function is used to test the forwarding path on the remote system.

The system supports BFD in asynchronous mode with optional Echo capability via static or BGP routing.

Configuring BFD

This section describes how to configure and enable basic BFD routing protocol support in the system.

There are several factors affecting the configuration of BFD protocol:

- Configuring a BFD Context
- Configuring IPv4 BFD for Static Routes
- Configuring IPv6 BFD for Static Routes
- Configuring BFD for Single Hop
- Configuring Multihop BFD
- Scaling of BFD
- Associating BGP Neighbors with the Context
- Associating OSPF Neighbors with the Context
- Associating BFD Neighbor Groups with the BFD Protocol
- Enabling BFD on OSPF Interfaces
- Monitoring BFD Connection for ICSR
Configuring a BFD Context

```
cfg
  context context_name
    bfd-protocol
      [ [no] bfd echo ]
  exit
```

Notes:
- Echo function can be optionally enabled for all interfaces in this context.
- 16 BFD sessions per context and 64 per chassis.

Configuring IPv4 BFD for Static Routes

Enable BFD on an interface.
```
cfg
  context bfd_context_name
    interface if_name
      ip address ipv4_address ipv4_mask
      bfd interval interval_value min_rx rx_value multiplier multiplier_value
      [ [no] bfd echo ]
  exit
```

Configure BFD static route.
```
ip route static bfd if_name ipv4_gw_address
```

Add static routes.
```
ip route ipv4_address ipv4_mask
ip route ipv4_address ipv4_mask
```

Configuring IPv6 BFD for Static Routes

Enable BFD on an Interface
```
cfg
  context bfd_context_name
    interface if_name
```
ipv6 address ipv6_address ipv6_mask

bfd interval interval_value min_rx rx_value multiplier multiplier_value

[ [no] bfd echo ]

exit

Configure BFD static route.

ipv6 route static bfd if_name ipv6_gw_address

Add static routes.

ipv6 route ipv6_address ipv6_mask

ipv6 route ipv6_address ipv6_mask

Configuring BFD for Single Hop

Enable BFD on an interface.

config

context bfd_context_name

interface if_name

ip address ipv4_address ipv4_mask

ipv6 address ipv6_address ipv6_mask

bfd interval interval_value min_rx rx_value multiplier multiplier_value

[ [no] bfd echo ]

exit

Enable BFD on a BGP Neighbor. For additional information, see Associating BGP Neighbors with the Context.

Enable BFD on an OSPF Neighbor. For additional information, see Associating OSPF Neighbors with the Context.

Configuring Multihop BFD

Enable BFD on an interface.

config

context bfd_context_name

interface if_name

ip address ipv4_address ipv4_mask

ipv6 address ipv6_address ipv6_mask
**Bidirectional Forwarding Detection**

```bash
bfd interval interval_value min_rx rx_value multiplier multiplier_value
[ [no] bfd echo ]
exit
```

Configure a Multihop BFD session.

```bash
bfd-protocol
    bfd multihop peer destination-address interval interval-value multiplier multiplier-value
```

Enable BFD on a BGP Neighbor. For additional information, see [Associating BGP Neighbors with the Context](#).

## Scaling of BFD

Configure an active BFD session using one of the above methods and use same BFD neighbor while configuring the active interface. For additional information, see [Associating BFD Neighbor Groups with the BFD Protocol](#).

```bash
bfd-protocol
    bfd nbr-group-name grp_name active-if-name if_name nexthop_address
```

Apply the same BFD results to one or more passive interfaces.

```bash
bfd nbr-group-name grp_name passive-if-name if_name nexthop_address
```

```bash
bfd nbr-group-name grp_name passive-if-name if_name nexthop_address
```

## Associating BGP Neighbors with the Context

```bash
config
    context context_name
    router bgp AS_number
        neighbor neighbor_ip-address remote-as rem_AS_number
        neighbor neighbor_ip-address ebgp-multihop max-hop max_hops
        neighbor neighbor_ip-address update-source update-src_ip-address
        neighbor neighbor_ip-address failover bfd [ multihop ]
```

**Notes:**
- Repeat the sequence to add neighbors.

## Associating OSPF Neighbors with the Context

```bash
config
```
context context_name
router ospf
neighbor neighbor_ip-address

Notes:
- Repeat the sequence to add neighbors.

Associating BFD Neighbor Groups with the BFD Protocol

cfg
context context_name
bfd-protocol
 bfd nbr-group-name grp_name active-if-name if_name nexthop_address
 bfd nbr-group-name grp_name passive-if-name if_name nexthop_address

Enabling BFD on OSPF Interfaces

All OSPF Interfaces

cfg
context context_name
router ospf
 bfd-all-interfaces

Specific OSPF Interface

cfg
context context_name
interface interface_name
 broadcast
 ip ospf bfd

Monitoring BFD Connection for ICSR

For ICSR configurations, the following command sequence initiates monitoring of the connection between the primary chassis and the BFD neighbor in the specified context. If the connection drops, the standby chassis becomes active.

cfg
context context_name

service-redundancy-protocol

monitor bfd context context_name { ipv4_address | ipv6_address } { chassis-to-chassis | chassis-to-router }

Notes:

- ipv4_address | ipv6_address defines the IP address of the BFD neighbor to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation
- chassis-to-chassis enables BFD to run between primary and backup chassis on non-SRP links.
- chassis-to-router enables BFD to run between chassis and router.

Saving the Configuration

Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Chassis-to-Chassis BFD Monitoring for ICSR

An operator can configure BFD to more quickly advertise routes during an ICSR switchover. This solution complements the feature that allows the advertising of BGP routes from a Standby ICSR chassis. The overall goal is to support more aggressive failure detection and recovery in an ICSR configuration when implementing of VoLTE.

You must configure the following features for chassis-to-chassis BFD monitoring in ICSR configurations:

- Enable Primary Chassis BFD Monitoring
- Set BFD to Ignore ICSR Dead Interval
- Configure ICSR Switchover Guard Timer
- Enable BFD Multihop Fallover
- Adjust BFD Interval
- Enable Advertising BGP Routes from Standby ICSR Chassis

Enable Primary Chassis BFD Monitoring

You must enable monitoring of the connection between the primary chassis and specified BFD neighbors. If the connection drops, the standby chassis becomes active. For more information, see Monitoring BFD Connection for ICSR.

Set BFD to Ignore ICSR Dead Interval

The SRP Configuration mode bfd-mon-ignore-dead-interval command causes the standby ICSR chassis to ignore the dead interval and remain in the standby state until all the BFD chassis-to-chassis monitors fail.

Enable this feature in association with BFD chassis-to-chassis monitoring to support more aggressive ICSR failure detection times.
context context_name

service-redundancy-protocol variable

bfd-mon-ignore-dead-interval

end

Configure ICSR Switchover Guard Timer

The SRP Configuration mode guard timer command configures the redundancy-guard-period and monitor-damping-period for SRP service monitoring.

Use these guard timers to ensure that local failures, such as card reboots and task restarts, do not result in ICSR events which can be disruptive.

configure

clear context context_name

service-redundancy-protocol variable

    guard-timer { aaa-switchover-timers { damping-period seconds | guard-period seconds } | diameter-switchover-timers { damping-period seconds | guard-period seconds } | srp-redundancy-timers { aaa { damping-period seconds | guard-period seconds } | bgp { damping-period seconds | guard-period seconds } | diam { damping-period seconds | guard-period seconds } } }

end

Notes:

- **aaa-switchover-timers** – sets timers that prevent back-to-back ICSR switchovers due to an AAA failure (post ICSR switchover) while the network is still converging.
  - **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
  - **guard-period** – configures the local-failure-recovery network-convergence timer.

- **diameter-switchover-timers** – sets timers that prevent a back-to-back ICSR switchover due to a Diameter failure (post ICSR switchover) while the network is still converging.
  - **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
  - **guard-period** – configures the local-failure-recovery network-convergence timer.

- **srp-redundancy-timers** – sets timers that prevent an ICSR switchover while the system is recovering from a local card-reboot/critical-task-restart failure.
  - **aaa** – local failure followed by AAA monitoring failure
  - **bgp** – local failure followed by BGP monitoring failure
  - **diam** – local failure followed by Diameter monitoring failure
Enable BFD Multihop Fall-over

A **fall-over bfd multihop mhsess_name** keyword in the Context Configuration mode ip route and ipv6 route commands enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure.

```configure
context context_name

ip route { ip_address/ip_mask | ip_address ip_mask } { gateway_ip_address | next-hop next_hop_ip_address | point-to-point | tunnel } egress_intrfc_name [ cost cost ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] [ vrf vrf_name [ cost_value ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] ] +
end
```

The **ip route** command now also allows you to add a static multihop BFD route.

```ip route static multihop bfd mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr```

**Important:** SNMP traps are generated when BFD sessions go up and down (BFDsessUp and BFDsessDown).

### ip route Command

```configure
context context_name

ip route { ip_address/ip_mask | ip_address ip_mask } { gateway_ip_address | next-hop next_hop_ip_address | point-to-point | tunnel } egress_intrfc_name [ cost cost ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] [ vrf vrf_name [ cost_value ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] ] +
end
```

The **ip route** command now also allows you to add a static multihop BFD route.

```ip route static multihop bfd mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr```

### ipv6 route Command

```configure
context context_name

ipv6 route ipv6_address/prefix_length { interface name | next-hop ipv6_address interface name } [ cost cost ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] [ vrf vrf_name [ cost_value ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] ]
```
The `ipv6 route` command now also allows you to add a static multihop BFD route.

```bash
ipv6 route static multihop bfd mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr
```

**Adjust BFD Interval**

Set the transmit interval (in milliseconds) between BFD packets to meet the convergence requirements of your network deployment.

```bash
configure
  context context_name
    interface interface_name broadcast
      bfd interval interval_num min_rx milliseconds multiplier value
    end
end
```

Notes:
- `milliseconds` is an integer from 50 through 10000. (Default 50)

**Enable Advertising BGP Routes from Standby ICSR Chassis**

For information on configuring the feature, see Enable Advertising BGP Routes from Standby ICSR Chassis.

**Saving the Configuration**

Save your configuration as described in the Verifying and Saving Your Configuration chapter.
Viewing Routing Information

To view routing information for the current context, run one of the following Exec mode commands:

- **show ip route**: Displays information for IPv4 routes in the current context.
- **show ipv6 route**: Displays information for ipv6 routes in the current context.
- **show ip static**: Displays information only for IPv4 static routes in the current context.
- **show ip ospf**: Displays IPv4 OSPF process summary information in the current context.
- **show ipv6 ospf**: Displays IPv6 OSPFv3 process summary information in the current context.
- **show ip bgp**: Displays IPv4 BGP information.

This example shows sample output of the command, **show ip route**.

```
[local]host_name# show ip route

"*" indicates the Best or Used route.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop</th>
<th>Protocol</th>
<th>Prec</th>
<th>Cost</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>*44.44.44.0/24</td>
<td>208.230.231.50</td>
<td>static</td>
<td>1</td>
<td>0</td>
<td>local1</td>
</tr>
<tr>
<td>*192.168.82.0/24</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>*192.168.83.0/24</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>208.230.231.0/24</td>
<td>0.0.0.0</td>
<td>ospf</td>
<td>110</td>
<td>10</td>
<td>local1</td>
</tr>
<tr>
<td>*208.230.231.0/24</td>
<td>0.0.0.0</td>
<td>connected</td>
<td>0</td>
<td>0</td>
<td>local1</td>
</tr>
</tbody>
</table>

Total route count: 5
```
Chapter 17
VLANs

This chapter provides information on configuring virtual local area networks (VLANs) in support of enhanced or extended services. The SecGW Administration Guide provides examples and procedures for configuration of StarOS services that may utilize VLANs. You should select the configuration example that best meets your service model before using the procedures described below.

This chapter includes the following sections:

- Overview
- VLANs and KVM Hypervisor
- VLANs and StarOS

Important: VLAN – Layer 2 Traffic Management is a Cisco feature that requires a separate license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter.
Overview

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services. They are configured as “tags” on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.

VLANs can be created at the hypervisor and StarOS levels. Where you create the VLAN depends on your specific network requirements.

Depending on the type of packets being processed over the network, the hypervisor performs different VLAN tasks prior to exchanging packets with the StarOS virtual machine (VM).

- **Management packets** – MGMT packets arrive untagged and the hypervisor exchanges these packets with the VM without additional VLAN processing.
- **Access packets** – arrive from the physical network with VLAN tags. The hypervisor removes the VLAN tags before forwarding them to the VM. It retags the packets received from the VM prior to sending them across the physical network.
- **Trunking** – packets arrive and depart across the physical network with VLAN tags. The hypervisor filters the tags before sending tagged packets to the VM for additional processing.

Management, access and trunking packets should be defined in separate contexts and bound to unique interfaces. The hypervisor should be configured to provide the appropriate type of VLAN tagging or filtering based on the packet type.
VLANs and KVM Hypervisor

Network Isolation

NGOS networking stack implementation allows the KVM host to act as a simple layer 2 bridge (that is, an Ethernet switch), a forwarding or NAT router, a stateful firewall, or any combination of those roles.

VLANs versus Bridged Interfaces

In the KVM virtualization scenario, VLAN usage can be seen as an extension to the simple bridge interface sharing. The difference lies in which interface participates in the bridge set. In the standard mode of operation (as seen in the examples in Network port sharing with Ethernet bridges), the physical interfaces (such as eth0, eth1...) are bound to the bridge, which is used by each guest. These interfaces carry unmodified packets coming externally or being generated internally, with or without a VLAN ID tag.

It is possible to filter out every package not carrying a particular VLAN ID by creating subinterfaces. These subinterfaces become part of the VLAN defined by a specific VLAN ID.

Applying this concept to the bridged interface sharing method involves replacing the bound physical interface by a subinterface that is part of a particular VLAN segmentation. This way, every virtual machine guest with interfaces bound to this bridge is part of that particular VLAN. Like in the simple Ethernet bridge environment, the network provided is transparent.

Important: Not all NIC types support VLAN trunking into a bridge, as many filter out VLANs in hardware.

Additional Information

For additional information on configuring VLANs with the KVM hypervisor see the URLs below:

- Configuring 802.1q VLANs –
  http://pic.dhe.ibm.com/infocenter/lnxinfo/v3r0m0/index.jsp?topic=%2Fliaat%2Fliatkvmsconfgvlans.htm
VLANs and StarOS

Creating VLAN Tags via StarOS

Use the following example to create VLANs on a port and bind them to pre-existing interfaces. For information on creating interfaces, refer to the *System Interfaces and Ports* chapter.

```
config
  port ethernet slot/port
    no shutdown
    vlan vlan_tag_ID
    no shutdown
    bind interface interface_name context_name
  end
```

Notes:

- *Optional:* Configure VLAN-subscriber associations. Refer to *Configuring Subscriber VLAN Associations* for more information.
- Repeat this procedure as needed to configure additional VLANs for the port.
- Refer to *VLAN-Related StarOS CLI Commands* and the *Command Line Interface Reference* for additional information.
- Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Verifying the StarOS Port Configuration

Run the following command to verify the port configuration:

```
show port info slot/port
```

An example of this command’s output when at least one VLAN has been configured for the port is shown below:

```
Port: 1/11
  Port Type : Virtual Ethernet
  Role : Service Port
  Description : (None Set)
  Redundancy Mode : Port Mode
  Redundant With : Non-redundant
```
Preferred Port : Non-Revertive
Physical ifIndex : 17432576
Administrative State : Enabled
Configured Duplex : Auto
Configured Speed : Auto
MAC Address : 00-50-56-AB-11-5D
Boxer Interface TAP : port1_10
Link State : Up
Link Duplex : Full
Link Speed : 1000 Mb
Link Aggregation Group : None

Untagged:
Logical ifIndex : 17432577
Operational State : Up, Active

Tagged VLAN: VID 1010
Logical ifIndex : 17432578
VLAN Type : Standard
VLAN Priority : 0
Administrative State : Enabled
Operational State : Up, Active

Number of VLANs : 1

Notes:
- Repeat this sequence as needed to verify additional ports.
- Optional: Configure VLAN-subscriber associations. Refer to Configuring Subscriber VLAN Associations for more information.
- Refer to VLAN-Related StarOS CLI Commands for additional information.
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.
Configuring StarOS Subscriber VLAN Associations

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. This functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

RADIUS Attributes Used

The following RADIUS attributes can be configured within subscriber profiles on the RADIUS server to allow the association of a specific VLAN to the subscriber:

- **SN-Assigned-VLAN-ID**: In the Starent VSA dictionary
- **SN1-Assigned-VLAN-ID**: In the Starent VSA1 dictionary

**Important**: Since the instructions for configuring subscriber profiles differ between RADIUS server applications, this section only describes the individual attributes that can be added to the subscriber profile. Please refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

Configuring Local Subscriber Profiles

Use the configuration example below to configure VLAN associations within local subscriber profiles on the system.

**Important**: These instructions assume that you have already configured subscriber-type VLAN tags according to the instructions provided in Creating VLAN Tags.

```config
context context_name

subscriber name user_name

ip vlan vlan_id

end
```

Verify the Subscriber Profile Configuration

Use the following command to view the configuration for a subscriber profile:

```show subscriber configuration username user_name```

Notes:

- Repeat this command for each subscriber.
- Save your configuration as described in the Verifying and Saving Your Configuration chapter.
VLAN-Related StarOS CLI Commands

VLAN-related features and functions are supported across several CLI command modes. The following tables identify commands associated with configuration and monitoring of VLAN-related functions.

For detailed information regarding the use of the commands listed below, see the Command Line Interface Reference.

Table 11. VLAN-Related Configuration Commands

<table>
<thead>
<tr>
<th>CLI Mode</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| AAA Server Group                | radius attribute nas-ip-address address ip_address nexthop-forwarding-address ip_address vlan vlan_id | Sets the RADIUS client to provide the VLAN ID with the nexthop forwarding address to a system when running in single nexthop gateway mode.  
**Note:** To access the vlan keyword, aaa-large configuration must be enabled via the Global Configuration mode. |
| ACS Charging Action             | ip vlan vlan_id                                                         | Configures the VLAN identifier to be associated with the subscriber traffic in the destination context.                                           |
| Context                         | ip pool pool_name nexthop forwarding address ip_address overlap vlanid vlan_id | When a nexthop forwarding address is configured, the overlap vlanid keyword enables support for overlapping IP address pools and associates the pool with the specified VLAN ID. |
| Context                         | ip routing overlap-pool                                                | Advertises overlap-pool addresses in dynamic routing protocols when overlap pools are configured using VLAN IDs. When enabled, the overlap addresses are added as interface addresses and advertised. |
| Context                         | radius attribute nas-ip-address address ip_address nexthop-forwarding-address ip_address vlan vlan_id | Specifies the VLAN ID to be associated with the next-hop IP address.                                                                 |
| Ethernet Interface              | [no] logical-port-statistics                                           | Enables or disables the collection of logical port (VLAN and NPU) bulk statistics for the first 32 configured Ethernet or PVC interface types. |
| Ethernet Interface              | vlan-map next-hop ipv4_address                                          | Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The vlan-map is associated with a specific interface. |
| Ethernet Port Configuration Mode| vlan vlan_id                                                            | Enters VLAN Configuration mode.                                                                                                          |
| PVC Configuration Mode          | [no] shutdown                                                           | Enables or disables traffic over a specified VLAN. See below.                                                                           |
| Subscriber Configuration Mode    | ip vlan vlan_id                                                         | Configures the subscriber VLAN ID that is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it. |
| VLAN Configuration Mode         | bind interface interface_name context_name                              | Binds a virtual interface and context to support VLAN service.                                                                           |
### VLAN-Related Monitoring Commands

<table>
<thead>
<tr>
<th>CLI Mode</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Mode show commands</td>
<td>clear port slot/port vlan vlan_id</td>
<td>Clears NPU statistics for the port that has a previously configured VLAN ID.</td>
</tr>
<tr>
<td>Exec Mode show commands</td>
<td>show logical-port utilization table vlan { 5-minute</td>
<td>Displays VLAN utilization for a specified collection interval.</td>
</tr>
<tr>
<td></td>
<td>hourly }</td>
<td></td>
</tr>
<tr>
<td>Exec Mode show commands</td>
<td>show port info slot/port vlan vlan_id</td>
<td>Displays NPU counters for a previously configured VLAN ID.</td>
</tr>
</tbody>
</table>
Chapter 18
Session Recovery

With robust failover and redundancy protection, a VPC-VSM instance can quickly recover from hardware and software failures without loss of service.

This chapter describes the Session Recovery feature that provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault.

**Important:** Session Recovery is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *StarOS Management Operations* chapter.

This chapter includes the following sections:

- How Session Recovery Works
- Configuring VPC-VSM to Support Session Recovery
How Session Recovery Works

This section provides an overview of how this feature is implemented and the recovery process.

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within StarOS that prevents a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes within StarOS. These mirrored processes remain in an idle state (standby-mode) wherein they perform no processing, until they may be needed in the event of a software failure (for example, a session manager task aborts).

StarOS spawns new instances of “standby mode” sessions for each active control processor (CP) being used.

There are some situations wherein session recovery may not operate properly. These include:

- Additional software or hardware failures occur during the session recovery operation
- A lack of hardware resources (memory and CPU cores) leaves StarOS unable to support session recovery.

Important: After a session recovery operation, some statistics, such as those collected and maintained on a per task manager basis are in general not recovered.

Session Recovery is available for a SecGW (Security Gateway) running as a VPC-VSM instance (StarOS VM) on an ASR 9000 VSM CPU.

Important: Always refer to the SecGW Administration Guide and StarOS Release Notes for other possible session recovery and Interchassis Session Recovery (ICSR) support limitations.

When session recovery occurs, StarOS reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior.
- A minimal set of subscriber data statistics; required to ensure that accounting information is maintained.
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others.
- The idle time timer is reset to zero and the re-registration timer is reset to its maximum value for HA sessions to provide a more conservative approach to session recovery.

Important: Any partially connected calls are not recovered when a failure occurs.

Important: Failure of critical tasks will result in restarting StarOS. Kernel failures, hypervisor failures or hardware failures will result in the VM restarting or going offline. The use of ICSR between two VPC-VSM instances is the recommended solution for these types of failure.
Configuring VPC-VSM to Support Session Recovery

The following procedures allow you to configure the session recovery feature for either an operational VPC-VSM instance that is currently in-service (able to accept incoming calls) or an instance that is out-of-service (not part of your production network and, therefore, not processing any live subscriber/customer data).

**Important:** The session recovery feature, even when the feature use key is present, is disabled by default in StarOS.

**Important:** Session Recovery must be separately configured for each VPC-VSM instance (StarOS VM) running on VSM CPUs (one VM per CPU, up to four VMs per VSM).

### Enabling Session Recovery

As noted previously, session recovery can be enabled on a VPC-VSM instance that is out-of-service (OOS) and does not yet have any contexts configured, or on an in-service system that is currently capable of processing calls. However, if the instance is in-service, it must be restarted before the session recovery feature takes effect.

### Enabling Session Recovery on an OOS Instance

The following procedure is for a VPC-VSM instance that does not have any contexts configured.

To enable the session recovery feature on an OOS instance, follow the procedure below. This procedure assumes that you begin at the StarOS CLI Exec mode prompt.

**Step 1**  
At the Exec mode prompt, verify that the session recovery feature is enabled with a feature use license by running the `show license info` command.

**Important:** If the current status of the Session Recovery feature is Disabled, you cannot enable this feature until a license key is installed in the instance.

**Step 2**  
Use the following configuration example to enable session recovery.

```
configure
  require session recovery
end
```

**Step 3**  
Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

When started, StarOS enables session recovery, creates all mirrored “standby-mode” tasks, and performs packet processing reservations and other operations automatically.

**Step 4**  
After a VPC-VSM instance has been configured and placed in-service, you should verify its preparedness to support this feature as described in *Viewing Session Recovery Status*. 
Enabling Session Recovery on an In-Service Instance

When enabling session recovery on a VPC-VSM instance that already has a saved configuration, the session recovery commands are automatically placed before any service configuration commands in the configuration file.

To enable the session recovery feature on an in-service instance, follow the procedure below. This procedure assumes that you begin at the StarOS CLI Exec mode prompt.

Step 1 At the Exec mode prompt, verify that the session recovery feature is enabled with a feature use license by running the `show license info` command:

```
show license info
```

**Important**: If the current status of the Session Recovery feature is Disabled, you cannot enable this feature until a license key is installed in the system.

Step 2 Use the following configuration example to enable session recovery.

```
configure

require session recovery

end
```

**Important**: This feature does not take effect until after the VPC-VSM instance has been restarted.

Step 3 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Step 4 Perform a StarOS restart by entering the `reload` command:

The following prompt appears:

```
Are you sure? [Yes|No]:
```

Confirm your desire to perform a StarOS restart by entering `yes`.

When restarted, StarOS enables session recovery and creates all mirrored “standby-mode” tasks and other operations automatically.

Step 5 After StarOS has been restarted, you should verify its preparedness to support this feature as described in Viewing Session Recovery Status.

**Important**: More advanced users may opt to simply insert the `require session recovery` command syntax into an existing configuration file using a text editor or other means, and then applying the configuration file manually. Exercise caution when doing this to ensure that this command is placed among the first few lines of any existing configuration file; it must appear before the creation of any non-local context.

Disabling the Session Recovery Feature

To disable the session recovery feature on a VPC-VSM instance, enter the `no require session recovery` command from the Global Configuration mode prompt.
Important: If this command is issued on an in-service instance, StarOS must be restarted by issuing the \texttt{reload} command.

**Viewing Session Recovery Status**

To determine if a VPC-VSM instance is capable of performing session recovery, when enabled, enter the \texttt{show session recovery status verbose} command from the StarOS CLI Exec mode prompt.

The output of this command should be similar to the examples shown below.

```
[local]host_name# show session recovery status
Session Recovery Status:
  Overall Status : SESSMGR Not Ready For Recovery
  Last Status Update : 1 second ago

[local]host_name# show session recovery status
Session Recovery Status:
  Overall Status : Ready For Recovery
  Last Status Update : 8 seconds ago

[local]host_name# show session recovery status verbose
Session Recovery Status:
  Overall Status : Ready For Recovery
  Last Status Update : 2 seconds ago

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th>--------</th>
<th>--------</th>
<th>--------</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessmgr</td>
<td>active</td>
<td>standby</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>aaamgr</td>
<td>active</td>
<td>standby</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>demux</td>
<td>active</td>
<td>status</td>
<td></td>
</tr>
</tbody>
</table>
```

<table>
<thead>
<tr>
<th>CPU State</th>
<th>Active</th>
<th>Standby</th>
<th>Active</th>
<th>Standby</th>
<th>Active</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1 Active</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Good</td>
</tr>
<tr>
<td>1/2 Active</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Good</td>
</tr>
<tr>
<td>1/3 Active</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>Good</td>
</tr>
<tr>
<td>1/4 Active</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>Good</td>
</tr>
</tbody>
</table>
Viewing Recovered Session Information

To view session state information and any session recovery status, enter the following command:

```
show subscriber debug-info { callid id | msid id | username name }
```

The following example shows the output of this command both before and after a session recovery operation has been performed. The “Redundancy Status” fields in this example have been bold-faced for clarity.

```
username: user1      callid: 01callb1      msid: 0000100003
Card/Cpu: 1/1
Sessmgr Instance: 7
Primary callline:

Redundancy Status: Original Session

<table>
<thead>
<tr>
<th>Checkpoints</th>
<th>Attempts</th>
<th>Success</th>
<th>Last-Attempt</th>
<th>Last-Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full:</td>
<td>69</td>
<td>68</td>
<td>29800ms</td>
<td>29800ms</td>
</tr>
<tr>
<td>Micro:</td>
<td>206</td>
<td>206</td>
<td>20100ms</td>
<td>20100ms</td>
</tr>
</tbody>
</table>

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

```
State                  Event
SMGR_STATE_OPEN        SMGR_EVT_NEWCALL
SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP
SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
```

Data Reorder statistics

```
Total timer expiry:    0     Total flush (tmr expiry):    0
```
Session Recovery

Configuring VPC-VSM to Support Session Recovery

Total no buffers: 0
Total flush (no buffers): 0
Total flush (queue full): 0
Total flush (out of range): 0
Total flush (svc change): 0
Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:

Success: 0
In P 0
Failure (timeout): 0
Failure (no buffers): 0
Failure (other reasons): 0

Redirected Session Entries:

Allowed: 2000
Current: 0
Added: 0
Deleted: 0

Revoked for use by different subscriber: 0

Peer callline:

Redundancy Status: Original Session

<table>
<thead>
<tr>
<th>Checkpoints</th>
<th>Attempts</th>
<th>Success</th>
<th>Last-Attempt</th>
<th>Last-Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full:</td>
<td>0</td>
<td>0</td>
<td>0ms</td>
<td>0ms</td>
</tr>
<tr>
<td>Micro:</td>
<td>0</td>
<td>0</td>
<td>0ms</td>
<td>0ms</td>
</tr>
</tbody>
</table>

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGR_STATE_LINE_CONNECTED</td>
<td>SMGR_EVT_LOWER_LAYER_UP</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_AUTH_REQ</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_AUTH_SUCCESS</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_REQ_SUB_SESSION</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_RSP_SUB_SESSION</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_ADD_SUB_SESSION</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_AUTH_REQ</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_AUTH_SUCCESS</td>
</tr>
<tr>
<td>SMGR_STATE_CONNECTED</td>
<td>SMGR_EVT_AUTH_REQ</td>
</tr>
</tbody>
</table>
Configuring VPC - VSM to Support Session Recovery

SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED  SMGR_EVT_AUTH_SUCCESS

Data Reorder statistics
Total timer expiry: 0  Total flush (tmr expiry): 0
Total no buffers: 0  Total flush (no buffers): 0
Total flush (queue full): 0  Total flush (out of range): 0
Total flush (svc change): 0  Total out-of-seq pkt drop: 0
Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:
Success: 0  In Progress: 0
Failure (timeout): 0  Failure (no buffers): 0
Failure (other reasons): 0

Redirected Session Entries:
Allowed: 2000  Current: 0
Added: 0  Deleted: 0
Revoked for use by different subscriber: 0

Notice that in the example above, where the session has been recovered/recreated, that state events (FSM Event State field) no longer exist. This field is re-populated as new state changes occur.
Chapter 19
Interchassis Session Recovery

This chapter describes how to configure Interchassis Session Recovery (ICSR) and its associated Service Redundancy Protocol (SRP). Refer to the Reverse Route Injection (RRI) chapter of the Security Gateway Administration Guide for High Availability (HA) configuration examples that best match your service model. This section focuses on the ICSR operation and parameter settings in StarOS running in a virtual machine on each VSM CPU.

In the context of an ASR 9000 router, a chassis is an ASR 9000 equipped with Virtualized Service Modules (VSMs). At least one VSM in each chassis is running one or more VPC-VSM instances as virtual machines (VMs). Each VPC-VSM instance is considered to be the server.

**Important:** ICSR is a licensed Cisco feature that requires a separate license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the StarOS Management Operations chapter.

This chapter discusses the following:

- Overview
- ICSR Operation
- ICSR Configuration
- StarOS Updates in an ICSR Configuration

**Important:** An ASR 9000 VSM contains four physical CPUs. Each CPU runs an individual VPC-VSM instance (StarOS VM). ICSR must be separately configured on each instance.
Overview

Instance-to-Instance Communication

VPC-VSM instances configured to support ICSR communicate using periodic Hello messages. These messages are sent by each instance to notify the peer of its current state. The Hello message contains information about the instance such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the instance’s peer. If the standby instance does not receive a Hello message from the active instance within the dead interval, the standby instance transitions to the active state.

In situations where the SRP link goes out of service, a priority scheme is used to determine which instance processes the session. The following priority scheme is used:

- route modifier
- chassis (VPC-VSM instance) priority
- VPC-VSM MAC address

Checkpoint Messages

Checkpoint messages are sent from the active instance to the standby instance. These messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby instance, if that instance were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. There are full checkpoint messages and micro-checkpoint messages.

AAA Monitor

AAA servers are monitored using the authentication probe mechanism. AAA servers are considered Up if the authentication-probe receives a valid response. AAA servers are considered Down when the max-retries count specified in the configuration of the AAA server has been reached. SRP initiates a switchover when none of the configured AAA servers responds to an authentication probe. AAA probing is only performed on the active VSM.

Important: A switchover event caused by an AAA monitoring failure is non-revertible.

If the newly active instance fails to monitor the configured AAA servers, it remains as the active instance until one of the following occurs:

- a manual switchover
- another non-AAA failure event causes StarOS to switchover
- a CLI command is used to clear the AAA failure flag and allow the instance to switch to standby

Maximum Number of sessmgrs

The maximum number of session manager tasks (sessmgrs) supported by a VPC-VSM instance is 32. For ICSR you must run the following command on both the Active and Standby instances:
config

task facility sessmgr max 32

This command limits the number of sessmgrs to 32. The actual number of sessmgrs that are created varies based on the amount of vRAM allocated when the StarOS virtual machine is created.

High Availability for RRI

Interchassis Session Recovery (ICSR) is implemented for Reverse Route Injection (RRI) to ensure that the routes are injected correctly on the appropriate VPC-VSM instance to route the traffic to the correct interface after an ICSR switchover.

ICSR can be implemented for:
- Intrachassis or cluster card-level redundancy
- Interchassis L2 card-level redundancy
- Interchassis L3 card-level redundancy (requires anchor route and HSRP)

**Important:** RRI is mandatory for site-to-site (S2S) StarOS WSG service and optional for remote access service (RAS).

For additional information, see the *Security Gateway Administration Guide*.

HSRP

Chassis-to-chassis redundancy employs Cisco Hot Standby Router Protocol (HSRP) to detect failure in the system and notify other elements of the need to change their HA State. Each VPC-VSM instance receives these notifications via oneP (Connected Apps) communication.

An external HSRP-aware entity switches traffic from the primary to the backup ASR 9000 chassis. All application instances must failover to the backup ASR 9000 chassis.
Each StarOS VM requires a separate oneP connection to the RSP (four oneP connections per VSM). Each StarOS VM is monitored by a separate HSRP link that is established using sub-interfaces. For additional information, see the *Security Gateway Administration Guide*. 
ICSR Operation

This section shows operational flows for ICSR.
The following figure shows an ICSR process flow due to a primary failure.
The following figure shows an ICSR process flow due to a manual switchover.

Figure 5. ICSR Process Flow (Primary Failure)

- **Primary**
  - State = Active

- **Backup**
  - State = Standby

**Pass Hello messages.**

Send session checkpoint message after call duration of 60 seconds

Fails and stops sending hello messages.
  - State = Active

Hello Message
  - State = Standby

Hello Message
  - State = Standby

Hello Message
  - State = Standby

Detections that the primary has not sent a hello within the dead-interval and initiates switchover from the standby to the active state.
  - State = Active

Dead Interval (Default = 60 secs)

Recover and begins sending hello messages.
  - State = Standby

Hello Message
  - State = Standby

Hello Message
  - State = Active

Receives hello message with backup status of active and transitions to the standby state.
  - State = Standby
Figure 6. ICSR Process Flow (Manual Switchover)

- **Primary**
  - State = Active
  - Pass Hello messages every hello interval.
  - User initiates ICSR switchover by shutting down the corresponding HSRP interface.
  - State = Active-Pending-Standby
  - Switchover Request Message initiating switchover
  - Waiting for Peer system to respond to switchover request.
  - State = Active-Pending-Standby
  - Switchover Response Message acknowledging successful switchover to Active state.
  - State = Active
  - Transitions to Standby and updates Route Modifier.
  - State = Standby
  - Begins processing traffic as routing domain converges based on lower route modifier.
  - State = Active
  - Session Subsystem retains all checkpoint data.
  - Session Audit Request
  - Session Audit Response
  - Send Checkpoint data (from newly Active).
  - Session subsystem invalidates old checkpoint data and refreshes with new checkpoints from Active chassis.

- **Backup**
  - State = Standby
  - Send outstanding checkpoints.
  - State = Standby

Switchover complete.
Exchange Hello Messages every hello interval.
ICSR Initialization

When StarOS is simultaneously initialized on each VPC-VSM instance, the instances send Hello messages to their configured peer. The peer sends a response, establishes communication between the instances, and messages are sent that contain configuration information.

During initialization, if both instances are misconfigured in the same mode - both active (primary) or both standby (backup), the instance with the highest priority (lowest number set with the ICSR `priority` command) becomes active and the other instance becomes the standby.

If the instance priorities are the same, StarOS compares the two MAC addresses and the instance with the higher MAC address becomes active. For example, if the instances have MAC addresses of `00-02-43-03-1C-2B` and `00-02-43-03-01-3B`, the last three sets of octets (the first three sets are the vendor code) are compared. In this example, the `03-1C-2B` and `03-01-3B` are compared from left to right. The first pair of octets in both MAC addresses are the same, so the next pairs are compared. Since the `01` is lower than the `1C`, the instance with the MAC address of `00-02-43-03-1C-2B` becomes active and the other instance the standby.

Operation

This section describes how the VPC-VSM instances communicate, maintain subscriber sessions, and perform a switchover.

Communication

If one VPC-VSM instance is in the active state and one in the standby state, they both send Hello messages at each hello interval. Subscriber sessions that exceed the checkpoint session duration are included in checkpoint messages that are sent to the standby instance. The checkpoint message contains subscriber session information so if the active chassis goes out of service, the backup instance becomes active and is able to continue processing the subscriber sessions. Additional checkpoint messages occur at various intervals whenever subscriber session information is updated on the standby instance.

Switchover

If the active VPC-VSM instance goes out of service, the standby instance continues to send Hello messages. If the standby instance does not receive a response to the Hello messages within the dead interval, the standby instance initiates a switchover. During the switchover, the standby instance begins advertising its srp-activated loopback and pool routes into the routing domain. Once the instance becomes active, it continues to process existing AAA services and subscriber sessions that had checkpoint information, and is also able to establish new subscriber sessions.

When the primary instance is back in service, it sends Hello messages to the configured peer. The peer sends a response, establishes communication between the instances, and sends Hello messages that contain configuration information. The primary instance receives an Hello message that shows the backup instance state as active and then transitions to standby. The Hello messages continue to be sent to each peer, and checkpoint information is now sent from the active instance to the standby instance at regular intervals.

When switchover occurs, the session timers are recovered. The access gateway session recovery is recreated with the full lifetime to avoid potential loss of the session and the possibility that a renewal update was lost in the transitional checkpoint update process.
ICSR Configuration

**Important:** The StarOS ICSR configuration must be identical on the primary and backup VPC-VSM instances. If each instance has a different SRP configuration, the session recovery feature does not function and sessions cannot be recovered when the active instance goes out of service.

This section describes how to configure basic ICSR on each VPC-VSM instance. For information on commands that configure additional parameters and options, refer to the Command Line Interface Reference.

The procedures described below assume the following:

- VPC-VSM has been installed and configured as a StarOS VM with core network services on each VSM CPU. For more configuration information and instructions on configuring services, refer to the Reverse Route Injection (RRI) chapter of the Security Gateway Administration Guide.
- In addition, the IP address pools must be srp activated.
- AAA server is installed, configured and accessible by both VSMs. For more information on configuring the AAA server, refer to the AAA Interface Administration and Reference.
- HSRP is configured via the ASR 9000 RP using IOS-XR commands. See the Reverse Route Injection (RRI) chapter of the Security Gateway Administration Guide for more information on configuring HSRP and SecGW high availability.

To configure the ICSR on a primary and/or backup VPC-VSM instance:

**Step 1** Configure the SRP context by applying the example configuration in Configure the SRP Context.

**Step 2** Configure ICSR and OneP/ConnectedApps interfaces by applying the examples in Configure ICSR and OneP/CA Interfaces.

**Step 3** Configure the subscriber to default mode by applying the example in Set Subscriber to Default Mode.

**Step 4** Optional: Disable bulk statistics collection on the standby instance by applying the example configuration in Disable Bulk Statistics Collection on a Standby Instance.

**Step 5** Verify your primary and backup instance configuration by following the steps in Verify the Primary and Backup Configurations.

**Step 6** Configure the periodic audit process by following the procedure in Configure the Subscriber State Management Audit Process.

**Step 7** Save your configuration as described in the Verifying and Saving Your Configuration chapter.

**Configure the SRP Context**

To configure the system to work with ICSR:

**Step 1** Create the SRP context and bind it to the IP address of the primary VPC-VSM instance by applying the example configuration in Creating and Binding the SRP Context.
Step 2 Configure the SRP context with priority, chassis mode, hello interval, dead-interval and peer IP address by applying the example configuration in Configuring SRP Context Parameters.

Step 3 Configure the SRP context with interface parameters (including interface name, IP address and port number) for interchassis communication by applying the example configuration in Configuring the SRP Context Interface Parameters.

Step 4 Verify your SRP context configuration by following the steps in Verifying SRP Configuration.

Step 5 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

Creating and Binding the SRP Context

Use the example below to create the SRP context and bind it to primary chassis IP address:

```bash
configure

context srp_ctxt_name [-noconfirm]

service-redundancy-protocol

bind address ip_address

end
```

Notes:
- ICSR should be configured and maintained in a separate context.
- Be sure to bind the local IP address to the primary instance. When configuring the backup instance, be sure to bind the local IP address to the backup instance.

### Configuring SRP Context Parameters

**Important:** StarOS CLI commands must be executed on both VPC-VSM instances. Log into both instances before continuing. Always make configuration changes on the primary instance first.
Basic Parameters

This configuration assigns a chassis mode and priority, and also configures the redundancy link between the primary and backup chassis:

```plaintext
configure
context srp_ctxt_name
  service-redundancy-protocol
    chassis-mode { primary | backup }
    priority priority
    peer-ip-address ip_address
    hello-interval dur_sec
    dead-interval dead_dur_sec
end
```

Notes:
- ICSR should be configured and maintained in a separate context.
- When assigning the chassis mode on the backup chassis be sure to enter the `backup` keyword.
- The `checkpoint` command sets the amount of time the chassis waits before checkpointing an existing call session. Checkpoints can be set for IMS (VoLTE) and/or non-IMS sessions. The checkpoint is a snapshot of the current application state that can be used to restart its execution in case of failure. The default setting is 60 seconds.
- The `priority` determines which chassis becomes active in the event that both chassis are misconfigured with the same chassis mode; see Chassis Initialization. The higher priority chassis has the lower number. Be sure to assign different priorities to each chassis.
- Enter the IP chassis of the backup chassis as the `peer-ip-address` to the primary chassis. Assign the IP address of the primary chassis as the `peer-ip-address` to the backup chassis.
- The `dead-interval` must be at least three times greater than the `hello-interval`. For example, if the hello interval is 10, the dead interval should be at least 30. System performance is severely impacted if the hello interval and dead interval are not set properly. An optional `delay-interval` command allows you to delay the start dead-interval for an interval following the loading of configuration files.

SRP Redundancy, AAA and Diameter Guard Timers

Guard timers ensure that local failures, such as VM reboots and task restarts, do not result in ICSR events which can be disruptive.

The `guard` timer command configures the redundancy-guard-period and monitor-damping-period for SRP service monitoring.

```plaintext
configure
context context_name
  service-redundancy-protocol variable
```
guard-timer { aaa-switchover-timers { damping-period seconds | guard-period seconds } | diameter-switchover-timers { damping-period seconds | guard-period seconds } | srp-redundancy-timers { aaa { damping-period seconds | guard-period seconds } | bgp { damping-period seconds | guard-period seconds } | diam { damping-period seconds | guard-period seconds } } }

end

Notes:

- **aaa-switchover-timers** – sets timers that prevent back-to-back ICSR switchovers due to an AAA failure (post ICSR switchover) while the network is still converging.
- **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
- **guard-period** – configures the local-failure-recovery network-convergence timer.
- **diameter-switchover-timers** – sets timers that prevent a back-to-back ICSR switchover due to a Diameter failure (post ICSR switchover) while the network is still converging.
- **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
- **guard-period** – configures the local-failure-recovery network-convergence timer.
- **srp-redundancy-timers** – sets timers that prevent an ICSR switchover while the system is recovering from a local card-reboot/critical-task-restart failure.
  - **aaa** – local failure followed by AAA monitoring failure
  - **bgp** – local failure followed by BGP monitoring failure
  - **diam** – local failure followed by Diameter monitoring failure

**DSCP Marking of SRP Messages**

You can enable separate DSCP marking of SRP control and checkpoint messages. The **dscp-marking** command sets DSCP marking values for SRP control and checkpoint (session maintenance) messages.

```
configure
  context context_name
    service-redundancy-protocol
      dscp-marking { control | session } dscp_value
```

Notes:

- **dscp_value** can be:
  - **af11** – Assured Forwarding Class 1 low drop PHB (Per Hop Behavior)
  - **af12** – Assured Forwarding Class 1 medium drop PHB
  - **af13** – Assured Forwarding Class 1 high drop PHB
  - **af21** – Assured Forwarding Class 2 low drop PHB
  - **af22** – Assured Forwarding Class 2 medium drop PHB
Interchassis Session Recovery

ICSR Configuration

VPC - VSM System Administration Guide, StarOS Release 19

% ▀ ▄ 259

- **af23** – Assured Forwarding Class 2 high drop PHB
- **af31** – Assured Forwarding Class 3 low drop PHB
- **af32** – Assured Forwarding Class 3 medium drop PHB
- **af33** – Assured Forwarding Class 3 high drop PHB
- **af41** – Assured Forwarding Class 4 low drop PHB
- **af42** – Assured Forwarding Class 4 medium drop PHB
- **af43** – Assured Forwarding Class 4 high drop PHB
- **be** – Best effort Per-Hop-Behaviour (default)
- **cs1** – Class selector 1 PHB
- **cs2** – Class selector 2 PHB
- **cs3** – Class selector 3 PHB
- **cs4** – Class selector 4 PHB
- **cs5** – Class selector 5 PHB
- **cs6** – Class selector 6 PHB
- **cs7** – Class selector 7 PHB
- **ef** – Expedited Forwarding PHB, for low latency traffic

**Configuring the SRP Context Interface Parameters**

This procedure configures the communication interface with the IP address and port number within the SRP context. This interface supports inter-process communication.

---

**Important:** CLI commands must be executed on both VPC-VSM instances. Log into both instances before continuing. Always make configuration changes on the primary instance first.

---

**Important:** There are only two interfaces available (1/10 and 1/11) for SRP. The SRP interface must be configured as a VLAN (typically on 1/11).

```
configure

context srp_ctxt_name [-noconfirm]

interface srp_if_name

ip-address { ip_address | ip_address/mask } srp-activate

exit

exit

port ethernet slot_num/port_num
```
ICSR Configuration

description string
no shutdown
bind interface local_if_name local_ctxt_name
vlan vlanid
no shutdown
bind interface srp_if_name srp_ctxt_name
end

Configuring NACK Generation for SRP Checkpoint Messaging Failures

Transport (TCP) level re-transmission is supported on the SRP link between ICSR chassis. SRP configuration also supports optional application level checks to ensure checkpoints are received at the Standby chassis. Failed attempts to receive and apply checkpoints send NACK messages to the Active chassis.

When this feature is enabled and the standby chassis sends a NACK in response to the receipt of a micro-checkpoint (MC) that fails to be successfully applied, the standby chassis sends another NACK. The standby chassis will send more NACKs (configurable, default = 3) within a 10-minute window if a macro-checkpoint (FC) is not received. NACKs will continue to be sent and the 10-minute reset until an FC is received and applied, or the configured number of max-responses is reached.

You can also specify the number of times a NACK is sent within the 10-minute window in response to a failed MC or FC (Default = 3).

A nack keyword in the SRP Configuration mode checkpoint session command allows you to enable generation of NACK messages in response to checkpoint message failures on a Standby ICSR chassis.

**Important:** The nack keyword will only appear if a special ICSR optimization feature license has been purchased and installed. Contact your Cisco account representative for assistance.

```
configure
context context_name

service-redundancy-protocol variable

  checkpoint session nack { macro | micro } [ max-response number ]

  no checkpoint session nack { macro | micro }

end
```

Notes:

- **max-response** is the number of times a NACK is sent within the 10-minute window in response to a failed MC or FC expressed as an integer from 0 through 65535 (Default = 3).

A periodic-interval keyword in the SRP Configuration mode checkpoint session command allows you to configure the interval between the sending of macro-checkpoints (FCs) between the active and standby chassis.
Important: The periodic-interval keyword will only appear if a special ICSR optimization feature license has been purchased and installed. Contact your Cisco account representative for assistance.

```plaintext
configure
c
context context_name

service-redundancy-protocol variable

checkpoint session periodic-interval minutes
default checkpoint session periodic-interval
no checkpoint session periodic-interval
end
```

Verifying SRP Configuration

**Step 1**  Verify that your SRP contexts were created and configured properly by entering the `show srp info` command (Exec Mode).

Configure ICSR and OneP/CA Interfaces

Configuring an ICSR Traffic Interface

To enable ICSR SRP traffic to and from the VPC-VSM instances you must configure an ICSR interface in the local context of each instance and bind it to an IP address.

```plaintext
interface icsr_if_name
ip address ip_address mask
exit
port ethernet 1/slot
description string
no shutdown
bind interface icsr_if_name
exit
```

Configuring a OneP/CA Interface

To enable HSRP support between VPC-VSM instances and the ASR 9000 RP you must configure a CA interface in the local context of each instance and bind it to an IP address.
interface ca_if_name
  ip address ip_address mask
  exit
port ethernet 1/slot
  description string
  no shutdown
  bind interface ca_if_name
  exit

Set Subscriber to Default Mode

Use the following example to set the subscriber mode to default.

configure
  context dest_ctxt_name
  subscriber default
  end

Disable Bulk Statistics Collection on a Standby Instance

You can disable the collection of bulk statistics from a VPC-VSM instance when it is in the standby mode of operation.

**Important:** When this feature is enabled and a VPC-VSM instance transitions to standby state, any pending accumulated statistical data is transferred at the first opportunity. After that no additional statistics gathering takes place until the instance comes out of standby state.

Use the following example to disable the bulk statistics collection on a standby VSM.

configure
  bulkstat mode
  no gather-on-standby
  end

Repeat this procedure for both VPC-VSM instances.
Verify the Primary and Backup Configurations

Enter the Exec mode `show configuration` command on both VPC-VSM instances. Verify that both instances have the same SRP configuration information.

Configure the Subscriber State Management Audit Process

This audit ensures that two ICSR peers are synchronized and identifies any discrepancies prior to any scheduled or unscheduled switchover events.

Step 1 Enter the SRP Context mode and enter the `service-redundancy-protocol` command.

Step 2 Enter the `audit daily-start-time` command. Specify the daily start time as an hour and minute. For example, a start time of 06 00 indicates that the audit will begin at 6:00 AM.

Step 3 Enter the `audit periodicity` command. Specify the interval in minutes for generating SRP audit statistics as an integer from 60 through 1440. For example, a periodicity of 90 indicates that SRP audit statistics will be generated every 90 minutes beginning at the specified start time. Default = 60.

A sample configuration sequence appears below.

```
config
context srp
  service-redundancy-protocol
    audit daily-start-time 06 00
    audit periodicity 90
end
```

Save the Configuration

Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Additional Configuration Requirements

When using StarOS ICSR to support a high availability (HA) configuration for a Security Gateway, there are several tasks that must completed using IOS-XP via the ASR 9000 RP. For detailed instructions and sample configurations with ICSR utilized within and across ASR 9000 chassis and VSMs, see the *Reverse Route Insertion (RRI)* chapter of the *Security Gateway Administration Guide*. 
StarOS Updates in an ICSR Configuration

Updating StarOS on an ICSR-configured VPC-VSM instances requires performing an off-line update of each instance while it is standby mode. Traffic disruption is minimal since an active instance will be handling call sessions while the standby instance is being updated.

The general upgrade sequence is as follows:

- Download the StarOS software image and copy/transfer it to a location accessible by both instances.
- Save the currently running configurations on both instances.
- Update the standby backup instance first.
- Initiate an SRP switchover from the active primary instance to make the standby backup instance active. Initiate the switchover by shutting down the HSRP interface being monitored by SRP.
- Update the standby primary instance.
- Initiate an SRP switchover from the active backup instance to make the standby primary instance active. Initiate the switchover by shutting down the HSRP interface being monitored by SRP.

The four-part flowchart below shows a more complete view of all the procedures required to complete the StarOS upgrade process.
Figure 7. ICSR Software Upgrade – Part 1

START Primary
Active

Save Configuration
Copy Build onto Instance
Copy build and Template File onto Instance

START Backup
Standby

Save Configuration
Copy Build onto Instance
Copy build and Template File onto Instance

Fix Problems

Heath Check Passed ?

SRP Check Passed ?

Update Boot Record
Reload

A

B
Figure 8. ICSR Software Upgrade – Part 2

A

Optional: Use TAC-prepared Config scripts.

B

Update Config File

Verify Version

Save Configuration

Fix Problems

No

Heath Check Passed?

Yes

Fix Problems

No

SRP Check Passed?

Yes

Allow Time for Session Synchronization

C

D

Initiate SRP Switchover

VPC-VSM System Administration Guide, StarOS Release 19
Figure 9. ICSR Software Upgrade – Part 3

C

Primary Becomes Standby

Update Boot Record

Reload

Update Config File

Verify Version

Save Configuration

Synchronize File Systems

Heath Check Passed?

No

Fix Problems

Yes

SRP Check Passed?

No

Fix Problems

Yes

Optional: Use TAC-prepared Config scripts.

D

Backup Becomes Active

Optional: Based on network deployment

Fix Problems

AAA Monitor Okay?

No

Yes

E

F
Both ICSR Instances

Log into the StarOS CLI of the primary and backup instances and perform the tasks described below.

Downloading and Transferring the StarOS Build

Step 1 Verify that there is enough free space on the /flash device to accommodate the new operating system image file by entering the following Exec mode command:

```
[local]host_name# directory /flash
```

Step 2 Access to the Cisco support site and download facility is username and password controlled. Download the software image to a network location or local drive from which it can be uploaded to the /flash device.

Step 3 Transfer the new operating system image file to the /flash device using one of the following methods:

Step a Copy the file from a network location or local drive using the `copy` command

```
[local]host_name# copy from_url to_url [-noconfirm]
```
Step b. Transfer the file to the /flash device using an FTP client with access to the system. The FTP client must be configured to transfer the file using binary mode.

Step c. Transfer the file to the /flash device using an SFTP client with access to the system.

Step 4. Verify that the image file was successfully transferred to the /flash device by running the Exec mode the following command:

```
[local]host_name# directory /flash
```

Step 5. Run the show version /flash/image_filename command to verify the build information. For example:

```
local]host_name# show version /flash/image_filename.bin
```

**Standby Backup Instance**

Log into the backup standby chassis and perform the tasks described below.

**Performing Health Checks**

Health checks are a series of Exec mode show commands to determine the readiness of the instance to handle a software update.

Step 1. Run `show card table all |grep unknown`. No output should be displayed.

Step 2. Run `show card table |grep offline`. No output should be displayed.

Step 3. Run `show resources |grep Status`. The output should display “Within acceptable limits”.

Step 4. Run `show alarm outstanding`. Review the output for any issues that may preclude performing the software update.

**Performing SRP Checks**

Service Redundancy Protocol (SRP) checks verify that the mechanism for monitoring ICSR status is operational.

Step 1. Run `show srp monitor all`.

Step 2. Review the output for any issues that may preclude performing the software update.

**Updating the Boot Record**

You must add a new boot stack entry for the recently downloaded software image (.bin) file.

Step 1. Run the Exec mode `show boot` command to verify that there are less than 10 entries in the boot.sys file and that a higher priority entry is available (minimally there is no priority 1 entry in the boot stack).

Step 2. Create a new boot stack entry for the new file group, consisting of the new operating system image file and the currently used CLI configuration file by entering the following Global Configuration command:

```
[local]host_name(config)# boot system priority number image image_url /flash/hostname config cfg_url /flash/hostname
```
Assign the next highest priority to this entry, by using the <N-1> method, wherein you assign a priority number that is one number less than your current highest priority.

If priority 1 is in use, you must renumber the existing entries to ensure that at least that priority is available.

The maximum number of boot stack entries that can be contained in the boot.sys file is 10. If there are already 10 entries in the boot stack, you must delete at least one of these entries (typically, the lowest priority) and, if necessary, renumber some or all of the other entries before proceeding. Use the no boot system priority command to delete a boot stack entry.

For information on using the boot system priority command, refer to the Adding a New Boot Stack Entry section of the StarOS Management Operations chapter.

Reloading StarOS

Reboot StarOS by entering the following command:

```
[local]host_name# reload [-noconfirm]
```

As StarOS reboots, it loads the new .bin software image and its corresponding CLI configuration file using the new boot stack entry configured earlier.

After the system reboots, establish a StarOS CLI session and enter the show version command to verify that the active software version is correct.

Updating the Configuration File

Features in the new operating system may require changes to the configuration file. These changes can be done manually or facilitated by custom scripts prepared by Cisco TAC. Make whatever changes are necessary prior to saving the updated configuration file.

Verifying the Software Version

After StarOS has successfully booted, verify that the new StarOS version is running by executing the Exec mode show version command.

Saving the Configuration File

Use the Exec mode save configuration command to save the currently running configuration to the /flash device and to an off-chassis location (network URL). The off-chassis copy assures that you will have a fallback, loadable configuration file should a problem be encountered.

Completing the Update Process

Repeat the following tasks to complete the upgrade process on the standby secondary instance:

- Performing Health Checks
- Performing SRP Checks
Waiting for Session Synchronization

Allow time for session synchronization to occur between the ICSR chassis before preceding to the next steps.

Step 1  Run the `show session recovery status verbose` command on both chassis. Proceed to the next steps only when no errors are seen in the output of this command.

Step 2  On the standby instance, run `show srp checkpoint statistics |more`.

Step 3  On active instance, run `show subs summary |grep Total`.

Step 4  Compare the number of subscribers on the active instance and the number of Current pre-allocated calls: on the standby instance. They should be similar (within 5%). Allow a few minutes for the instances to complete synchronization.

Primary Instance

Log into the active primary VPC-VSM instance and complete the tasks described below.

Initiating an SRP Switchover

An SRP switchover places the primary instance in standby mode and makes the backup instance active. The secondary instance is now processing sessions with the upgraded software.

Step 1  On the primary instance run the `srp initiate-switchover` command. All existing sessions will be migrated to the backup chassis and it begins servicing new session requests. Allow the switchover process to complete.

Step 2  On the primary instance, run the `show srp info` command. Chassis State should indicate Standby when switchover is complete.

Step 3  On the backup instance, confirm the switchover is complete by running the `show srp info` command. Chassis State should indicate Active when switchover is complete.

Checking AAA Monitor Status on the Newly Active Instance

If your network deployment requires communication with AAA servers, log into the newly active VPC-VSM instance and perform an AAA monitor check. You will be checking for the existence of any SNMP traps that indicate the instance cannot communicate with AAA servers (starSRPAAAUnreachable).

Step 1  Run the Exec mode command `show snmp trap history |grep starSRPAAAUnreachable`.

Step 2  There should be no output for this command, or no very recent SNMP trap notifications (based on the event timestamp).

Step 3  If the active chassis cannot communicate with one or more AAA servers, refer to Checking AAA Monitor Status on the Newly Active Chassis for additional information on how to proceed.

Completing the Software Update

Log into the standby instance and repeat the following tasks to complete the upgrade process on the standby primary instance:

- Updating the Boot Record
- Reloading StarOS
- Updating the Configuration File
- Verifying the Software Version
- Saving the Configuration File
- Performing Health Checks
- Performing SRP Checks
- Waiting for Session Synchronization

### Initiating an SRP Switchover

An SRP switchover places the backup VPC-VSM instance in standby mode and makes the primary instance active. The primary instance is now processing sessions with the upgraded software.

**Step 1** Initiate the switchover by shutting down the HSRP interface being monitored by SRP. All existing sessions will be migrated to the primary instance and it begins servicing new session requests. Allow the switchover process to complete.

**Step 2** On the backup instance, run the `show srp info` command. Chassis State should indicate Standby when switchover is complete.

**Step 3** On the primary instance, confirm the switchover is complete by running the `show srp info` command. Chassis State should indicate Active when switchover is complete.

### Checking AAA Monitor Status

If your network deployment requires communication with AAA servers, check the status of communication with AAA servers as described in [Checking AAA Monitor Status on the Newly Active Chassis](#).

### Making Test Calls

After verifying the VPC-VSM instance state and migrating subscribers, perform new call testing to make sure calls are successful.

### Fallback Procedure

To revert to the previous configuration and software build, perform the following steps as a user with administrative privileges.

**Step 1** Run the Exec mode `show boot` command. The topmost lowest numbered entry of the displayed output should be the new configuration with the new software build. The second topmost entry should be the backup configuration.

**Step 2** Remove the topmost boot entry `<n>`.

```
[local]host_name# config

[local]host_name(config)# no boot system priority n
```
Step 3   Reboot StarOS to load its previous configuration.

   [local]host_name# reload

Step 4   Perform health checks as described in Performing Health Checks.
Chapter 20
Support Data Collector

The Support Data Collector (SDC) is a system feature that allows scheduled collection of process state, counter, event and attribute data that may be useful when troubleshooting problems at an installation site.

This chapter includes the following sections:

- Overview
- Configuring SDC Collection
- Displaying the SDC Collection Configuration
- Collecting and Storing the SDC Information
- Managing Record Collection
- Using SDRs to Diagnose Problems
- SDC CLI Commands
Overview

The task of collecting the support data is performed by a background CLI task called the record collector. The administrator configures the SDC via the CLI with the commands to be executed on a periodic basis. The record collector always runs in the background and checks if there are records to be collected.

When it is time to collect support data, the scheduler executes the configured sequence of CLI commands and stores the results in a gunzipped (.gz) file on the hard-disk. This file is called an SDR (Support Data Record), and represents a snapshot of the overall state of the system at that time.

Technical Assistance Center (TAC) personnel and local administrators can review the SDRs on-line or by transferring them off the system. They may also wish to investigate the collector state information. The figure below shows system tasks that contain state and counter information. Arrows between tasks and processes represent messenger requests and indicate the predominant flow of data.

Figure 11. SDC Tasks and Processes
Configuring SDR Collection

The Support Data Record (SDR) is an ordered set of the CLI support commands' display output that is stored in a stand-alone compressed file. Each CLI support command output is stored in its own record section. The record section is identified by a record section name and its ASCII command syntax. For example, the record section `show_version` would have a CLI command string of “show version”.

The order in which the record section commands appear in the configuration is significant. All of the support record section commands must be configured together as an ordered set. In other words, just specifying one command by itself will result in just that one command output constituting the contents of the entire SDR.

The user may configure a specific set of record sections for the SDR which may or may not include some or all of the default SDR record sections. This configuration is stored in the Global Configuration section of the configuration file. Refer to Configuration Commands (Global Configuration Mode) for more detail on the `support record section` command.
Displaying the SDR Collection Configuration

The `show configuration verbose` command displays the default support record sections, if the user has not specified any support record sections. If the user has configured support record sections, then the `show configuration` command displays user-configured support record sections. The support collection schedule configuration also appears in the `show configuration` output under the Global Configuration section.
Collecting and Storing the SDR Information

At the scheduled time, the Support Data Collector (SDC), if active, runs in the background to collect all the record section commands that have been specified. This information is concatenated as one contiguous output. The output is compressed and stored as a file on disk in the /hd-raid/support/record/ directory.

The periodicity of the SDC is configured by the support collection schedule command under Global Configuration Mode. Once the SDR is stored, the SDC waits the sleep-duration interval specified via the support collection command before collecting another SDR.

Important: The period between SDRs is equal to the configured sleep-duration interval + the time taken to collect the previous record.
Managing Record Collection

The SDRs are stored together in a self-relative set. This self-relative set is called a Support Record Collection. Each individual SDR is identified with a record-id. The record-id of the most recent SDR is always 0 (zero). The next older SDR is record-id 1, and so on, for the number of records in the stored collection. For example, if there are five SDRs, they are identified as SDR-0 through SDR-4.

Figure 12. Support Data Collection Hierarchy

When a new SDR is created, the numbers all increment by one and the newest SDR is given the value of 0. If the total number of records exceeds a configured maximum, then the oldest SDR is deleted.

Using the example above, when the maximum SDR count of 5 is reached, the SDRs continue to be SDR-0 through SDR-4, with the file timestamps indicating that the files are changing over time.
The time interval between collections may vary by several minutes in relation to the specified sleep-duration. This is because the interval specifies the idle time between scheduled collection runs. Since the actual overhead of the collecting process is not included in the scheduled intervals, the time differences between collections includes this non-deterministic amount of time.

**Important:** Using a shorter interval to compensate for this behavior is not recommended, since it will only add to the overhead incurred by the collection process and will ultimately impact the overall system performance. The sleep-duration (idle-time) between scheduled collections is an important component of the “self-throttling” mechanism that should not be circumvented by the user.

The Exec Mode `show support collection` command displays useful information about the Support Data Collector. The output includes information about when the collector last ran, how long it took to run, when it is scheduled to run again, as well as the number of SDRs currently stored, where they are stored, and how much storage space is being used. Refer to `show Commands (Exec Mode)` for more detail about this command.
Using SDRs to Diagnose Problems

The user can compare the SDRs by examining two or more in sequence. These SDRs are dumped out in their CLI-formatted output display. Comparing the display outputs reveals trends and performance or configuration differences that indicate problem areas.

Once specific record sections have been identified as having problematic characteristics, only the CLI `show` commands associated with those sections need be monitored and compared to further isolate the problem areas. In addition, individual SDRs may be transferred via system-supported protocols to remote system, or the current collection may be transferred as a set for later analysis.
SDR CLI Commands

You may use the collected support data records to view support data chronologically. If the default list and sequence of sections is inadequate for system monitoring, you can configure your own set of record section commands that make up a particular support record.

**Important:** Refer to the *SDR CLI Command Strings* appendix for a listing of supported CLI strings (show commands) for record sections. The listing also identifies the CLI strings supported as default record sections. You can obtain the same listing by running the `show support collection definitions` command.

**Important:** You may enter up to 200 SDR CLI strings in a single record section command. If you attempt to add more than 200 CLI strings, an error message appears. You may also receive an error message if the system is unable to parse all of the requested CLI strings because they are too complicated to parse.

After configuring the SDR you then configure the sleep-duration interval between record collections and the number of historical records to be retained before being overwritten. By default, configuring this collection information makes the collector mechanism active (if not already active).

After one or more collection intervals have passed, the SDR data becomes available for analysis. The administrator can then use CLI commands to examine the SDR information to perform root cause analysis and trend analysis based on how the data has changed over time. The administrator may decide to transfer the SDRs off the system to be analyzed remotely, for example, by Cisco TAC.

For complete descriptions of the CLI commands discussed below, refer to the *Command Line Interface Reference*.

**Configuration Commands (Global Configuration Mode)**

**support record**

```
support record section section-name command "command-string" [ section section-name command "command-string" ] ...

no support record [ all | section section_name ]
default support record [ all | section section_name ]
```

The `support record section` command configures a specific record section or set of record sections for a support information output command. The order in which record sections are saved is fixed, regardless of the sequence in which the CLI commands were entered.

For example:

```
[local]host_name(config)# support record section show_context command "show context"
```
If the **support record section** command is not explicitly configured by the user, a default set of record section commands are used. These default record section commands are displayed when you run the **show configuration verbose** command. If support record section commands are explicitly configured, they replace the default commands.

### Important: Refer to the SDR CLI Command Strings appendix for a listing of supported CLI strings (show commands) for record sections. The listing also identifies the CLI strings included in default record sections.

The **no support record** command removes either a specific section of the record definition or all of the sections. If you specify the **default support record** command, the default record section definition of that specified record section is used. If neither the keyword **all** or **section** is specified, all the record section definitions are removed.

#### support collection

```
support collection [ sleep-duration [ hours h | minutes m ] ] [ max-records n ]
nosupport collection
default support collection
```

The **support collection** command modifies and/or enables the support collection process. If support collection has been previously disabled, this command enables the collection activity. If the support collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of SDRs that can be collected and stored.

The **sleep duration** keyword specifies the time interval between the collection of support data. It can be specified in hours or minutes with a default of one hour (60 minutes).

The **max-records** keyword specifies the number of SDRs to store as an integer from 1 to 65535. When this value is exceeded, the new SDR overwrites the oldest SDR. The default value is 168.

### Important: SDR files will be stored in the `/hd-raid/support/records/` directory.

For example:

```
[local]host_name(config)# support collection sleep-duration minute 30 max-records 50
```

Use the **no support collection** command to explicitly disable the collection of the SDRs. If no record section commands are defined, the support data collector mechanism is also effectively disabled.

Use the **default support collection** command to enable the support data collector using the default record sections.

### Exec Mode Commands

#### show support record

```
show support record record-id [ to record-id ] [ section section_name ]
```

The **show support record** command displays a collection of SDRs. The SDRs are displayed in order from lowest record-id to highest record-id.
Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

When a new record is collected it is given a record-id of 0. The previously most recent record is renamed to record-id 1, and so on. The display includes the record-id along with the collection time-stamp.

The record-id variable identifies a single SDR. The to keyword specifies the endpoint record-id when displaying a range of SDRs.

The section keyword displays a particular section of the record.

delete support record

```
delete support record  record-id [ to record-id ]
```

The delete support records command removes an SDR with a specified record-id or all SDRs in the specified range of record-ids.

to support collection

```
show support collection [ definitions ]
```

The show support collection command displays information on SDC activity. It display informations such as the start time of the last scheduled collection, the duration of the last scheduled collection, whether the collection is still in progress, etc. In addition this command lists the currently stored set of SDR record-ids, their respective timestamps, and size of each SDR.

```
[local]host_name# show support collection

Record Collection Enabled : yes
Last Collection Start Time : Monday October 21 06:29:05 PDT 2013
Last Collection End Time : Monday October 21 06:29:09 PDT 2013
Est. Collection Next Start : Monday October 21 07:29:13 PDT 2013 (40 minutes)

Support Data Records at /var/tmp/support-records/

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Size</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>167</td>
<td>sdr.167.gz</td>
<td>42863</td>
<td>Monday October 21 04:40:00 PDT 2013</td>
</tr>
<tr>
<td>166</td>
<td>sdr.166.gz</td>
<td>170425</td>
<td>Monday October 21 05:40:08 PDT 2013</td>
</tr>
</tbody>
</table>

total SDRs 2, total bytes 2132880, time span is last 1 day(s) 1 hour(s)
```

The optional definitions keyword displays the list of default support record section definitions. This is the list of all valid record section definitions. The display also indicates whether the record section is enabled or disabled by default.

```
[local]host_name# show support collection definitions
```
The output of this command reflects the sequence in which record sections will be output, regardless of the sequence in which they may have been entered by the user. Refer to the *SDR CLI Command Strings* appendix for additional information.
Appendix A
Installation Guidelines

This appendix provides guidelines for installing and initially configuring a StarOS VM on each of the four CPUs on an ASR 9000 VSM.

Topics addressed in this appendix include:

- OVA Packaging
- Installation Procedure
- Miscellaneous Procedures
OVA Packaging

Two OVA (Open Virtual Application) packages are available to support four StarOS VMs on a single VSM along with the asynchronous distribution of vCPUs:

- `qvpc-si-asr9k-16cpu.ova` (16 vCPUs, 24GB memory, 3 interfaces, 6GB disk)
- `qvpc-si-asr9k-20cpu.ova` (20 vCPUs, 24GB memory, 3 interfaces, 6GB disk)

Both OVA packages are available in a single tar file named `qvpc-si-asr9k.ova.tar`. 
Installation Procedure

Based on requirements, choose one out of the following two installation procedures:

- **Asynchronous distribution**: This installation assures effective usage of the available resources. In this installation, VM1 and VM2 are created with 16 CPUs, while VM3 and VM4 are created with 20 CPUs, each.

- **Synchronous distribution**: This installation assures the resources are distributed evenly in all the VMs. In this installation, all the 4 VMs are created with 16 CPUs each.

**Important**: All ASR 9000 TenG interfaces (0 to 11) will be distributed among four StarOS VMs. 0 to 2 for the first VM, 3 to 5 for the second VM, 6 to 8 for the third VM, and 9 to 11 for fourth VM.

How to Install StarOS VMs — Asynchronous distribution

**Step 1** Untar the qvpc-si-asr9k.ova.tar file (tar -xf qvpc-si-asr9k.ova.tar) to extract the two OVA packages: qvpc-si-asr9k-16cpu.ova and qvpc-si-asr9k-20cpu.ova.

**Step 2** Copy both OVA packages to the ASR 9000 RSP.

**Step 3** Create the first StarOS VM by installing a virtual service using qvpc-si-asr9k-16cpu.ova on the VSM node. Use the virtual-service install name SecGW1 package /disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0.

**Step 4** After the service is installed, activate the SecGW1 service by configuring three interfaces. See the port mapping table below and RSP virtual-service Sample Configuration.

Start installation of the second VM only after the SecGW1 is activated. This assures proper resource allocation for the second VM.

**Step 5** Create the second VM by using qvpc-si-asr9k-16cpu.ova on the VSM node. Use virtual-service install name SecGW2 package /disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0.

**Step 6** Activate SecGW2 by configuring three of the remaining interfaces. See the port mapping table below and RSP virtual-service Sample Configuration.

**Step 7** After SecGW2 is active, create the third StarOS VM using qvpc-si-asr9k-20cpu.ova on the VSM node. Use virtual-service install name SecGW3 package /disk0:/qvpc-si-asr9k-20cpu.ova node 0/1/CPU0.

**Step 8** Activate SecGW3 by configuring three of the remaining interfaces. See the port mapping table below and RSP virtual-service Sample Configuration.

**Step 9** After SecGW3 is activated, create the fourth VM using qvpc-si-asr9k-20cpu.ova on the VSM node. Use virtual-service install name SecGW4 package /disk0:/qvpc-si-asr9k-20cpu.ova node 0/1/CPU0.

**Step 10** Activate SecGW4 by configuring three of the remaining interfaces. See the port mapping table below and RSP virtual-service Sample Configuration.
Table 13. ASR 9000 TenGig interface to StarOS VM Port Mapping

<table>
<thead>
<tr>
<th>TenG Port</th>
<th>StarOS VM</th>
<th>StarOS VM Port</th>
<th>Application Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGx/y/z/0</td>
<td>SecGW1</td>
<td>1/10</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/1</td>
<td></td>
<td>1/11</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/2</td>
<td></td>
<td>1/1</td>
<td>Management port</td>
</tr>
<tr>
<td>TenGx/y/z/3</td>
<td>SecGW2</td>
<td>1/10</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/4</td>
<td></td>
<td>1/11</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/5</td>
<td></td>
<td>1/1</td>
<td>Management port</td>
</tr>
<tr>
<td>TenGx/y/z/6</td>
<td>SecGW3</td>
<td>1/10</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/7</td>
<td></td>
<td>1/11</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/8</td>
<td></td>
<td>1/1</td>
<td>Management port</td>
</tr>
<tr>
<td>TenGx/y/z/9</td>
<td>SecGW4</td>
<td>1/10</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/10</td>
<td></td>
<td>1/11</td>
<td>Service port</td>
</tr>
<tr>
<td>TenGx/y/z/11</td>
<td></td>
<td>1/1</td>
<td>Management port</td>
</tr>
</tbody>
</table>

RSP virtual-service Sample Configuration

RP/0/RSP0/CPU0:<ASR9K_hostname>#show running-config
<timestamp>
Building configuration...
!! IOS XR Configuration 5.2.2
!! Last configuration change at <timestamp>
!
hostname <ASR9K_hostname>
clock timezone <timezone>
clock <settings>
logging console disable
logging buffered 99999999
telnet vrf default ipv4 server max-servers 4
configuration commit auto-save filename save_config
line console
exec-timeout 35791 0
length 50
session-timeout 0
!
onep
transport type tls localcert onep-tp disable-remotecert-validation
!
virtual-service enable
virtual-service SecGW1
  vnic interface TenGigE0/1/1/0
  vnic interface TenGigE0/1/1/1
  vnic interface TenGigE0/1/1/2
  activate
!
virtual-service SecGW2
  vnic interface TenGigE0/1/1/3
  vnic interface TenGigE0/1/1/4
  vnic interface TenGigE0/1/1/5
  activate
!
virtual-service SecGW3
  vnic interface TenGigE0/1/1/6
  vnic interface TenGigE0/1/1/7
  vnic interface TenGigE0/1/1/8
  activate
!
virtual-service SecGW4
  vnic interface TenGigE0/1/1/9
How to Install StarOS VMs — Synchronous distribution

To support synchronous distribution, use the existing OVA package `qvpc-si-asr9k-16cpu.ova`, available with 16 CPUs, to install all the 4 VMs. There is no change to the virtual-service configuration.

**Step 1** Copy the `qvpc-si-asr9k-16cpu.ova` package to the ASR 9000 RSP.

**Step 2** Create the first StarOS VM by installing a virtual service using `qvpc-si-asr9k-16cpu.ova` on the VSM node. Use the virtual-service install name SecGW1 package `/disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0`.

**Step 3** After the service is installed, activate the SecGW1 service by configuring three interfaces. Start installation of the second VM only after the SecGW1 is activated. This assures proper resource allocation for the second VM.

**Step 4** Create the second VM by using `qvpc-si-asr9k-16cpu.ova` on the VSM node. Use virtual-service install name SecGW2 package `/disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0`.

**Step 5** Activate SecGW2 by configuring three of the remaining interfaces.

**Step 6** After SecGW2 is active, create the third StarOS VM using `qvpc-si-asr9k-16cpu.ova` on the VSM node. Use virtual-service install name SecGW3 package `/disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0`.

**Step 7** Activate SecGW3 by configuring three of the remaining interfaces.

**Step 8** After SecGW3 is activated, create the fourth VM using `qvpc-si-asr9k-16cpu.ova` on the VSM node. Use virtual-service install name SecGW4 package `/disk0:/qvpc-si-asr9k-16cpu.ova node 0/1/CPU0`.

**Step 9** Activate SecGW4 by configuring three of the remaining interfaces.

The rest of the procedure is same as How to Install StarOS VMs — Asynchronous distribution.
Miscellaneous Procedures

How to Uninstall StarOS VMs

Each StarOS VM is installed within single virtual-service. The virtual-service uninstall procedure is described below.

Step 1  In IOS-XR rsp virtual-service config mode, do a no active for the particular service and then commit.

Step 2  Un-configure the virtual-service: no virtual-service <name>.

Step 3  Uninstall the service in exec mode: virtual-service uninstall <name>.

How to Upgrade form the StarOS CLI

Once the StarOS VMs are created, you can initiate an upgrade via the StarOS CLI by upgrading to a new .bin image, unless the image requires a fresh installation of the StarOS VMs. See StarOS Management Operations in this guide for detailed procedures.

Refer to the Release Notes supplied with the code drop for additional information.

How to Upgrade StarOS VMs from RSP

This type of upgrade requires uninstalling and installing the StarOS VMs. This can either be done for each VM sequentially, or by uninstalling all the VMs first. Upgrade requires completing the virtual-service installation procedure for all four StarOS VMs.
Appendix B
Engineering Rules

This appendix provides engineering guidelines for configuring the system to meet network deployment requirements. This appendix consists of the following topics:

- StarOS CLI Session Rules
- VPC Interface and Port Rules
- Context Rules
- Subscriber Rules
- Service Rules
- Access Control List ACL Engineering Rules

**Important:** The Engineering Rules listed in this appendix reflect the maximum capacity of StarOS. The actual limits of VPC running in a VM are governed by the amount of vCPU and vMemory capacity allocated to the instance.
StarOS CLI Session Rules

Multiple StarOS CLI session support is based on the amount of available memory. The Resource Manager reserves enough resources to support a minimum of six CLI sessions at all times. One of the six sessions is further reserved for use exclusively by a CLI session on the vSerial interface.

Additional CLI sessions beyond the pre-reserved limit are permitted if sufficient VPC resources are available. If the Resource Manager is unable to reserve resources for a CLI session beyond those that are pre-reserved, users with administrator-privileges are prompted to create the new CLI session, even without reserved resources.
VPC Interface and Port Rules

The rules discussed in this section pertain to the vNIC Ethernet ports designated via the hypervisor for subscriber traffic.

vNIC Ethernet Ports

- Give all hypervisor-assigned logical interfaces a unique name to differentiate the interface from others in the same context.
- A single virtual port can support multiple hypervisor-assigned logical interfaces when you configure VLAN tags for that port. You can use VLAN tagging to bind a single port to multiple logical interfaces that reside in different contexts.
- Each vNIC port for subscriber traffic may contain up to a maximum of 1,024 VLAN tags (maximum of 4,000 VLANs per VPC chassis).
- All hypervisor-assigned logical interfaces must have a valid IP address and subnet.
- If multi-homing is supported on the network, you can assign all logical interfaces a single primary IP address and up to 16 secondary IP addresses.
- You configure a single StarOS logical (named) interface per context. That named interface can have up to 512 ethernet+ppp+tunnel interfaces.
- Different StarOS contexts can share the same logical (named) interface.
- You can apply a maximum of 256 access control list (ACL) rules to a StarOS logical interface.
- In StarOS all ports are identified by their <slot#/><port#>.

Packet Data Network (PDN) Interface Rules

The following engineering rules apply to the interface to the packet data network (PDN):

- Configure the logical interfaces used to facilitate the PDN interface within the egress context.
- The default is to use a single interface within the egress context to facilitate the PDN interface.
- You can configure multiple interfaces in the egress context by using static routes or dynamic routing protocols.
- You may also configure next-hop default gateways.
Context Rules

- A maximum of 63 contexts may be configured per VPC.
- Interfaces per Context
  - Up to 16 interfaces can be configured within a single context.
  - 512 Ethernet+PPP+tunnel interfaces
  - 32 ipv6ip tunnel interfaces
  - 511 GRE tunnels (2,048 GRE tunnels per chassis)
  - 256 loopback interfaces
- IP Addresses and IP Address Pools
  - Up to 2,000 IPv4 address pools can be configured within a single context (regardless of the number of packet processing cards) with a total system limit of 5,000 IPv4 address pools for all contexts.
  - Up to 256 IPv6 pools can be configured within a single context.
  - There is also a limit of 4,000,000 pool addresses and 32,000,000 static addresses that can be configured per context. Therefore, the number of pools depends on how many addresses are being used and how they are subnetted.
  - Each context supports up to 32,000,000 static IP pool addresses. You can configure a maximum total of 96,000,000 static IP pool addresses per chassis. Each static IP pool can contain up to 500,000 addresses.
  - Each context supports up to 16,000,000 dynamic IP pool addresses. You can configure a maximum total of 32,000,000 dynamic IP pool addresses per chassis. Each dynamic IP pool can contain up to 500,000 addresses.

**Important:** Each address in the pool requires approximately 60 bytes of memory. The amount of memory required, however, depends on a number of factors such as the pool type, and hold-timer usage. Therefore, in order to conserve available memory, you may need to limit the number of pools depending on the number of addresses to be configured and the number of installed application cards.

- The maximum number of simultaneous subscriber sessions is controlled by the installed capacity license for the service(s) supported.
- The maximum number of static address resolution protocol (ARP) entries per context is 128.
- The maximum number of domains per context is 2,048.
- Routes
  - Up to 1,200 static routes per context (48,000 per chassis).
  - 6,000 pool routes per context (6,000 per chassis)
  - 5,000 pool explicit host routes per context (6,000 per chassis)
  - 64 route maps per context
- BGP
  - 16,000 BGP prefixes can be configured per context (64,000 per chassis)
- 64 EBGP peers can be configured per context (512 per chassis)
- 16 IBGP peers per context
- 512 BGP/AAA monitors per context in support of Interchassis Session Recovery (ICSR)

**OSPF**
- 200 OSPF neighbors per chassis
- 10,000 OSPF routes per context (64,000 per chassis)

**VRF (GGSN)**
- 300 virtual routing and forwarding (VRF) tables per context (2,048 VRFs per chassis) [256 VRFs per context with demux functions enabled on the MIO card]
- APN limit is 2,048 per chassis; VRF limits and APN limits should be identical.
- 16,384 IP routes
- 128 AAA servers per context for a default AAA server group. The servers can be configured as accounting, authentication, charging servers, or any combination thereof.
- You can configure up to 800 AAA server groups per context with following limitations:
  - 128 servers per AAA server group (accounting, authentication, charging server, or any combination thereof)
  - 1,600 servers per context in AAA Server group mode (accounting, authentication, charging server, or any combination thereof)
  - 800 NAS-IP address/NAS identifier (one primary and one secondary per server group) per context
- Up to 12 charging gateway functions (CGFs) for GTPP accounting can be configured per context.
- Up to 16 bidirectional forwarding detection (BFD) sessions per context (64 per chassis)

**Important:** Refer to the *Engineering Rules* appendix in your product administration guide for additional information on product-specific operating limits.
Subscriber Rules

The following engineering rules apply to subscribers configured within the system:

- Configure a maximum of 2,048 local subscribers per context.
- You may configure attributes for each local subscriber.
- VPC creates a default subscriber for each context when the context is made. Configure attributes for each default subscriber. If a AAA-based subscriber is missing attributes in the authentication reply message, the default subscriber attributes in the context where the subscriber was authenticated are used.

**Important**: Default is not used when local authentication (for local subscribers) is performed.

- Configure default subscriber templates on a per AAA realm (domain aliases configured within a context) basis.
- Configure default subscriber templates on a per PDSN, FA, or HA service.
- For AAA authenticated subscribers, the selection of local subscriber template to use for setting attributes is in the following order:
  - If the username (NAI) matches any local domain name and the domain name has a local subscriber name configured, that local subscriber template is used.
  - If the first case fails, and if the serving service has a default username configured, that subscriber template is used.
  - If the first two cases fail, the default subscriber template in the AAA context is used.
Service Rules

The following engineering rules apply to services configured within the system:

- Configure a maximum of 256 services (regardless of type) per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may affect overall system performance. Therefore, you should not configure a large number of services unless your application absolutely requires it. Please contact your Cisco service representative for more information.

- The total number of entries per table and per chassis is limited to 256.
- Although you can use service names that are identical to those configured in different contexts on the same system, this is not a good practice. Services with the same name can lead to confusion and difficulty in troubleshooting problems, and make it difficult to understand the output of `show` commands.
Access Control List (ACL) Engineering Rules

The following rules apply to Access Control Lists:

- The maximum number of rules per ACL is 128.
- The maximum number of ACL rules applied per port is 128.
- The maximum number of ACL rules applied per context is 1,024.
- The maximum number of ACL rules per IPSec policy is 1.
- The maximum number of IPSec ACL rules per context is 1,024.
- The maximum number of IPSec ACL rules per crypto map is 8.
- The maximum number of ACLs you can configure per context is limited by the number of rules allowed within each ACL. If each ACL contained the maximum number of rules (128), the maximum number of ACLs per context is 8 (128 X 8 ACLs = 1,024 ACL rules per context).
- The maximum number of ACLs applied to an IP access group is 1, whether it is configured for a port or context. Since the maximum number of IP access groups you can apply to an interface or context is 16, the following calculations apply:
  - For each interface/port: 8 rules per ACL multiplied by 16 IP access groups = 128 (the ACL rules limit per port)
  - For each context: 64 rules per ACL multiplied by 16 IP access groups = 1,024 (the ACL rules limit per context)
Appendix C
StarOS Tasks

This appendix describes system and subsystem tasks running under StarOS on an ASR 5x00 and virtualized platforms. It includes the following sections:

- Overview
- Primary Task Subsystems
- Controllers and Managers
- Subsystem Tasks

**Important**: This appendix is not a comprehensive list of all StarOS tasks. It simply provides general descriptions of the primary tasks and subsystems within StarOS.
Overview

For redundancy, scalability and robust call processing, StarOS supports a series of tasks that perform specific functions. These tasks communicate with each other as needed to share control and data signals. As a result, processes can be distributed across multiple tasks thus reducing the overall work-load on any given task and improving system performance. This distributed design provides fault containment that greatly minimizes the impact to processes or sessions due to a failure.

The Exec mode `show task` command displays snapshots of running processes within StarOS. For detailed information about this command, see the `Command Line Interface Reference` and `Statistics and Counters Reference`.

The following sections describe the primary tasks that are implemented by StarOS:

- Primary Task Subsystems
- Controllers and Managers
Primary Task Subsystems

The individual tasks that run on the CPUs are divided into subsystems. Following is a list of the primary subsystems responsible for call session processing:

- **System Initiation Task (SIT):** This subsystem starts tasks and initializes the system. This includes starting a set of initial tasks at system startup time (static tasks), and starting individual tasks on demand at arbitrary times (dynamic tasks).

- **High Availability Task (HAT):** With the Recovery Control Task (RCT) subsystem, the HAT subsystem maintains the operational state of the system. HAT monitors the various software and hardware components of the system. If there are unusual activities, such as the unexpected termination of another task, the HAT subsystem takes a suitable course of action, such as triggering an event to the RCT subsystem to take corrective action or to report the status. The primary function of the HAT task is to minimize service impacts.

- **Recovery Control Task (RCT):** This subsystem executes a recovery action for any failure that occurs in the system. The RCT subsystem receives signals from the HAT subsystem (and in some cases from the NPU subsystem) and determines what recovery actions are needed.

  The RCT subsystem runs on the active management card and synchronizes the information it contains with the RCT subsystem on the standby management card.

- **Shared Configuration Task (SCT):** This subsystem provides a facility to set, retrieve, and receive notification of system configuration parameters. The SCT is mainly responsible for storing configuration data for the applications that run on the system.

  The SCT subsystem runs only on the active management card and synchronizes the information it contains with the SCT subsystem on the standby management card.

- **Resource Management (RM):** This subsystem assigns resources, such as CPU loading and memory, for every system task upon start-up. The RM subsystem monitors resource use to verify that allocations are as specified. RM also monitors all sessions and communicates with the Session Controller to enforce capacity licensing limits.

- **Virtual Private Network (VPN):** This subsystem manages the administrative and operational aspects of all VPN-related entities in the system. The functions performed by the VPN subsystem include:
  - Creating separate VPN contexts
  - Starting the IP services within a VPN context
  - Managing IP pools and subscriber IP addresses, and distributing the IP flow information within a VPN context.

  All IP operations within StarOS are done within specific VPN contexts. In general, packets are not forwarded across different VPN contexts. The only exception currently is the Session subsystem.

- **Network Processing Unit** (npuctrl/npumgr on ASR 5000; npusim on ASR 5500, and knpusim on VPC-DI and VPC-SI): This subsystem is responsible for the following:
  - Using the database to match address and port numbers to destination tasks for fast-path forwarding of dataframes
  - Receiving and transmitting user data frames to/from various physical interfaces
  - IP forwarding decisions (both unicast and multicast)
  - Per-interface packet filtering
  - Traffic management and traffic engineering
- Passing user data frames to/from packet processing CPUs
- Modifying, adding, or stripping datalink/network layer headers
- Recalculating checksums
- Maintaining statistics
- Managing external Ethernet interfaces

- **Card/Slot/Port (CSP):** Coordinates the events that occur when any card is inserted, locked, unlocked, removed, shutdown, or migrated. CSP also performs auto-discovery and configures ports on a newly-inserted interface card. It determines how interface cards map to packet processing cards.
  
The CSP subsystem runs only on the active management card and synchronizes the information it contains with the SCT subsystem on the standby management card. It is started by the SIT subsystem and monitored by the HAT subsystem.

- **Session Manager (SM):** Performs high-touch processing of mobile subscribers’ packet-oriented data session flows. High-touch user data processing consists of the following:
  - Payload transformation
  - Filtering and scheduling
  - Statistics collection
  - Policing
Controllers and Managers

Many of the primary subsystems are composed of controller tasks called Controllers, and subordinated tasks called Managers.

Controllers serve several purposes:

- Monitor the state of their Managers and allow communication between Managers within the same subsystem.
- Enable inter-subsystem communication since they can communicate with the controllers of other subsystems.
- Mask the distributed nature of the software from the user allowing for ease of management.

Managers manage resources and mappings between resources. In addition, some managers are directly responsible for call processing.

For information about the primary subsystems that are composed of critical, controller, and/or manager tasks, see Subsystem Tasks.
Subsystem Tasks

The following subsections list and briefly describe StarOS tasks for various subsystems:

- System Initiation Subsystem
- High Availability Subsystem
- Resource Manager Subsystem
- Virtual Private Networking Subsystem
- Network Processing Unit Subsystem
- Session Subsystem
- Platform Processes
- Management Processes

System Initiation Subsystem

Table 14. System Initiation Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SITMAIN</td>
<td>System Initiation Task – Main</td>
<td>Initiated at system start-up. Reads and provides startup configuration to other SIT components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starts SITREAP sub-function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains CPU state information.</td>
</tr>
<tr>
<td>SITPARENT</td>
<td>SIT Parent Sub-function</td>
<td>Starts management cards in either active or standby mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Registers tasks with HAT task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notifies CSP task of CPU startup completion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brings up packet processing cards in standby mode.</td>
</tr>
<tr>
<td>SITREAP</td>
<td>SIT Reap Sub-function</td>
<td>Shuts down tasks as required.</td>
</tr>
</tbody>
</table>

High Availability Subsystem

Table 15. High Availability Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
</table>

VPC-VSM System Administration Guide, StarOS Release 19
## StarOS Tasks

### Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hatcpu</td>
<td>High Availability Task CPU</td>
<td>Performs device initialization and control functions based on the CPUs hardware capabilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reports the loss of any task on its CPU to hatsystem sub-function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controls the LEDs on the packet processing cards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initializes and monitors the dedicated hardware on packet processing cards. (ASR 5x00 only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collects CPU monitoring information periodically and reports to the master hatcpu sub-function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reports the loss of any task on its CPU to the master hatcpu sub-function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performs device initialization and control functions because of the CPU’s hardware capabilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reports the loss of any task on its CPU to hatsystem sub-function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controls the LEDs on the management card. (ASR 5x00 only)</td>
</tr>
<tr>
<td>hatsystem</td>
<td>High Availability Task System Controller</td>
<td>Controls all the HAT sub-function tasks in the system. It is initiated on system start-up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initializes system components (such as the Gigabit Ethernet switches and switch fabric).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitors system components such as fans for state changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Triggers actions for redundancy in the event of fault detection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The HAT subsystem on the redundant management card mirrors the HAT subsystem on the active management card.</td>
</tr>
</tbody>
</table>

## Resource Manager Subsystem

### Table 16. Resource Manager (RM) Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmctrl</td>
<td>Resource Manager Controller</td>
<td>Started by the sitparent task on StarOS startup, and monitored by HAT for a failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initializes resources such as CPUs and memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requests updated card status from the CSP subsystem and updates the system card table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communicates with all rmctrls to request their most recent set of resource data.</td>
</tr>
<tr>
<td></td>
<td>Resource Manager</td>
<td>Started by the sitparent task, and monitored by HATs for failures.</td>
</tr>
</tbody>
</table>
### StarOS Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
</table>
| rmctrl | Managers | Initializes the local resource data and local resource scratch space.  
Communicates with the SIT task on the local CPU to get its entire task table and the resources associated with each task.  
Gathers current resource utilization for each task.  
Sends the resource data to the rmctrl task. |

### Virtual Private Networking Subsystem

#### Table 17. Virtual Private Networking (VPN) Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
</table>
| vpnctrl | VPN Controller | Created at system start-up.  
Initiates the VPN Manager for each context.  
Informs the Session Controller task when there are additions or changes to contexts. Only one Session Controller operates at any time.  
Routes context specific operation information to the appropriate VPN Manager.  
Performs VPN Manager recovery and saves all VPN-related configuration information in SCT. |
| vpmgr | VPN Manager | Started by the VPN Controller for each configured context (one is always present for the local context).  
Performs IP address pool and subscriber IP address management.  
Performs all context specific operations including but not limited to: UCM services, IP interfaces, the Address Resolution Protocol (ARP), IP address pool management, slow path forwarding, NPU flows, port Access Control Lists (ACLs), and logging.  
Provides IP interface address information for each context to the Session Controller. |
| bgp | Border Gateway Protocol | Created by the VPN Manager for each context that has enabled the BGP routing protocol (*router bgp* Context Configuration mode CLI command).  
Responsible for learning and redistributing routing information via the BGP protocol.  
Maintains the BGP peering connections.  
Applies any defined BGP routing policy. |
| ospf | Open Shortest Path First | Created by VPN Manager for each context that has enabled the OSPF routing protocol (*router ospf* Context Configuration mode CLI command).  
Responsible for learning and redistributing routing information via the OSPF protocol.  
Maintains the OSPF neighboring relationship.  
Maintains the LSA database. |
### StarOS Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Performs SPF calculations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applies any defined OSPF routing policy.</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First</td>
<td>Created by VPN Manager for each context that has enabled the OSPFv3 routing protocol (router ospfv3 Context Configuration mode CLI command). Responsible for learning and redistributing routing information via the OSPFv3 protocol. Maintains the OSPFv3 neighboring relationship. Maintains the LSA database. Performs OSPFv3 SPF calculations. Applies any defined OSPFv3 routing policy.</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol</td>
<td>Created by VPN Manager for each context that has enabled the RIP routing protocol (router rip Context Configuration mode CLI command). Responsible for learning and redistributing routing information via the RIP protocol. Maintains the RIP database. Sends periodic RIP update messages. Applies any defined RIP routing policy.</td>
</tr>
<tr>
<td>zebos</td>
<td>L2 and L3 Switching</td>
<td>Created by VPN Manager for each context. Maintains the routing table (RIB and FIB) for the context. Performs static routing. Interfaces to the kernel for routing &amp; interface updates. Redistributes routing information to dynamic routing protocols. Calculates nexthop reachability.</td>
</tr>
</tbody>
</table>

### Network Processing Unit Subsystem

#### Table 18. Network Processing Unit (NPU) Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>knpusim</td>
<td>Kernel-based NPU Simulator [VPC-DI, VPC-SI]</td>
<td>Created at StarOS start up. Provides port configuration services to the CSP task. Provides interface binding and forwarding services to the VPN Manager. Provides flow insertion and removal services to Session Manager and AAA Manager tasks.</td>
</tr>
</tbody>
</table>
### StarOS Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>npuctrl</td>
<td>NPU Controller</td>
<td>Provides recovery services to the NPU Controller.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Created at StarOS start-up. Only one NPU Controller operates in the system at any time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitors the state of NPU Managers in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Registers to receive notifications when NPU Manager crashes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controls recovery operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides a centralized location for CLI commands related to NPU Manager state.</td>
</tr>
<tr>
<td>npumgr</td>
<td>NPU Manager</td>
<td>Provides port configuration services to the CSP task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides interface binding and forwarding services to the VPN Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides flow insertion and removal services to Session Manager and AAA Manager tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides recovery services to the NPU Controller.</td>
</tr>
<tr>
<td>npusim</td>
<td>NPU Simulator</td>
<td>Provides port configuration services to the CSP task.</td>
</tr>
<tr>
<td></td>
<td>[ASR 5500]</td>
<td>Provides interface binding and forwarding services to the VPN Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides flow insertion and removal services to Session Manager and AAA Manager tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides recovery services to the NPU Controller.</td>
</tr>
</tbody>
</table>

### Session Subsystem

**Table 19. Session Subsystem Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessctr</td>
<td>Session Controller</td>
<td>Created at StarOS start-up. Only one Session Controller instantiated in the system at any time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acts as the primary point of contact for the Session Subsystem. Since it is aware of the other subsystems running within the system, the Session Controller acts as a proxy for the other components, or tasks, that make up the subsystem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starts, configures, and coordinates the efforts of the Session Processing Subsystem submanagers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Works with Resource Manager to start new Session Managers when all existing Session Managers exceed their capacity.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>sessmgr</td>
<td>Session Manager</td>
<td>Created by the Session Controller. Receives context information from VPN Managers. Distributes IP interface address information to other Session Processing Subsystem sub-managers. Manages Enhanced Charging Service (ECS), Content Filtering and URL Blacklisting services.</td>
</tr>
<tr>
<td>a11mgr</td>
<td>A11 Manager</td>
<td>Created by the Session Controller for each context in which a PDSN service is configured. Receives the R-P sessions from the PCF and distributes them to different Session Manager tasks for load balancing. Maintains a list of current Session Manager tasks to aid in system recovery. The A11 Manager task is also known as the Signaling De-multiplexing task (SDT). With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>aaamgr</td>
<td>Authorization, Authentication, and Accounting (AAA) Manager</td>
<td>Paired with Session Managers. Performs all AAA protocol operations and functions for subscribers and administrative users within the system. Acts as a AAA client to AAA servers. Manages GTP Prime (GTP’) messaging with charging gateway functions (CGFs). Multiple AAA Managers can run on a single CPU and/or can be distributed throughout any CPU present in the system. AAA operations for the CLI are done through a AAA Manager running on the active management card.</td>
</tr>
<tr>
<td>aaaproy</td>
<td>Authorization, Authentication, and Accounting (AAA) Proxy Manager</td>
<td>Starts whenever the Global Configuration mode <code>gtpp single-source</code> command is configured. When GTPPP single-sourcing is enabled, aaaproy generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers.</td>
</tr>
</tbody>
</table>
### StarOS Tasks

#### Subsystem Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaaproxy</td>
<td>Runs on a demux card when session recovery is enabled. If session recovery is not enabled, the Global Configuration mode <code>require demux card</code> command starts aaaproxy on the designated demux card.</td>
<td>Writes CDRs to a file in its VRAM-disk. The enqueued CDRs are then periodically synchronized with a HDD for transfer.</td>
</tr>
<tr>
<td>acsctrl</td>
<td>Active Charging System (ACS) Controller</td>
<td>Active Charging service is defined at the global level and can be utilized through CSS commands from any VPN context. Enable via the Global Configuration mode <code>active-charging service</code> CLI command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reads and writes ACS configuration information into SCT.</td>
</tr>
<tr>
<td>acsmgr</td>
<td>Active Charging System (ACS) Controller</td>
<td>Created by ACS Controller to perform IP session processing for a specific number of flows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active/Standby acsmgr tasks are created when session recovery (SR) is enabled.</td>
</tr>
<tr>
<td>alcapmgr</td>
<td>Access Link Control Application Part Manager</td>
<td>Starts when an ALCAP service configuration is detected. There can be multiple instances of this task for load sharing.</td>
</tr>
<tr>
<td></td>
<td>[ASR 5000 only]</td>
<td>Runs the ALCAP protocol stack and handles the IuCS-over-ATM associations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains AAL2 node entity databases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides nodal functions for IuCS-over-ATM interface on ALCAP protocol.</td>
</tr>
<tr>
<td>cdrmod</td>
<td>Charging Detail Record Module</td>
<td>Responsible for receiving EDR/UDR records from different ACSMGR instances in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Responsible for writing the received EDR/UDR records in files using the configured file naming conventions.</td>
</tr>
<tr>
<td>dgmbmgr</td>
<td>Diameter Gmb interface Application Manager</td>
<td>Provides Multimedia Broadcast/Multicast Service (MBMS) feature support for GGSN. It is instantiated when an MBMS policy CLI is configured in the GGSN Service configuration mode. dgmbmgr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains the MBMS UE and bearer contexts.</td>
</tr>
<tr>
<td>diamproxy</td>
<td>Diameter Proxy</td>
<td>Created by diactrl (which runs as part of vpnctrl) and the number of diamproxy tasks spawned is based on the configuration to use “multiple” or “single” proxies. In instances that a single proxy is configured, only one diamproxy task is spawned for the entire chassis and runs on demux packet processing cards. When multiple proxies are configured, one diamproxy task is run per packet processing card.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Informs applications about any change in the connection status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acts as a pass-through to the messages from application to the Diameter server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Just acts as a forwarding agent (does not maintain any queues).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A single Diameter proxy is used to service multiple Diameter applications.</td>
</tr>
<tr>
<td>egtpemgr</td>
<td>Enhanced GPRS Tunneling Protocol Egress Manager</td>
<td>Created by the Session Controller for each context in which an egtp-service of interface type sgw-egress or MME is configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handles certain EGTP messages from SGW, PGW.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains list of current EGTP sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains list of current Session Manager tasks which aids in session recovery.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handles GTP Echo messaging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>egtpmgr</td>
<td>Enhanced GPRS Tunneling Protocol Ingress Manager</td>
<td>Created by Session Controller for each context in which an egtp-service of interface type sgw-ingress or pgw-ingress is configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receives EGTP sessions from MME/S4 SGSN/SGW and distributes them to different Session Manager tasks for load balancing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains list of current EGTP sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains list of current Session Manager tasks which aids in session recovery.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handles GTP Echo messaging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>gtpcmgr</td>
<td>GPRS Tunneling Protocol Control (GTP-C) Message Manager</td>
<td>Created by the Session Controller for each context in which a GGSN service is configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receives the GTP sessions from the SGSN and distributes them to different Session Manager tasks for load balancing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains a list of current Session Manager tasks to aid in system recovery.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verifies validity of GTPC messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains a list of current GTPC sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handles GTPC Echo messaging to/from SGSN.</td>
</tr>
<tr>
<td>gtpumgr</td>
<td>GPRS Tunneling Protocol User (GTP-U Manager</td>
<td>Created by the Session Controller for each context in which a GTPU service is configured. Supported for both GTPUv0 and GTPUv1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains a list of the GTPU-services available within the context and performs load-balancing (of only Error-Ind) for them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supports GTPU Echo handling.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides Path Failure detection on no response for GTPU echo.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Receives Error-Ind and demuxes it to a particular Session Manager.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Serves as the Default GTPU listener. GTPUMGR will process GTPU packets with invalid TEID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
<td></td>
</tr>
<tr>
<td>hamgr</td>
<td>Home Agent (HA) Manager</td>
<td>Created by the Session Controller for each context in which an HA service is configured.</td>
</tr>
<tr>
<td></td>
<td>Receives Mobile IP sessions from the Foreign Agents (FAs) and distributes them to different Session Manager tasks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintains a list of current Session Manager tasks that aids in system recovery.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Functions as the DemuxMgr – handles all the PMIP signaling packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Functions as the Demuxmgr for MIPv6/MIPv4 HA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
<td></td>
</tr>
<tr>
<td>imsimgr</td>
<td>International Mobile Subscriber Identity Manager for MME</td>
<td>Starts when an MME service configuration is detected. There is only one instance of this task:</td>
</tr>
<tr>
<td></td>
<td>Selects which SessMgr to use for new subscriber sessions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintains and reports MME-related demux statistics on events like Attach by IMSI, Attach by GUTI, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can interact with the following tasks in the system:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Session Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MME Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Session Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
<td></td>
</tr>
<tr>
<td>imsimgr</td>
<td>International Mobile Subscriber Identity Manager for SGSN</td>
<td>Started by the Session Controller.</td>
</tr>
<tr>
<td></td>
<td>Selects SessMgr, when not done by linkmgr or sgtpcmgr tasks, for calls sessions based on IMSI/P-TMSI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Load-balances across SessMgers to select one to which a subscriber will be assigned.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintains records for all subscribers on the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintains mapping between the IMSI/P-TMSI and SessMgers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active demux packet processing card.</td>
<td></td>
</tr>
<tr>
<td>ipsgmgr</td>
<td>IP Services Gateway Manager</td>
<td>Created by the Session Controller.</td>
</tr>
<tr>
<td></td>
<td>In Server mode, acts as a RADIUS server, and supports Proxy functionality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Snoop mode supports snooping RADIUS Accounting messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Load balances requests among different SessMgers.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>l2tpdemux</td>
<td>L2TP Demultiplexor Task</td>
<td>Created by the Session Controller when an LNS service is created. Only one L2TPDemux task is invoked for the entire system. De-multiplexes and forwards new incoming tunnel create requests to L2TPMgrs. Maintains information about current active tunnels in all L2TPMgrs. Load balances requests among L2TPMgrs. With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>l2tpmgr</td>
<td>Layer 2 Tunneling Protocol Manager</td>
<td>Created by the Session Controller for each context in which a LAC or LNS service is configured. Additional managers are created as needed depending on loading. Responsible for all aspects of L2TP processing. Maintains protocol state machines for all L2TP sessions and tunnels. Triggers IPSec encryption for new L2TP tunnels as needed. Works with Session Managers to gracefully bring down tunnels. With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>linkmgr</td>
<td>SS7 Link Manager</td>
<td>Created by the Session Controller when the first SS7RD (routing domain) is activated. Multi-instanted for redundancy and scaling purposes. Provides SS7 and Gb connectivity to the platform. Routes per subscriber signalling across the SS7 (including Lu) and Gb interfaces to the SessMgr.</td>
</tr>
<tr>
<td>magmgr</td>
<td>Mobile Access Gateway (MAG) Manager</td>
<td>Created by the Session Controller when the first MAG service is created in a context. Sends and receives PMIP control messages (PBU/PBA). Adds an NPU flow to receive MIPv6 PBA packets. This flow is identical to the flow used in the HAMgr. Maintains the Binding Update List used to keep track of the mobile node’s bindings. Originates PBU-based on trigger received from the Session Manager during error conditions. Receives PBA and forwards it to Session Manager. Supports debugging facility – “magmgr” and “mobile-ipv6”.</td>
</tr>
<tr>
<td>mmgr</td>
<td>SGSN Master Manager</td>
<td>Created upon provisioning of SS7RDs/SCCP-NWs/etc. The Session Controller provides the initial system configuration which includes a detailed description of each distributed protocol layer, its resources sets, and a list of its service user protocol layers and service provider protocol layers. Runs as a single instance.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mmedemux</td>
<td>Mobility Management</td>
<td>Started as part of MME service creation procedure. There is only one mmedemux in the chassis.</td>
</tr>
<tr>
<td></td>
<td>Entity Demux Manager</td>
<td>Distributes incoming S1-MME SCTP connections to mmemgr tasks in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remains aware of all the active MME services in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>mmemgr</td>
<td>Mobility Management</td>
<td>Starts when an MME service configuration is detected. All mmemgrs will have all the Active MME Services configured and will be identical in configuration and capabilities.</td>
</tr>
<tr>
<td></td>
<td>Entity Manager</td>
<td>Runs the SCTP protocol stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handles the SCTP associations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains TA List.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manage eNodeB databases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides nodal functions for S1-MME protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>pccdemux</td>
<td>Policy and Charging Control</td>
<td>Started as part of PCC service creation procedure. There is only one instance of BindMux MGR in the chassis.</td>
</tr>
<tr>
<td></td>
<td>Bindmux Manager</td>
<td>Handles multiplexing of the sessions across the available pccmgrs along with the session binding functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitors load on pccmgrs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributes incoming IP-CAN connections across pccmgrs in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performs session binding; binds IP-CAN/Gateway session with the AF-Session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensures all messaging for an IMSI across various interfaces is directed towards the selected pccmgr.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remains aware of all the active PCC services in the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active packet processing card.</td>
</tr>
<tr>
<td>pccmgr</td>
<td>Policy and Charging Control</td>
<td>pccmgr is part of a Session Manager instance.</td>
</tr>
<tr>
<td></td>
<td>Bindmux</td>
<td>Handles all PCRF service sessions.</td>
</tr>
</tbody>
</table>

VPC-VSM System Administration Guide, StarOS Release 19
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manager</td>
<td>Interfaces with PCC-Core while processing different events associated with individual subscriber sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintains subscriber information while applying business logic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creates calline and corresponding APN session for each subscriber.</td>
</tr>
<tr>
<td>sGPC</td>
<td>GPR SSGN Tunneling Protocol Control Message Manager</td>
<td>Created by the Session Controller for each VPN context in which an SGSN service is configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terminates Gn/Gp and GTP-U interfaces from peer GGSNs and SGSNs for SGSN Services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terminates GTP-U interfaces from RNCs for IuPS Services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controls standard ports for GTP-C and GTP-U.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes and distributes GTP-traffic received from peers on these ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performs all node level procedures associated with Gn/Gp interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With session recovery (SR) enabled, this demux manager is usually established on one of the CPUs on the first active demux packet processing card.</td>
</tr>
<tr>
<td>srb</td>
<td>Standard Routing Database</td>
<td>Eight srb are created by the Session Controller when Content Filtering in the Enhanced Charging Service is enabled. A minimum of two packet processing cards are required to initiate these eight tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receives the static database from the session controller. Each srb task loads two database volumes (one primary and one secondary). The srb task also stores the static DB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rates and categorizes the URL based on the DB volumes and CSI (Category Set Index) stored on it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performs peer loading in case its peer fails. If both the srb task and its peer fail, the session controller performs the loading.</td>
</tr>
</tbody>
</table>

## Platform Processes

### Table 20. Platform Process Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>afcrl</td>
<td>ASR 5500 Fabric Controller</td>
<td>Responsible for the overall management of the system fabric. Manages the pool of Rendezvous Destinations and coordinates fabric recovery by the afmgr proclets after a fault. A single afcrl instance runs on the active MIO/UMIO only.</td>
</tr>
<tr>
<td>afmgr</td>
<td>ASR 5500 Fabric Manager</td>
<td>Responsible for the management of fabric resources on a particular card. There is one afmgr on every CPU that is responsible for one or more fabric access processors (FAPs) or fabric elements (FEs). afmgr supports recovery but not migration.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>afio</td>
<td>ASR 5500 Fabric I/O Driver</td>
<td>Responsible for the direct configuration of the fabric chipset. afio supports non-messenger interprocess communication (IPC) with the local afmgr and with other local afio instances</td>
</tr>
<tr>
<td>connproxy</td>
<td>TCP/SCTP Connection proxy</td>
<td>Allows applications on any card to share the same TCP/SCTP connection to the same remote endpoint instead of opening a new connection for each application on the card.</td>
</tr>
<tr>
<td>cspctrl</td>
<td>Card-Slot-Port Controller</td>
<td>Manages physical chassis components.</td>
</tr>
<tr>
<td>cssctrl</td>
<td>Content Server Selection (CSS) Controller</td>
<td>Maintains all global CSS properties which include a list of CSS servers that can be bound to a service in a context.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSS defines how traffic will be handled based on the “content” of the data presented by or sent to a mobile subscriber. CSS encompasses features such as load balancing, NAT, HTTP redirection, DNS redirection. The content server (services) can be either external to the platform or integrated within the platform. External CSS servers are configured via the Context Configuration mode <code>css server</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The CSS Controller does not create CSS Managers. CSS Managers are stopped and started by VPN Managers. A CSS Manager is automatically created for each context.</td>
</tr>
<tr>
<td>cssmgr</td>
<td>Content Server Selection (CSS) Manager</td>
<td>Spawned by the VPN Manager within a StarOS context.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manages the keepalives to a CSS server within the specific VPN context.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fetches the CSS related information for a subscriber</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a CSS server goes down, the cssmgr task reprograms the NPUs to by-pass the service or redistribute the data among the rest of the servers in the service.</td>
</tr>
<tr>
<td>dcardctrl</td>
<td>Daughter Card Controller</td>
<td>Spawns daughter card managers during system initialization and monitors daughter card managers during system steady state execution. It also spawns daughter card managers whenever a daughter card manager task fails.</td>
</tr>
<tr>
<td>dcardmgr</td>
<td>Daughter Card Manager</td>
<td>Responsible for managing IPSec Security Associations for AH- and ESP-based sessions.</td>
</tr>
<tr>
<td></td>
<td>[ASR 5x00 only]</td>
<td>Interfaces with the on-board hardware accelerated cryptographic chip which executes cryptographic algorithms associated with the given IPSec Security Associations.</td>
</tr>
<tr>
<td>dhmgr</td>
<td>Distributed Host Manager</td>
<td>Started automatically on each CPU by SITPARENT.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coordinates establishment of locally terminated TCP, SCTP, and UDP connections on behalf of multi-instanced tasks such as Diameter endpoints among sessmgr tasks.</td>
</tr>
<tr>
<td>drvctrl</td>
<td>Driver Controller</td>
<td>Centralizes access to many of the system device drivers. It also performs temperature and voltage monitoring.</td>
</tr>
<tr>
<td>hdctrl</td>
<td>Hard Drive Controller</td>
<td>Controls and manages the drive array spanning the management cards.</td>
</tr>
<tr>
<td>hwctrl</td>
<td>Hardware Controller</td>
<td>The hwctrl task has several timers that manage polling loops for hardware sensor readings, sensor threshold monitoring, and fan tray monitoring.</td>
</tr>
<tr>
<td>hwmgr</td>
<td>Hardware Manager</td>
<td>The hwmgr task runs on all cards in the chassis to read local accessible hardware sensors and report them back to the hwctrl.</td>
</tr>
<tr>
<td>inetd</td>
<td>InterNet Service</td>
<td>The subsystem responsible for starting most of the network services.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Function</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Daemon</td>
<td>Listens for requests from connecting clients, such as FTP, SFTP, and telnet. When a TCP packet or UDP packet arrives with a particular destination port number, inetd launches the appropriate server program to handle the connection.</td>
</tr>
<tr>
<td>ipsecctrl</td>
<td>IPSec Controller</td>
<td>Started by SIT on system startup regardless of configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starts ipsecmgr tasks based on configuration and maintains its list for task recovery.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receives and maintains user configuration for IPSec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manages the configured IPSec crypto maps and its assignment to ipsecmgrs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interfaces with the vpnmgr task for required IPSec configuration parameters such as IP Access Lists, IP pools, interface addresses, and interface state notifications.</td>
</tr>
<tr>
<td>ipsecmgr</td>
<td>IPSec Manager</td>
<td>Created by the Session Controller, establishes and manages secure IKEv1, IKEv2 and IPSec data tunnels.</td>
</tr>
<tr>
<td>kvctrl</td>
<td>Key Value Controller</td>
<td>Central key value store (kvstore) function that runs on the management card. Its primary function is to support recovery and distribution functions.</td>
</tr>
<tr>
<td>lagmgr</td>
<td>Link Aggregation Group Manager [ASR 5x00 only]</td>
<td>Started by npuctrl on the demux card's primary CPU (ASR 5000) or MIO (ASR 5500) with a facility level between CSP and npumgr to receive configuration/status notification from npumgr and build global LAG database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exchanges control packets (LACP and Marker) over configured physical ports with peers to reach agreement on an aggregation of links.</td>
</tr>
<tr>
<td>msgd</td>
<td>Messenger Daemon</td>
<td>Implements the Name Service and related functions for the internal message passing system.</td>
</tr>
<tr>
<td>msgproxy</td>
<td>Message Proxy</td>
<td>The Messenger Proxy process handles broadcast messages send from any single application (referred to as a client) to any facility which has one instance per thread (referred to as the Target Facility).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One msgproxy task runs on each CPU complex on the SMC (ASR 5000), DPCs (ASR 5500) and SF Virtual Machine (VPC-DI).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes incoming broadcast messages from the Client processes, such as sessctrl, distributes them to the correct Target Facility, such as sessmgr, creates the correct responses and sends them back to the correct Client.</td>
</tr>
<tr>
<td>nscontrol</td>
<td>Name Service Controller</td>
<td>As part of the Messenger process, provides a reliable channel for tasks to send control messages to the Messenger Daemon.</td>
</tr>
<tr>
<td>ntpd</td>
<td>Network Time Protocol (NTP) Daemon</td>
<td>Maintains the system time in synchronization with time servers using NTP. Enabled when one or more NTP servers have been configured via the NTP Configuration mode <code>ntp server</code> CLI command.</td>
</tr>
<tr>
<td>rct</td>
<td>Recovery Control Task</td>
<td>Monitors tasks/managers/facilities across the system and performs recovery in the event of a failure.</td>
</tr>
<tr>
<td>sct</td>
<td>Shared Configuration Task</td>
<td>Performs the redundant storage of configuration information and other state information in an in-memory database.</td>
</tr>
<tr>
<td>sft</td>
<td>Switch Fabric Task</td>
<td>Monitors the switch fabric and the gigabit Ethernet control plane.</td>
</tr>
</tbody>
</table>
### Management Processes

**Table 21. Management Process Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>sshd</td>
<td>Secure SHell Daemon</td>
<td>Supports secure login to the StarOS CLI. Enabled via the Context Configuration mode server sshd CLI command.</td>
</tr>
<tr>
<td>ucm</td>
<td>Utilities Configuration Manager</td>
<td>DHC PD, DNS, FTPD, INETD, NTPD, PING, RLOGIN, SFTP, SFTP-SERVER, SNMPD, SSH, SSHD, TELNET, TELNETD, TFTP, TRACEROUTE</td>
</tr>
<tr>
<td>bulkstat</td>
<td>Bulk Statistics Manager</td>
<td>Periodically polls and gathers bulk statistics and transfers this data to external management systems.</td>
</tr>
<tr>
<td>evlogd</td>
<td>Event Log Daemon</td>
<td>Handles event logging functions including the interface to external syslogd servers and the internal event logs.</td>
</tr>
<tr>
<td>orbs</td>
<td>ORBEM Service [ASR 5x00 only]</td>
<td>The orbs task is also known as the ORB Element Manager (ORBEM). An Element Management System (EMS) requests orbs to perform Element Management Functions on the system using secure IIOP. ORBS then interacts with concerned Controller Tasks to execute the function. The response/errors from the execution are interpreted, formulated into an EMF response, and handed off to EMS servers.</td>
</tr>
<tr>
<td>orbns</td>
<td>ORBEM Notification Service [ASR 5x00 only]</td>
<td>Notifies the EMS servers of event occurrences. Registers such EMS servers and subscribes them to associated event types. As the events occur, the concerned Controller Task notifies orbs (ORBEM), which then notifies the subscribing EMS servers.</td>
</tr>
<tr>
<td>sesstrc</td>
<td>Session Trace Collection Task</td>
<td>Implements the standards-based session trace functionality. Manages both CLI and signaling-based subscriber traces. It collects messages to be traced and generates trace files as needed. It uploads trace files to the Trace Collection Entity as needed.</td>
</tr>
<tr>
<td>snmp</td>
<td>Simple Network Management Protocol</td>
<td>Handles inboard SNMP operations if configured, and sends SNMP notifications (traps) if enabled.</td>
</tr>
<tr>
<td>threshold</td>
<td>Threshold Server</td>
<td>Handles monitoring of threshold crossing alerts, if configured. Polls the needed statistics/variables, maintains state, and generates log messages/SNMP notification of threshold crossings.</td>
</tr>
</tbody>
</table>
Appendix D
ICSR Checkpointing

This appendix lists and describes macro- and micro-checkpoints employed by the Interchassis Session Recovery framework. Checkpoints are exchanged between the active and standby ICSR chassis via the Service Redundancy Protocol (SRP).

The following topics are discussed:

- Overview of Checkpointing
- Macro-checkpoints
- Micro-checkpoints
Overview of Checkpointing

Interchassis Session Recovery (ICSR) provides a framework for sessmgr instance-level checkpointing within an ICSR framework. A checkpoint is a snapshot of the status of an application. Checkpointing can be used by sessmgr to push instance level information to the peer chassis.

Instance-level checkpointing sends messages to specific sessmgr instances. Each application, such as GGSN, PDSN, PGW, S-GW or SGSN, is responsibility for encoding and decoding the checkpoint message. The ICSR framework provides the APIs for transport of the instance-level checkpoint information and associated statistics.

Macro-checkpoints contain full session information and micro-checkpoints contain only a few variables. Macro-checkpoints are sent initially from the active chassis to the standby chassis on power up and reload, and periodically thereafter. When a standby chassis receives macro-checkpoints, it clears any existing CRR (Call Recovery Record) or CLP (Call Line Pointer) related to that session, and creates a new CRR or CLP. Macro-checkpoints are also known as full checkpoints (FCs).

To conserve processing cycles and memory, dynamic and periodic updates from an active chassis to a standby chassis are done using micro-checkpoints.

The output of the Exec mode `show srp info` command displays a complete list of SRP checkpoints.
Macro-checkpoints

This section lists and briefly describes ICSR macro-checkpoints.

GGSN_APN ID MAPPING

This macro-checkpoint is sent from the active to the standby chassis to map APN names on the standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever a TCP connection is established between the sessmgs and they move to READY_STATE.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **Related CLI command:** show session subsystem facility sessmgr instance <instance no> debug-info and show srp micro-checkpoint statistics

INSTANCE LEVEL CHECKPOINT

This macro-checkpoint is generated by ECS (Enhanced Charging System) to send new rules to the standby chassis. It is also used by ECS to delete or modify a rule on the standby chassis.

- **Time based:** Yes
- **Frequency:** 30 minutes
- **Event based:** Yes
- **Events:** Occurs:
  1. When a new rule is added or deleted on the active chassis.
  2. Every 30 minutes if the ECS is registered for periodic micro-checkpointing.
- **Accounting:** —
- **Delta/Cumulative:** —
- **Related CLI command:** show session subsystem facility sessmgr instance <instance no> debug-info and show srp micro-checkpoint statistics

SERVICE_ID MAPPING

This macro-checkpoint is sent from the active to the standby chassis to map Service IDs on the standby chassis.

- **Time based:** No
- **Frequency:** N/A
**Macro-checkpoints**

- **Event based:** Yes
- **Events:** Occurs whenever a TCP connection is established between the sessmgrs and they move to READY_STATE.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **Related CLI command:** `show session subsystem facility sessmgr instance <instance no> debug-info`

**VPNMRG_ID MAPPING**

This macro-checkpoint is sent from the active to the standby chassis to map VPNs on the standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever a TCP connection is established between the sessmgrs and they move to READY_STATE.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **Related CLI command:** `show session subsystem facility sessmgr instance <instance no> debug-info`
Micro-checkpoints

This section lists and briefly describes the characteristics of micro-checkpoints by application category. Micro-checkpoints are listed in alphabetical order under the following categories:

- Uncategorised
- DCCA Category
- ECS Category
- ePDG Category
- Firewall/ECS Category
- GGSN Category
- Gx Interface Category
- NAT Category
- PGW Category
- Rf Interface Category
- S6b Interface Category
- SaMOG Category

Uncategorised

SESS_UCHKPT_CMD_INVALIDATE_CRR

This micro-checkpoint is sent to the standby chassis to clear a deleted call. It carries the Call ID and other information that must be deleted on the standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs when a call is deleted on the active chassis.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 1
- **Related CLI command:** None

SESS_UCKKPT_CMD_UPDATE_CLPSTATS

This micro-checkpoint sends VoLTE data statistics.

- **Time based:** Yes
- Frequency: —
- Event based: Yes
- Events: Occurs during ICSR background checkpointing. A chassis switchover triggers the sending of VoLTE data stats.
- Accounting: —
- Delta/Cumulative: —
- CMD-ID: 4
- Related CLI command: None

**SESSION_CHKPT_CMD_UPDATE_IDLESECS**

This micro-checkpoint sends remaining number of seconds before idle timeout.
- Time based: Yes
- Frequency: —
- Event based: No
- Events: Occurs during ICSR background checkpointing.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 2
- Related CLI command: None

**DCCA Category**

**SESSION_CHKPT_CMD_DCCA_SESS_INFO**

This micro-checkpoint sends Credit Control (CC) related information.
- Time based: Yes
- Frequency: 18 seconds for GR micro-checkpoint
- Event based: Yes
- Events: Sent along with the macro-checkpoint/CCA/Assume-positive-state-transitions.
- Accounting: Yes
- Delta/Cumulative: Cumulative
- CMD-ID: 19
- Related CLI command: None
ECS Category

**SESS_UCHKPT_CMD_ACS_CALL_INFO**

This micro-checkpoint sends critical ECS call level data.

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever ECS call level information is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 179
- **Related CLI command:** None

**SESS_UCHKPT_CMD_ACS_GX_LI_INFO**

This micro-checkpoint sources lawful intercept (LI) related information maintained by ECS.

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever LI information is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 75
- **Related CLI command:** None

**SESS_UCHKPT_CMD_ACS_SESS_INFO**

This micro-checkpoint sends ECS-level bearer-related data

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever ECS bearer information is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 33
- **Related CLI command:** None
SESS_UCHKPT_CMD_DEL_ACS_CALL_INFO

This micro-checkpoint notifies that a Release Call event has occurred.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever an ECS Release Call message is processed.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 188
- **Related CLI command:** —

SESS_UCHKPT_CMD_DEL_ACS_SESS_INFO

This micro-checkpoint notifies that a Release Bearer event has occurred.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever an ECS Release Bearer message is processed.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 187
- **Related CLI command:** None

SESS_UCHKPT_CMD_DYNAMIC_CHRG_CA_INFO

This micro-checkpoint sends dynamic charging action information maintained by ECS.

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever dynamic charging action information is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 141
- **Related CLI command:** None
SESS_UCHKPT_CMD_DYNAMIC_CHRG_DEL_CA_INFO
This micro-checkpoint notifies that a dynamic charging action has been deleted.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever a dynamic charging action has been deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 183
- **Related CLI command:** None

SESS_UCHKPT_CMD_DYNAMIC_CHRG_DEL_QG_INFO
This micro-checkpoint notifies that a dynamic QoS group has been deleted.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever a dynamic QoS group has been deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 182
- **Related CLI command:** None

SESS_UCHKPT_CMD_DYNAMIC_CHRG_QG_INFO
This micro-checkpoint sends dynamic QoS group related information maintained by ECS.

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever dynamic QoS group information is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 140
- **Related CLI command:** None
SESS_UCHKPT_CMD_DYNAMIC_RULE_DEL_INFO

This micro-checkpoint notifies that a dynamic rule has been deleted.

- **Time based:** No
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever a dynamic rule has been deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 178
- **Related CLI command:** None

SESS_UCHKPT_CMD_DYNAMIC_RULE_INFO

This micro-checkpoint sources predefined and dynamic rule related information maintained by ECS.

- **Time based:** Yes
- **Frequency:** —
- **Event based:** Yes
- **Events:** Occurs whenever a dynamic rule is created or modified.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 43
- **Related CLI command:** None

ePDG Category

SESS_UCHKPT_CMD_DELETE_EPDG_BEARER

This micro-checkpoint synchronizes deleted ePDG bearers between the active and standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** N/A
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 110
- **Related CLI command:** show srp micro-checkpoint statistics debug-info
SESS_UCHKPT_CMD_UPDATE_EPDG_BEARER

This micro-checkpoint synchronizes ePDG bearers between the active and standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** No
- **Events:** N/A
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 110
- **Related CLI command:** show srp micro-checkpoint statistics debug-info

SESS_UCHKPT_CMD_UPDATE_EPDG_PEER_ADDR

This micro-checkpoint synchronizes ePDG peer addresses between the active and standby chassis.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** —
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 110
- **Related CLI command:** show srp micro-checkpoint statistics debug-info

SESS_UCHKPT_CMD_UPDATE_EPDG_REKEY

This micro-checkpoint synchronizes ePDG rekey statistics between the active and standby chassis.

- **Time based:** Yes
- **Frequency:** 30 seconds
- **Event based:** No
- **Events:** N/A
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 110
- **Related CLI command:** show srp micro-checkpoint statistics debug-info
SESS_UCHKPT_CMD_UPDATE_EPDG_STATS

This micro-checkpoint synchronizes session statistics between the active and standby chassis.

- **Time based:** Yes
- **Frequency:** 30 seconds
- **Event based:** No
- **Events:** N/A
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 110
- **Related CLI command:** show srp micro-checkpoint statistics debug-info

**Firewall/ECS Category**

SESS_UCHKPT_CMD_SFW_DEL_RULE_INFO

This micro-checkpoint is sent when a ruledef is deleted for a bearer.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever PCRF sends a command to disable the predefined stateful firewall access rules.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 186
- **Related CLI command:** None

SESS_UCHKPT_CMD_SFW_RULE_INFO

This micro-checkpoint notifies the addition of dynamically enabled stateful firewall (SFW) access rules.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever PCRF sends a command to enable the predefined SFW access rules.
- **Accounting:** Yes
- **Delta/Cumulative:** Cumulative
- **CMD-ID:** 185
- **Related CLI command:** None
GGSN Category

**SESS_UCKPNT_CMD_GGSN_DELETE_SUB_SESS**

This micro-checkpoint sends an update when a secondary bearer is deleted.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs upon secondary bearer deletion
- **Accounting:** —
- **Delta/Cumulative:** —
- **CMD-ID:** 117
- **Related CLI command:** None

**SESS_UCKPNT_CMD_GGSN_UPDATE_RPR**

If RPR (Resilient Packet Ring) is configured in the GGSN service, an RPR timer is started during secondary bearer creation. This checkpoint is sent upon expiry of this timer.

- **Time based:** Yes
- **Frequency:** RPR timer
- **Event based:** Yes
- **Events:** Occurs when the secondary bearer creation RPR timer expires.
- **Accounting:** —
- **Delta/Cumulative:** —
- **CMD-ID:** 118
- **Related CLI command:** —

**SESS_UCKPNT_CMD_GGSN_UPDATE_SESSION**

This micro-checkpoint is sent in a Network or UE initiated update procedure except for updates that result in the following scenarios:

- Creation or deletion of the bearer
- TFT change or inter-RAT handovers
- Gn-Gp handoff

Parameters associated with this micro-checkpoint are shown below.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
Events: Occurs for a network initiated or UE initiated update.
Accounting: No
Delta/Cumulative: N/A
CMD-ID: 171
Related CLI command: show srp checkpoint statistics active verbose, and show session subsystem facility sessmgr instance <instance_number> debug-info.

SESS_UCHKPT_CMD_GGSN_UPDATE_STATS
This micro-checkpoint periodically sends session statistics.

- Time based: Yes
- Frequency: Every five minutes
- Event based: No
- Events: N/A
- Accounting: Yes
- Delta/Cumulative: Cumulative
- CMD-ID: 116
- Related CLI command: None

SESS_UCHKPT_CMD_UPDATE_COA_PARAMS
This micro-checkpoint updates input and output ACL parameters.

- Time based: —
- Frequency: —
- Event based: Yes
- Events: COA (Change of Authorization) response
- Accounting: —
- Delta/Cumulative: —
- CMD-ID: 83
- Related CLI command: None

Gx Interface Category

SESS_UCHKPT_CMD_ACS_VOLUME_USAGE
This micro-checkpoint sends volume usage over Gx accounting buckets.

- Time based: Yes
- Frequency: 4 seconds for aamgr micro-checkpoint and 18 seconds for GR micro-checkpoint
• Event based: No
• Events: Send along with macro-checkpoint
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 79
• Related CLI command: —None

**SESS_UCHKPT_CMD_UPDATE_SGX_INFO**

This micro-checkpoint sends Gx session-related information.

• Time based: No
• Frequency: N/A
• Event based: Yes
• Events: Triggered on receiving CCA-I/U or RAR from PCRF.
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 137
• Related CLI command: None

**NAT Category**

**SESS_UCHKPT_CMD_GR_UPDATE_NAT_REALM_PORT_INFO1**

This micro-checkpoint is sent when a port chunk is allocated or deallocated for a subscriber sharing a NAT IP address with other subscribers. The port chunk is allocated or deallocated while data is being received for that subscriber.

• Time based: No
• Frequency: N/A
• Event based: Yes
• Events: Triggered when a new NAT port chunk is allocated or deleted.
• Accounting: No
• Delta/Cumulative: N/A
• CMD-ID: 105
• Related CLI command: None

**SESS_UCHKPT_CMD_GR_UPDATE_NAT_REALMS**

This micro-checkpoint is sent when a NAT IP address is allocated to or deallocated from a subscriber.
For an on-demand case, it is triggered when the first packet matching a particular NAT realm is received and the NAT IP address is allocated to the subscriber.

If this is not an on-demand case, the NAT IP address is allocated during call setup and this micro-checkpoint is sent.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Triggered when a NAT IP address is allocated to or deallocated from a subscriber.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 45
- **Related CLI command:** None

**SESS_UCHKPT_CMD_NAT_SIP_ALG_CALL_INFO**

This micro-checkpoint is sent when a new SIP flow is created or deleted for a subscriber (while SIP data is being passed via the subscriber).

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Triggered when a new SIP flow is created or deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 98
- **Related CLI command:** None

**SESS_UCHKPT_CMD_NAT_SIP_ALG_CONTACT_PH_INFO**

This micro-checkpoint is sent when a received SIP packet is analyzed and pinholes are created in the NAT firewall.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Triggered when a SIP packet creates pinholes in the NAT firewall.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 97
- **Related CLI command:** None
**ICSR Checkpointing**

**Micro-checkpoints**

**SESS_UCHKPT_CMD_UPDATE_DSK_FLOW_CHKPT_INFO**

This micro-checkpoint is sent when a new NAT flow is created or deleted for a subscriber (while data is being passed via the subscriber).

This checkpoint is sent from a timer but it is not timer based. The timer is used to pace (10 micro-checkpoints) whenever the timer fires (granularity = 2 sec). This only occurs if there are new flows that need to be micro-checkpointed. Otherwise, no micro-micro-checkpoints are sent.

- **Time based:** No
- **Frequency:** See explanation above.
- **Event based:** Yes
- **Events:** Triggered when a new NAT flow is created or deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 96
- **Related CLI command:** None

**SESS_UCHKPT_CMD_UPDATE_NAT_BYPASS_FLOW_INFO**

This micro-checkpoint is sent when NAT is enabled for a subscriber but bypass-nat (no NATing) is configured for this flow (based on a rule-match), and a new bypass flow is created.

This checkpoint is sent when the flow is both added and deleted.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Triggered when a new flow with bypass-nat enabled is created or deleted.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 60
- **Related CLI command:** None

**P-GW Category**

**SESS_UCHKPT_CMD_PGW_DELETE_SUB_SESS**

Reserved for future use.

**SESS_UCHKPT_CMD_PGW_OVRCHRG_PRTCTN_INFO**

This micro-checkpoint indicates that the S-GW has set the Overcharging Protection bit in the MBR.
• **Time based:** No
• **Frequency:** N/A
• **Event based:** Yes
• **Events:** Triggered when the S-GW sets the Over Charging Protection Bit.
• **Accounting:** No
• **Delta/Cumulative:** N/A
• **CMD-ID:** 159
• **Related CLI command:** None

**SESS_UCHKPT_CMD_PGW_SGWRESTORATION_INFO**

This micro-checkpoint indicates the interval that a call will remain up when the S-GW is down.

• **Time based:** No
• **Frequency:** N/A
• **Event based:** Yes
• **Events:** Triggered when the S-GW goes into Restoration mode.
• **Accounting:** No
• **Delta/Cumulative:** N/A
• **CMD-ID:** 158
• **Related CLI command:** None

**SESS_UCHKPT_CMD_PGW_UBR_MBR_INFO**

This micro-checkpoint is sent at the end of a UBR (Update Bearer Request) or MBR (Modify Bearer Request) except when the UBR / MBR procedure results in the following scenarios:

• TFT change
• Bearer update or modification for a collapsed call
• Pure P to collapsed or collapsed to Pure P change
• Inter-technology handoff, for example, WiFi to LTE

Parameters associated with this micro-checkpoint are shown below.

• **Time based:** No
• **Frequency:** N/A
• **Event based:** Yes
• **Events:** Occurs as a result of a UBR or MBR procedure.
• **Accounting:** No
• **Delta/Cumulative:** N/A
• **CMD-ID:** 193
- Related CLI command: show srp checkpoint statistics active verbose and show session subsystem facility sessmgr instance <instance_number> debug-info.

SESS_UCHKPT_CMD_PGW_UPDATE_APN_AMBR

Reserved for future use.

SESS_UCHKPT_CMD_PGW_UPDATE_INFO

Reserved for future use.

SESS_UCHKPT_CMD_PGW_UPDATE_LI_PARAM

This micro-checkpoint indicates the state of Lawful Intercept (LI) for this call.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Triggered when there is a change in the LI state for this call.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 151
- Related CLI command: None

SESS_UCHKPT_CMD_PGW_UPDATE_PDN_COMMON_PARAM

Reserved for future use.

SESS_UCHKPT_CMD_PGW_UPDATE_QOS

Reserved for future use.

SESS_UCHKPT_CMD_PGW_UPDATE_SGW_CHAN

Reserved for future use.

SESS_UCHKPT_CMD_PGW_UPDATE_STATS

This micro-checkpoint periodically sends session statistics.

- Time based: Yes
- Frequency: Every five minutes
- Event based: No
- Events: N/A
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 65
• Related CLI command: None

Rf Interface Category

SESS_UCHKPT_CMD_ACS_ACCOUNTING_TYPE_QCI_RF
This micro-checkpoint indicates a change in the SDF+QCI-based Rf accounting buckets.
• Time based: Yes
• Frequency: 4 seconds for aamgr checkpoint and 18 seconds for GR checkpoint
• Event based: No
• Events: N/A
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 126
• Related CLI command: None

SESS_UCHKPT_CMD_ACS_ACCOUNTING_TYPE_QCI_RF_WITH_FC
This micro-checkpoint indicates complete SDF+QCI-based Rf accounting buckets.
• Time based: Yes
• Frequency: 4 seconds for aamgr checkpoint and 18 seconds for GR checkpoint
• Event based: No
• Events: Sent along with macro-checkpoint.
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 164
• Related CLI command: None

SESS_UCHKPT_CMD_ACS_ACCOUNTING_TYPE_RATING_GROUP_RF
This micro-checkpoint indicates a change in the SDF-based Rf accounting buckets.
• Time based: Yes
• Frequency: 4 seconds for aamgr checkpoint and 18 seconds for GR checkpoint
• Event based: No
ICSR Checkpointing

Micro-checkpoints

• Events: N/A
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 125
• Related CLI command: None

SESS_UCHKPT_CMD_ACS_ACCOUNTING_TYPE_RATING_GROUP_RF_WITH_FC

This micro-checkpoint indicates complete SDF-based Rf accounting buckets.

• Time based: Yes
• Frequency: 4 seconds for aamgr checkpoint and 18 seconds for GR checkpoint;
• Event based: No
• Events: Sent along with macro-checkpoint.
• Accounting: Yes
• Delta/Cumulative: Cumulative
• CMD-ID: 163
• Related CLI command: None

S6b Interface Category

SESS_UCHKPT_CMD_S6B_INFO

This micro-checkpoint sends the Restoration Priority Indicator when reauthorization occurs over the S6b interface.

• Time based: No
• Frequency: N/A
• Event based: Yes
• Events: Occurs when an Sb6 reauthorization results in a change in value of the Restoration Priority Indicator.
• Accounting: No
• Delta/Cumulative: N/A
• CMD-ID: 202
• Related CLI command: None

SaMOG Category

SESS_UCHKPT_CMD_CGW_DELETE_BEARER

Reserved for future use.
SESS_UCHKPT_CMD_CGW_DELETE_PDN

This micro-checkpoint indicates a PDN connection has been deleted.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs whenever SaMOG sends a Delete-Session-Req or upon receiving a Delete-Bearer-Request.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 169
- **Related CLI command:** show subscriber samog-only full

SESS_UCHKPT_CMD_CGW_UPDATE_BEARER_QOS

This micro-checkpoint indicates a QoS update for the bearer.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs when a change in Bearer QoS is received from the P-GW due to a reauthorization (AAR Received from AAA Server) or Update-Bearer-Request.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 167
- **Related CLI command:** show subscriber samog-only full

SESS_UCHKPT_CMD_CGW_UPDATE_PDN

This micro-checkpoint indicates a PDN update for a change in APN-AMBR.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs when a change in APN-AMBR is received from the P-GW due to a reauthorization (AAR Received from AAA Server) or Update-Bearer-Request.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 168
- **Related CLI command:** show subscriber samog-only full
SESS_UCHKPT_CMD_CGW_UPDATE_STATS

Reserved for future use.

SESS_UCHKPT_CMD_CGW_UPDATE UE_PARAM

Reserved for future use.

SESS_UCHKPT_CMD_SAMOG ACCT INTERIM INFO

This micro-checkpoint is sent for a SaMOG session on receipt of an Accounting Req (INTERIM-UPDATE) from the WLC.

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs on receipt of an Accounting Req (INTERIM-UPDATE) from the WLC.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 177
- **Related CLI command:** show subscriber samog-only full

SESS_UCHKPT_CMD_SAMOG ACCT START INFO

This micro-checkpoint is sent for a SaMOG session on receipt of an Accounting Req (START) from the WLC (Wireless LAN Controller).

- **Time based:** No
- **Frequency:** N/A
- **Event based:** Yes
- **Events:** Occurs when an Account Req (START) request is received from the WLC.
- **Accounting:** No
- **Delta/Cumulative:** N/A
- **CMD-ID:** 174
- **Related CLI command:** show subscriber samog-only full

SESS_UCHKPT_CMD_SAMOG EOGRE TUNNEL INFO

This micro-checkpoint is sent for an Inter-RG handoff for EoGRE subscriber sessions. This checkpoint updates the VMAC Address and WLC EoGRE tunnel end-point address.

- **Time based:** No
- **Frequency:** N/A
ICSR Checkpointing

Micro-checkpoints

- Event based: Yes
- Events: Occurs whenever a DHCP-Discover message is received over a different EoGRE tunnel.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 201
- Related CLI command: show subscriber samog-only full

SESS_UCHKPT_CMD_SAMOG_GTPV1_UPDATE_PDN_INFO

This micro-checkpoint is sent for a SaMOG session upon receipt of an Update-PDP-Context-Req from the GGSN to update the PDN information.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs after successful SaMOG processing of an Update-PDP-Context-Req from the GGSN.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 191
- Related CLI command: show subscriber samog-only full

SESS_UCHKPT_CMD_SAMOG_HANDOFF_AUTHEN_INFO

This micro-checkpoint is sent for a SaMOG session that is Re-authenticating the subscriber while the subscriber session is in Handoff state.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs on completion of Re-Authentication for an existing SaMOG subscriber session currently in Handoff state.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 176
- Related CLI command: show subscriber samog-only full

SESS_UCHKPT_CMD_SAMOG_HANDOFF_INIT_INFO

This micro-checkpoint is sent for a SaMOG session on receipt of an Accounting Req (STOP) from the WLC (Wireless LAN Controller).

SaMOG will delay handoff as it expects an Accounting Req (START) from the subscriber.
- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs when a Account Req (STOP) request is received from the WLC.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 175
- Related CLI command: show subscriber samog-only full

**SESS_UCKPRT_CMD_SAMOG_LI_PROV_INFO**

This micro-checkpoint is sent for a SaMOG session that is on lawful intercept (LI) Active-Camp-on mode.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs after an LI trigger is received after SaMOG session has been created.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 189
- Related CLI command: show subscriber samog-only full

**SESS_UCKPRT_CMD_SAMOG_MIPV6_TIMER_INFO**

This micro-checkpoint updates the Binding Cache Life timer and MIPv6 binding status for a SaMOG session.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs whenever a PMIPv6 PBU is received with a lifetime of zero from the WLC.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 190
- Related CLI command: show subscriber samog-only full

**SESS_UCKPRT_CMD_SAMOG_MULTI_ROUND_AUTHEN_INFO**

This micro-checkpoint is sent for a SaMOG session when SaMOG is waiting on the UE after sending an Access-Challenge while Re-authenticating the subscriber session.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs after SaMOG sends an Access-Challenge for an existing SaMOG subscriber session during Re-authentication.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 184
- Related CLI command: show subscriber samog-only full

**SESS_UCHKPT_CMD_SAMOG_REAUTHEN_INFO**

This micro-checkpoint is sent for a SaMOG session when subscriber Re-authentication is completed.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs on completion of Re-Authentication for an existing SaMOG subscriber session.
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 172
- Related CLI command: show subscriber samog-only full

**SESS_UCHKPT_CMD_SAMOG_REAUTHOR_INFO**

This micro-checkpoint is sent for a SaMOG session when subscriber Re-authorization is completed.

- Time based: No
- Frequency: N/A
- Event based: Yes
- Events: Occurs on receiving and successfully processing AAR from the AAA Server to re-authorize the subscriber
- Accounting: No
- Delta/Cumulative: N/A
- CMD-ID: 173
- Related CLI command: show subscriber samog-only full
Appendix E  
VPC SDR CLI Command Strings

This appendix identifies the StarOS CLI command strings that can be entered for a record section via the `support record section` command in the Global Configuration Mode. The string must be entered within double quotation marks (" ") to be recognized. The table below also indicates default and non-default strings.

For detailed command string information, refer to the *Command Line Interface Reference* or the online Help for the command.

The table below also indicates default and non-default strings. It reflects the output sequence of the `show support collection definitions` command.

Table 22. VPC SDR CLI Command Strings

<table>
<thead>
<tr>
<th>No.</th>
<th>Default SDR</th>
<th>Command String</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Enabled</td>
<td>“show version verbose”</td>
</tr>
<tr>
<td>1</td>
<td>Enabled</td>
<td>“show clock”</td>
</tr>
<tr>
<td>2</td>
<td>Enabled</td>
<td>“show clock universal”</td>
</tr>
<tr>
<td>3</td>
<td>Enabled</td>
<td>“show configuration”</td>
</tr>
<tr>
<td>4</td>
<td>Enabled</td>
<td>“show_profile”</td>
</tr>
<tr>
<td>5</td>
<td>Enabled</td>
<td>“show context”</td>
</tr>
<tr>
<td>6</td>
<td>Enabled</td>
<td>“show boot”</td>
</tr>
<tr>
<td>7</td>
<td>Enabled</td>
<td>“show boot initial-config”</td>
</tr>
<tr>
<td>8</td>
<td>Enabled</td>
<td>“show system uptime”</td>
</tr>
<tr>
<td>9</td>
<td>Disabled</td>
<td>“show license information”</td>
</tr>
<tr>
<td>10</td>
<td>Disabled</td>
<td>“show license history”</td>
</tr>
<tr>
<td>11</td>
<td>Disabled</td>
<td>“show hardware inventory”</td>
</tr>
<tr>
<td>12</td>
<td>Disabled</td>
<td>“show hardware version”</td>
</tr>
<tr>
<td>13</td>
<td>Disabled</td>
<td>“show card hardware”</td>
</tr>
<tr>
<td>14</td>
<td>Disabled</td>
<td>“show card dhaccel hardware counters”</td>
</tr>
<tr>
<td>15</td>
<td>Enabled</td>
<td>“show hd raid verbose”</td>
</tr>
<tr>
<td>16</td>
<td>Enabled</td>
<td>“debug hdctrl mdstat”</td>
</tr>
<tr>
<td>17</td>
<td>Enabled</td>
<td>“debug hdctrl history”</td>
</tr>
<tr>
<td>18</td>
<td>Disabled</td>
<td>“debug hdctrl lsas”</td>
</tr>
<tr>
<td>19</td>
<td>Disabled</td>
<td>“debug hdctrl mapping”</td>
</tr>
<tr>
<td>20</td>
<td>Enabled</td>
<td>“show hd iocnt all”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>21</td>
<td>Disabled</td>
<td>“show hd logs all”</td>
</tr>
<tr>
<td>22</td>
<td>Enabled</td>
<td>“show hd smart all”</td>
</tr>
<tr>
<td>23</td>
<td>Enabled</td>
<td>“debug hdctrl state”</td>
</tr>
<tr>
<td>24</td>
<td>Enabled</td>
<td>“debug hdctrl client list”</td>
</tr>
<tr>
<td>25</td>
<td>Disabled</td>
<td>“show card info”</td>
</tr>
<tr>
<td>26</td>
<td>Enabled</td>
<td>“show card diag”</td>
</tr>
<tr>
<td>27</td>
<td>Enabled</td>
<td>“show card table all”</td>
</tr>
<tr>
<td>28</td>
<td>Enabled</td>
<td>“show port table all”</td>
</tr>
<tr>
<td>29</td>
<td>Enabled</td>
<td>“show port info”</td>
</tr>
<tr>
<td>30</td>
<td>Enabled</td>
<td>“show port utilization table”</td>
</tr>
<tr>
<td>31</td>
<td>Enabled</td>
<td>“show data-path congestion”</td>
</tr>
<tr>
<td>32</td>
<td>Disabled</td>
<td>“show npu details”</td>
</tr>
<tr>
<td>33</td>
<td>Disabled</td>
<td>“show lagmgr details”</td>
</tr>
<tr>
<td>34</td>
<td>Enabled</td>
<td>“show fans”</td>
</tr>
<tr>
<td>36</td>
<td>Enabled</td>
<td>“show power chassis”</td>
</tr>
<tr>
<td>37</td>
<td>Enabled</td>
<td>“show temperature”</td>
</tr>
<tr>
<td>39</td>
<td>Disabled</td>
<td>“show alarm audible”</td>
</tr>
<tr>
<td>40</td>
<td>Disabled</td>
<td>“show alarm central-office”</td>
</tr>
<tr>
<td>41</td>
<td>Disabled</td>
<td>“show alarm outstanding”</td>
</tr>
<tr>
<td>42</td>
<td>Disabled</td>
<td>“show alarm statistics”</td>
</tr>
<tr>
<td>43</td>
<td>Enabled</td>
<td>“show cpu table”</td>
</tr>
<tr>
<td>44</td>
<td>Disabled</td>
<td>“show cpu info verbose”</td>
</tr>
<tr>
<td>45</td>
<td>Enabled</td>
<td>“show cpu errors verbose”</td>
</tr>
<tr>
<td>46</td>
<td>Enabled</td>
<td>“show cpu performance verbose”</td>
</tr>
<tr>
<td>47</td>
<td>Disabled</td>
<td>“show resources”</td>
</tr>
<tr>
<td>48</td>
<td>Disabled</td>
<td>“show task table”</td>
</tr>
<tr>
<td>49</td>
<td>Disabled</td>
<td>“show task memory”</td>
</tr>
<tr>
<td>50</td>
<td>Disabled</td>
<td>“show task memory max”</td>
</tr>
<tr>
<td>51</td>
<td>Disabled</td>
<td>“show task resources”</td>
</tr>
<tr>
<td>52</td>
<td>Disabled</td>
<td>“show task resources max”</td>
</tr>
<tr>
<td>53</td>
<td>Enabled</td>
<td>“show crash list”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>54</td>
<td>Enabled</td>
<td>“show crash all”</td>
</tr>
<tr>
<td>55</td>
<td>Disabled</td>
<td>“show persistdump list”</td>
</tr>
<tr>
<td>56</td>
<td>Disabled</td>
<td>“show persistdump display”</td>
</tr>
<tr>
<td>57</td>
<td>Enabled</td>
<td>“show snmp trap history verbose”</td>
</tr>
<tr>
<td>58</td>
<td>Disabled</td>
<td>“show snmp trap statistics verbose”</td>
</tr>
<tr>
<td>59</td>
<td>Enabled</td>
<td>“show logs”</td>
</tr>
<tr>
<td>63</td>
<td>Disabled</td>
<td>“show messenger settings”</td>
</tr>
<tr>
<td>64</td>
<td>Enabled</td>
<td>“show messenger nameservice”</td>
</tr>
<tr>
<td>65</td>
<td>Enabled</td>
<td>“show messenger statistics”</td>
</tr>
<tr>
<td>66</td>
<td>Enabled</td>
<td>“show messenger bounces”</td>
</tr>
<tr>
<td>67</td>
<td>Disabled</td>
<td>“debug limits checkup detailed”</td>
</tr>
<tr>
<td>68</td>
<td>Disabled</td>
<td>“show plugin”</td>
</tr>
<tr>
<td>69</td>
<td>Disabled</td>
<td>“show module”</td>
</tr>
<tr>
<td>70</td>
<td>Disabled</td>
<td>“show ppp statistics”</td>
</tr>
<tr>
<td>71</td>
<td>Disabled</td>
<td>“show rsvp statistics”</td>
</tr>
<tr>
<td>72</td>
<td>Enabled</td>
<td>“show session disconnect-reasons verbose”</td>
</tr>
<tr>
<td>73</td>
<td>Disabled</td>
<td>“show apn statistics all”</td>
</tr>
<tr>
<td>74</td>
<td>Disabled</td>
<td>“show ipsg statistics”</td>
</tr>
<tr>
<td>75</td>
<td>Disabled</td>
<td>“show pdsn-service all”</td>
</tr>
<tr>
<td>76</td>
<td>Disabled</td>
<td>“show hsgw-service all”</td>
</tr>
<tr>
<td>77</td>
<td>Disabled</td>
<td>“show hsgw-service statistics all”</td>
</tr>
<tr>
<td>78</td>
<td>Disabled</td>
<td>“show epdg-service all counters”</td>
</tr>
<tr>
<td>79</td>
<td>Disabled</td>
<td>“show epdg-service statistics”</td>
</tr>
<tr>
<td>80</td>
<td>Disabled</td>
<td>“show fa-service all”</td>
</tr>
<tr>
<td>81</td>
<td>Disabled</td>
<td>“show ha-service all”</td>
</tr>
<tr>
<td>82</td>
<td>Disabled</td>
<td>“show mag-service all”</td>
</tr>
<tr>
<td>83</td>
<td>Disabled</td>
<td>“show mipv6ha-service all”</td>
</tr>
<tr>
<td>84</td>
<td>Disabled</td>
<td>“show lma-service all”</td>
</tr>
<tr>
<td>85</td>
<td>Disabled</td>
<td>“show dhcp-service all”</td>
</tr>
<tr>
<td>86</td>
<td>Disabled</td>
<td>“show sgsn-service all”</td>
</tr>
<tr>
<td>87</td>
<td>Disabled</td>
<td>“show sgsn sessmgr all memory statistics”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>88</td>
<td>Disabled</td>
<td>“show operator-policy all”</td>
</tr>
<tr>
<td>89</td>
<td>Disabled</td>
<td>“show call-control-profile all”</td>
</tr>
<tr>
<td>90</td>
<td>Disabled</td>
<td>“show apn-profile all”</td>
</tr>
<tr>
<td>91</td>
<td>Disabled</td>
<td>“show imei-profile all”</td>
</tr>
<tr>
<td>92</td>
<td>Disabled</td>
<td>“show gprs-service all”</td>
</tr>
<tr>
<td>93</td>
<td>Disabled</td>
<td>“show iups-service all”</td>
</tr>
<tr>
<td>94</td>
<td>Disabled</td>
<td>“show sgtp-service all”</td>
</tr>
<tr>
<td>95</td>
<td>Disabled</td>
<td>“show map-service all”</td>
</tr>
<tr>
<td>96</td>
<td>Disabled</td>
<td>“show gs-service all”</td>
</tr>
<tr>
<td>97</td>
<td>Disabled</td>
<td>“show ggsn-service all”</td>
</tr>
<tr>
<td>98</td>
<td>Disabled</td>
<td>“show ggsn-service sgsn-table”</td>
</tr>
<tr>
<td>99</td>
<td>Disabled</td>
<td>“show csf service all”</td>
</tr>
<tr>
<td>100</td>
<td>Disabled</td>
<td>“show csf service diameter policy-control statistics”</td>
</tr>
<tr>
<td>101</td>
<td>Disabled</td>
<td>“show csf service diameter location-info statistics”</td>
</tr>
<tr>
<td>102</td>
<td>Disabled</td>
<td>“show csf service li-packet-cable statistics”</td>
</tr>
<tr>
<td>103</td>
<td>Disabled</td>
<td>“show csf peer-servers full”</td>
</tr>
<tr>
<td>104</td>
<td>Disabled</td>
<td>“show demux-mgr statistics cscfmgr all”</td>
</tr>
<tr>
<td>105</td>
<td>Disabled</td>
<td>“show lac-service all”</td>
</tr>
<tr>
<td>106</td>
<td>Disabled</td>
<td>“show lns-service all”</td>
</tr>
<tr>
<td>107</td>
<td>Disabled</td>
<td>“show pdnclosedrp-service all”</td>
</tr>
<tr>
<td>108</td>
<td>Enabled</td>
<td>“show subscriber summary”</td>
</tr>
<tr>
<td>109</td>
<td>Enabled</td>
<td>“show connproxy sockets all”</td>
</tr>
<tr>
<td>110</td>
<td>Disabled</td>
<td>“show session progress”</td>
</tr>
<tr>
<td>111</td>
<td>Disabled</td>
<td>“show session subsystem data-info verbose”</td>
</tr>
<tr>
<td>112</td>
<td>Disabled</td>
<td>“show session subsystem full data-info”</td>
</tr>
<tr>
<td>113</td>
<td>Disabled</td>
<td>“show session subsystem facility sessmgr all debug-info”</td>
</tr>
<tr>
<td>114</td>
<td>Disabled</td>
<td>“show sessctrl config-reconciliation statistics”</td>
</tr>
<tr>
<td>115</td>
<td>Disabled</td>
<td>“show rp statistics”</td>
</tr>
<tr>
<td>116</td>
<td>Disabled</td>
<td>“show mipfa statistics”</td>
</tr>
<tr>
<td>117</td>
<td>Disabled</td>
<td>“show mipha statistics”</td>
</tr>
<tr>
<td>118</td>
<td>Disabled</td>
<td>“show mipv6ha statistics”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>119</td>
<td>Disabled</td>
<td>“show lma-service statistics”</td>
</tr>
<tr>
<td>120</td>
<td>Disabled</td>
<td>“show mag-service statistics”</td>
</tr>
<tr>
<td>121</td>
<td>Disabled</td>
<td>“show cli configuration-monitor”</td>
</tr>
<tr>
<td>122</td>
<td>Enabled</td>
<td>“show srp info”</td>
</tr>
<tr>
<td>123</td>
<td>Enabled</td>
<td>“show srp checkpoint statistics”</td>
</tr>
<tr>
<td>124</td>
<td>Disabled</td>
<td>“show srp checkpoint statistics verbose”</td>
</tr>
<tr>
<td>125</td>
<td>Disabled</td>
<td>“show srp checkpoint statistics sessmgr all”</td>
</tr>
<tr>
<td>126</td>
<td>Disabled</td>
<td>“show srp checkpoint statistics ipsecmgr all”</td>
</tr>
<tr>
<td>127</td>
<td>Enabled</td>
<td>“show srp checkpoint statistics sessmgr all write-list-stats”</td>
</tr>
<tr>
<td>128</td>
<td>Disabled</td>
<td>“show srp monitor”</td>
</tr>
<tr>
<td>129</td>
<td>Enabled</td>
<td>“show srp monitor all”</td>
</tr>
<tr>
<td>130</td>
<td>Disabled</td>
<td>“show srp monitor diameter debug”</td>
</tr>
<tr>
<td>131</td>
<td>Enabled</td>
<td>“show srp statistics”</td>
</tr>
<tr>
<td>132</td>
<td>Disabled</td>
<td>“show srp call-loss statistics”</td>
</tr>
<tr>
<td>133</td>
<td>Disabled</td>
<td>“show srp audit-statistics”</td>
</tr>
<tr>
<td>134</td>
<td>Disabled</td>
<td>“show gtpc statistics verbose”</td>
</tr>
<tr>
<td>135</td>
<td>Enabled</td>
<td>“show gtpu statistics verbose”</td>
</tr>
<tr>
<td>136</td>
<td>Enabled</td>
<td>“show gtpu debug-info”</td>
</tr>
<tr>
<td>137</td>
<td>Enabled</td>
<td>“show gmm-sm statistics verbose”</td>
</tr>
<tr>
<td>138</td>
<td>Enabled</td>
<td>“show sgtpc statistics verbose”</td>
</tr>
<tr>
<td>139</td>
<td>Enabled</td>
<td>“show sgtpu statistics”</td>
</tr>
<tr>
<td>140</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all scgp asp all status peer-server all peer-server-process all verbose”</td>
</tr>
<tr>
<td>141</td>
<td>Enabled</td>
<td>“show ss7-routing-domain all scgp asp all statistics gen”</td>
</tr>
<tr>
<td>142</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all m3ua status peer-server all”</td>
</tr>
<tr>
<td>143</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all m3ua statistics peer-server all peer-server-process all”</td>
</tr>
<tr>
<td>144</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all qsaal statistics linkset all link all”</td>
</tr>
<tr>
<td>145</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all ssf statistics linkset all link all”</td>
</tr>
<tr>
<td>146</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all mtp3 status linkset all link all”</td>
</tr>
<tr>
<td>147</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all mtp3 statistics gen”</td>
</tr>
<tr>
<td>148</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all mtp3 statistics linkset all link all”</td>
</tr>
<tr>
<td>149</td>
<td>Disabled</td>
<td>“show ss7-routing-domain all routes”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>150</td>
<td>Disabled</td>
<td>“show sccp-network all status all”</td>
</tr>
<tr>
<td>151</td>
<td>Disabled</td>
<td>“show global-title-translation association”</td>
</tr>
<tr>
<td>152</td>
<td>Disabled</td>
<td>“show global-title-translation address-map”</td>
</tr>
<tr>
<td>153</td>
<td>Enabled</td>
<td>“show egtpc peers”</td>
</tr>
<tr>
<td>154</td>
<td>Disabled</td>
<td>“show egtpc statistics interface mme”</td>
</tr>
<tr>
<td>155</td>
<td>Enabled</td>
<td>“show egtpc statistics interface sgsn”</td>
</tr>
<tr>
<td>156</td>
<td>Enabled</td>
<td>“show egtpc statistics interface sgw-ingress”</td>
</tr>
<tr>
<td>157</td>
<td>Enabled</td>
<td>“show egtpc statistics interface sgw-egress”</td>
</tr>
<tr>
<td>158</td>
<td>Enabled</td>
<td>“show egtpc statistics interface pgw-ingress”</td>
</tr>
<tr>
<td>159</td>
<td>Enabled</td>
<td>“show egtpc statistics interface cgw-egress”</td>
</tr>
<tr>
<td>160</td>
<td>Enabled</td>
<td>“show egtpc statistics interface epdg-egress”</td>
</tr>
<tr>
<td>161</td>
<td>Disabled</td>
<td>“show egtp-service all”</td>
</tr>
<tr>
<td>162</td>
<td>Disabled</td>
<td>“show gtpu-service all”</td>
</tr>
<tr>
<td>163</td>
<td>Disabled</td>
<td>“show pgw-service all”</td>
</tr>
<tr>
<td>164</td>
<td>Disabled</td>
<td>“show sgw-service all”</td>
</tr>
<tr>
<td>165</td>
<td>Disabled</td>
<td>“show saegw-service all”</td>
</tr>
<tr>
<td>166</td>
<td>Disabled</td>
<td>“show henbgw-access-service statistics”</td>
</tr>
<tr>
<td>167</td>
<td>Disabled</td>
<td>“show henbgw-network-service statistics”</td>
</tr>
<tr>
<td>168</td>
<td>Disabled</td>
<td>“show mme-service all”</td>
</tr>
<tr>
<td>169</td>
<td>Disabled</td>
<td>“show mme-service enodeb-association full all”</td>
</tr>
<tr>
<td>170</td>
<td>Disabled</td>
<td>“show mme-service statistics debug”</td>
</tr>
<tr>
<td>171</td>
<td>Disabled</td>
<td>“show mme-service db statistics”</td>
</tr>
<tr>
<td>172</td>
<td>Disabled</td>
<td>“show sgs-service all”</td>
</tr>
<tr>
<td>173</td>
<td>Disabled</td>
<td>“show sgs-service vlr-status full”</td>
</tr>
<tr>
<td>174</td>
<td>Disabled</td>
<td>“show sgs-service statistics all”</td>
</tr>
<tr>
<td>175</td>
<td>Enabled</td>
<td>“show sgw-service statistics all”</td>
</tr>
<tr>
<td>176</td>
<td>Disabled</td>
<td>“show saegw-service statistics all verbose”</td>
</tr>
<tr>
<td>177</td>
<td>Disabled</td>
<td>“show saegw-service statistics all function sgw verbose”</td>
</tr>
<tr>
<td>178</td>
<td>Disabled</td>
<td>“show saegw-service statistics all function pgw verbose”</td>
</tr>
<tr>
<td>179</td>
<td>Enabled</td>
<td>“show pgw-service statistics all”</td>
</tr>
<tr>
<td>180</td>
<td>Disabled</td>
<td>“show sccp statistics”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>181</td>
<td>Disabled</td>
<td>“show tcap statistics”</td>
</tr>
<tr>
<td>182</td>
<td>Disabled</td>
<td>“show map statistics”</td>
</tr>
<tr>
<td>183</td>
<td>Disabled</td>
<td>“show sms statistics”</td>
</tr>
<tr>
<td>184</td>
<td>Disabled</td>
<td>“show pdg-service statistics”</td>
</tr>
<tr>
<td>185</td>
<td>Disabled</td>
<td>“show hnbgw sessmgr all memory statistics”</td>
</tr>
<tr>
<td>186</td>
<td>Disabled</td>
<td>“show hnbgw sessmgr all internal statistics”</td>
</tr>
<tr>
<td>187</td>
<td>Disabled</td>
<td>“show hnbgw disconnect-reasons”</td>
</tr>
<tr>
<td>188</td>
<td>Disabled</td>
<td>“show cs-network statistics”</td>
</tr>
<tr>
<td>189</td>
<td>Disabled</td>
<td>“show ps-network statistics”</td>
</tr>
<tr>
<td>190</td>
<td>Disabled</td>
<td>“show hnbgw statistics”</td>
</tr>
<tr>
<td>191</td>
<td>Disabled</td>
<td>“show hnbgw counters”</td>
</tr>
<tr>
<td>192</td>
<td>Disabled</td>
<td>“show demux-mgr statistics hnbmgr full”</td>
</tr>
<tr>
<td>193</td>
<td>Disabled</td>
<td>“show demuxmgr statistics bngmgr all”</td>
</tr>
<tr>
<td>194</td>
<td>Disabled</td>
<td>“show alcap statistics”</td>
</tr>
<tr>
<td>195</td>
<td>Disabled</td>
<td>“show pdg-service statistics micro-tunnel”</td>
</tr>
<tr>
<td>196</td>
<td>Disabled</td>
<td>“show pdg-service statistics transport”</td>
</tr>
<tr>
<td>197</td>
<td>Disabled</td>
<td>“show demuxmgr statistics a11mgr all”</td>
</tr>
<tr>
<td>198</td>
<td>Disabled</td>
<td>“show demuxmgr statistics famgr all”</td>
</tr>
<tr>
<td>199</td>
<td>Disabled</td>
<td>“show demuxmgr statistics hamgr all”</td>
</tr>
<tr>
<td>200</td>
<td>Disabled</td>
<td>“show demuxmgr statistics l2tpmgr all”</td>
</tr>
<tr>
<td>201</td>
<td>Disabled</td>
<td>“show demuxmgr statistics ipsgmgr all”</td>
</tr>
<tr>
<td>202</td>
<td>Enabled</td>
<td>“show demuxmgr statistics sgtpcmgr all”</td>
</tr>
<tr>
<td>203</td>
<td>Disabled</td>
<td>“show demuxmgr statistics insimgr all”</td>
</tr>
<tr>
<td>204</td>
<td>Enabled</td>
<td>“show demuxmgr statistics gtpcmgr all”</td>
</tr>
<tr>
<td>205</td>
<td>Enabled</td>
<td>“show demuxmgr statistics egtpinmgr all”</td>
</tr>
<tr>
<td>206</td>
<td>Disabled</td>
<td>“show demuxmgr statistics egtpegmgr all”</td>
</tr>
<tr>
<td>207</td>
<td>Disabled</td>
<td>“show demuxmgr statistics pdgdmgmgr all”</td>
</tr>
<tr>
<td>208</td>
<td>Enabled</td>
<td>“show demuxmgr statistics gtpumgr all”</td>
</tr>
<tr>
<td>209</td>
<td>Disabled</td>
<td>“show bcmcs statistics all”</td>
</tr>
<tr>
<td>210</td>
<td>Enabled</td>
<td>“show linkmgr all parser statistics all”</td>
</tr>
<tr>
<td>211</td>
<td>Disabled</td>
<td>“show gtp accounting servers”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>212</td>
<td>Disabled</td>
<td>“show gtpp statistics verbose”</td>
</tr>
<tr>
<td>213</td>
<td>Disabled</td>
<td>“show gtpp counters all”</td>
</tr>
<tr>
<td>214</td>
<td>Disabled</td>
<td>“show gtpp storage-server”</td>
</tr>
<tr>
<td>215</td>
<td>Disabled</td>
<td>“show gtpp storage-server statistics verbose”</td>
</tr>
<tr>
<td>216</td>
<td>Disabled</td>
<td>“show gtpp storage-server local file statistics verbose”</td>
</tr>
<tr>
<td>217</td>
<td>Disabled</td>
<td>“show gtpp storage-server local file counters all”</td>
</tr>
<tr>
<td>218</td>
<td>Disabled</td>
<td>“show gtpp storage-server streaming file statistics verbose”</td>
</tr>
<tr>
<td>219</td>
<td>Disabled</td>
<td>“show gtpp storage-server streaming file counters all”</td>
</tr>
<tr>
<td>220</td>
<td>Disabled</td>
<td>“show gtpp group all”</td>
</tr>
<tr>
<td>221</td>
<td>Enabled</td>
<td>“show hd-storage-policy statistics all verbose”</td>
</tr>
<tr>
<td>222</td>
<td>Enabled</td>
<td>“show hd-storage-policy counters all verbose”</td>
</tr>
<tr>
<td>223</td>
<td>Disabled</td>
<td>“show dhcp statistics verbose”</td>
</tr>
<tr>
<td>224</td>
<td>Disabled</td>
<td>“show npu table”</td>
</tr>
<tr>
<td>225</td>
<td>Disabled</td>
<td>“show npu sf hw-info”</td>
</tr>
<tr>
<td>229</td>
<td>Disabled</td>
<td>“show l2tp statistics”</td>
</tr>
<tr>
<td>230</td>
<td>Enabled</td>
<td>“show fabric asr5500”</td>
</tr>
<tr>
<td>231</td>
<td>Enabled</td>
<td>“show vpn subsystem facility vpnmgr”</td>
</tr>
<tr>
<td>232</td>
<td>Enabled</td>
<td>“show session recovery status verbose”</td>
</tr>
<tr>
<td>233</td>
<td>Enabled</td>
<td>“show clock all”</td>
</tr>
<tr>
<td>234</td>
<td>Disabled</td>
<td>“show sntp statistics verbose”</td>
</tr>
<tr>
<td>235</td>
<td>Disabled</td>
<td>“show llc statistics verbose”</td>
</tr>
<tr>
<td>236</td>
<td>Disabled</td>
<td>“show bssgp statistics verbose”</td>
</tr>
<tr>
<td>237</td>
<td>Disabled</td>
<td>“show bssap+ statistics verbose”</td>
</tr>
<tr>
<td>238</td>
<td>Disabled</td>
<td>“show network-service-entity ip-config”</td>
</tr>
<tr>
<td>239</td>
<td>Disabled</td>
<td>“show network-service-entity fr-config”</td>
</tr>
<tr>
<td>240</td>
<td>Disabled</td>
<td>“show gprsns statistics sns-msg-stats”</td>
</tr>
<tr>
<td>241</td>
<td>Disabled</td>
<td>“show radius authentication servers detail”</td>
</tr>
<tr>
<td>242</td>
<td>Disabled</td>
<td>“show radius accounting servers detail”</td>
</tr>
<tr>
<td>243</td>
<td>Enabled</td>
<td>“show radius counters all”</td>
</tr>
<tr>
<td>245</td>
<td>Enabled</td>
<td>“show rct stats”</td>
</tr>
<tr>
<td>246</td>
<td>Enabled</td>
<td>“show heartbeat stats hatcpu”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>247</td>
<td>Disabled</td>
<td>&quot;show ntp associations all&quot;</td>
</tr>
<tr>
<td>248</td>
<td>Disabled</td>
<td>&quot;show npu details&quot;</td>
</tr>
<tr>
<td>249</td>
<td>Disabled</td>
<td>&quot;show active-charging service all&quot;</td>
</tr>
<tr>
<td>250</td>
<td>Disabled</td>
<td>&quot;show active-charging tcp-proxy statistics all verbose debug-info&quot;</td>
</tr>
<tr>
<td>251</td>
<td>Disabled</td>
<td>&quot;show active-charging edr-udr-file flow-control-counters verbose debug-only&quot;</td>
</tr>
<tr>
<td>252</td>
<td>Disabled</td>
<td>&quot;show active-charging service statistics&quot;</td>
</tr>
<tr>
<td>253</td>
<td>Disabled</td>
<td>&quot;show active-charging analyzer statistics&quot;</td>
</tr>
<tr>
<td>254</td>
<td>Disabled</td>
<td>&quot;show active-charging dns-learnt-ip-addresses statistics sessmgr all verbose&quot;</td>
</tr>
<tr>
<td>255</td>
<td>Disabled</td>
<td>&quot;show active-charging analyzer statistics name ip verbose&quot;</td>
</tr>
<tr>
<td>256</td>
<td>Disabled</td>
<td>&quot;show active-charging analyzer statistics name ipv6 verbose&quot;</td>
</tr>
<tr>
<td>257</td>
<td>Disabled</td>
<td>&quot;show active-charging analyzer statistics name tcp verbose&quot;</td>
</tr>
<tr>
<td>258</td>
<td>Disabled</td>
<td>&quot;show active-charging analyzer statistics name http verbose&quot;</td>
</tr>
<tr>
<td>259</td>
<td>Disabled</td>
<td>&quot;show active-charging charging-action statistics&quot;</td>
</tr>
<tr>
<td>260</td>
<td>Disabled</td>
<td>&quot;show active-charging rulebase statistics&quot;</td>
</tr>
<tr>
<td>261</td>
<td>Disabled</td>
<td>&quot;show active-charging ruledef statistics all charging&quot;</td>
</tr>
<tr>
<td>262</td>
<td>Enabled</td>
<td>&quot;show active-charging ruledef statistics all firewall wide&quot;</td>
</tr>
<tr>
<td>263</td>
<td>Disabled</td>
<td>&quot;show active-charging regex status all&quot;</td>
</tr>
<tr>
<td>264</td>
<td>Disabled</td>
<td>&quot;show active-charging regex statistics memory summary&quot;</td>
</tr>
<tr>
<td>265</td>
<td>Disabled</td>
<td>&quot;show active-charging regex statistics ruledef summary&quot;</td>
</tr>
<tr>
<td>266</td>
<td>Disabled</td>
<td>&quot;show active-charging edr-format statistics&quot;</td>
</tr>
<tr>
<td>267</td>
<td>Disabled</td>
<td>&quot;show active-charging subsystem all debug-only&quot;</td>
</tr>
<tr>
<td>268</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats cumulative all-flows&quot;</td>
</tr>
<tr>
<td>269</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats cumulative http&quot;</td>
</tr>
<tr>
<td>270</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats cumulative ip&quot;</td>
</tr>
<tr>
<td>271</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats cumulative tcp&quot;</td>
</tr>
<tr>
<td>272</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats cumulative udp&quot;</td>
</tr>
<tr>
<td>273</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats max-simultaneous-flows all-flows&quot;</td>
</tr>
<tr>
<td>274</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats max-simultaneous-flows http&quot;</td>
</tr>
<tr>
<td>275</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats max-simultaneous-flows ip&quot;</td>
</tr>
<tr>
<td>276</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats max-simultaneous-flows tcp&quot;</td>
</tr>
<tr>
<td>277</td>
<td>Disabled</td>
<td>&quot;debug acsmgr show flow-stats max-simultaneous-flows udp&quot;</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>278</td>
<td>Disabled</td>
<td>“debug acsmgr show flow-stats duration-based all-flows”</td>
</tr>
<tr>
<td>279</td>
<td>Disabled</td>
<td>“debug acsmgr show flow-stats duration-based tcp”</td>
</tr>
<tr>
<td>280</td>
<td>Disabled</td>
<td>“debug acsmgr show flow-stats duration-based udp”</td>
</tr>
<tr>
<td>281</td>
<td>Disabled</td>
<td>“debug acsmgr show flow-stats lifetime-based all-flows”</td>
</tr>
<tr>
<td>282</td>
<td>Disabled</td>
<td>“debug acsmgr show p2p detection-params sct”</td>
</tr>
<tr>
<td>283</td>
<td>Disabled</td>
<td>“debug acsmgr show rule-optimization-information”</td>
</tr>
<tr>
<td>284</td>
<td>Disabled</td>
<td>“debug sessmgr charging-service show-stats all”</td>
</tr>
<tr>
<td>285</td>
<td>Disabled</td>
<td>“debug acsmgr show memory usage”</td>
</tr>
<tr>
<td>286</td>
<td>Disabled</td>
<td>“debug aaamgr show memory usage”</td>
</tr>
<tr>
<td>287</td>
<td>Disabled</td>
<td>“show active-charging credit-control statistics debug-info”</td>
</tr>
<tr>
<td>288</td>
<td>Disabled</td>
<td>“show active-charging credit-control session-states”</td>
</tr>
<tr>
<td>289</td>
<td>Disabled</td>
<td>“show active-charging credit-control statistics”</td>
</tr>
<tr>
<td>290</td>
<td>Disabled</td>
<td>“show diameter endpoints all”</td>
</tr>
<tr>
<td>291</td>
<td>Disabled</td>
<td>“show diameter endpoints all debug-info”</td>
</tr>
<tr>
<td>292</td>
<td>Disabled</td>
<td>“show diameter route table debug-info”</td>
</tr>
<tr>
<td>293</td>
<td>Disabled</td>
<td>“show diameter peers full debug”</td>
</tr>
<tr>
<td>294</td>
<td>Disabled</td>
<td>“show diameter aaa-statistics”</td>
</tr>
<tr>
<td>295</td>
<td>Disabled</td>
<td>“show diameter aaa-statistics all”</td>
</tr>
<tr>
<td>296</td>
<td>Disabled</td>
<td>“show diameter aaa-statistics debug-info”</td>
</tr>
<tr>
<td>297</td>
<td>Disabled</td>
<td>“show diameter accounting servers debug-info”</td>
</tr>
<tr>
<td>298</td>
<td>Disabled</td>
<td>“show diameter authentication servers debug-info”</td>
</tr>
<tr>
<td>299</td>
<td>Disabled</td>
<td>“show diameter statistics”</td>
</tr>
<tr>
<td>300</td>
<td>Disabled</td>
<td>“show diameter statistics debug-info”</td>
</tr>
<tr>
<td>301</td>
<td>Disabled</td>
<td>“show diameter statistics proxy”</td>
</tr>
<tr>
<td>302</td>
<td>Disabled</td>
<td>“show diameter statistics proxy debug-info”</td>
</tr>
<tr>
<td>303</td>
<td>Disabled</td>
<td>“show diameter dynamic-dictionary all contents”</td>
</tr>
<tr>
<td>304</td>
<td>Disabled</td>
<td>“show active-charging edr-udr-file statistics”</td>
</tr>
<tr>
<td>305</td>
<td>Disabled</td>
<td>“show active-charging firewall statistics debug-info”</td>
</tr>
<tr>
<td>306</td>
<td>Disabled</td>
<td>“show active-charging nat statistics”</td>
</tr>
<tr>
<td>307</td>
<td>Disabled</td>
<td>“show demuxmgr statistics asngwmgr all”</td>
</tr>
<tr>
<td>308</td>
<td>Disabled</td>
<td>“show asngw-service all”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>309</td>
<td>Disabled</td>
<td>“show asngw-service statistics verbose”</td>
</tr>
<tr>
<td>310</td>
<td>Disabled</td>
<td>“show demuxmgr statistics asnpcmgr all”</td>
</tr>
<tr>
<td>311</td>
<td>Disabled</td>
<td>“show asnpc-service all”</td>
</tr>
<tr>
<td>312</td>
<td>Disabled</td>
<td>“show asnpc-service statistics verbose”</td>
</tr>
<tr>
<td>313</td>
<td>Disabled</td>
<td>“show demuxmgr statistics phsgwmgmgr all”</td>
</tr>
<tr>
<td>314</td>
<td>Disabled</td>
<td>“show phsgw-service all”</td>
</tr>
<tr>
<td>315</td>
<td>Disabled</td>
<td>“show phsgw-service statistics verbose”</td>
</tr>
<tr>
<td>316</td>
<td>Disabled</td>
<td>“show demuxmgr statistics phspcmgr all”</td>
</tr>
<tr>
<td>317</td>
<td>Disabled</td>
<td>“show phspc-service all”</td>
</tr>
<tr>
<td>318</td>
<td>Disabled</td>
<td>“show phspc-service statistics verbose”</td>
</tr>
<tr>
<td>319</td>
<td>Disabled</td>
<td>“show demuxmgr statistics magmgr all”</td>
</tr>
<tr>
<td>320</td>
<td>Disabled</td>
<td>“show active-charging content-filtering category policy-id all”</td>
</tr>
<tr>
<td>321</td>
<td>Disabled</td>
<td>“show content-filtering category database all verbose”</td>
</tr>
<tr>
<td>322</td>
<td>Disabled</td>
<td>“show content-filtering category database facility srbmgr all verbose”</td>
</tr>
<tr>
<td>323</td>
<td>Disabled</td>
<td>“show content-filtering category statistics”</td>
</tr>
<tr>
<td>324</td>
<td>Disabled</td>
<td>“show content-filtering category statistics facility srbmgr all”</td>
</tr>
<tr>
<td>325</td>
<td>Disabled</td>
<td>“show active-charging content-filtering category statistics”</td>
</tr>
<tr>
<td>326</td>
<td>Disabled</td>
<td>“show active-charging content-filtering server-group statistics verbose”</td>
</tr>
<tr>
<td>327</td>
<td>Disabled</td>
<td>“show active-charging url-blacklisting statistics”</td>
</tr>
<tr>
<td>328</td>
<td>Disabled</td>
<td>“show url-blacklisting database all”</td>
</tr>
<tr>
<td>329</td>
<td>Disabled</td>
<td>“show url-blacklisting database facility acsmgr all”</td>
</tr>
<tr>
<td>330</td>
<td>Disabled</td>
<td>“show active-charging tethering-detection database”</td>
</tr>
<tr>
<td>331</td>
<td>Disabled</td>
<td>“show active-charging tethering-detection database sessmgr all”</td>
</tr>
<tr>
<td>332</td>
<td>Disabled</td>
<td>“show active-charging tethering-detection statistics”</td>
</tr>
<tr>
<td>333</td>
<td>Disabled</td>
<td>“show ims-authorization service statistics”</td>
</tr>
<tr>
<td>334</td>
<td>Disabled</td>
<td>“show ims-authorization policy-control statistics”</td>
</tr>
<tr>
<td>335</td>
<td>Disabled</td>
<td>“show ims-authorization policy-control statistics debug-info”</td>
</tr>
<tr>
<td>336</td>
<td>Disabled</td>
<td>“show local-policy statistics summary”</td>
</tr>
<tr>
<td>337</td>
<td>Disabled</td>
<td>“show rohc statistics”</td>
</tr>
<tr>
<td>338</td>
<td>Disabled</td>
<td>“show dns client statistics”</td>
</tr>
<tr>
<td>339</td>
<td>Disabled</td>
<td>“show hss-peer-service service all”</td>
</tr>
<tr>
<td>No.</td>
<td>Default SDR</td>
<td>Command String</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>340</td>
<td>Disabled</td>
<td>“show ipms status all”</td>
</tr>
<tr>
<td>341</td>
<td>Disabled</td>
<td>“show ipms status debug-info”</td>
</tr>
<tr>
<td>342</td>
<td>Disabled</td>
<td>“show kvstore”</td>
</tr>
<tr>
<td>343</td>
<td>Disabled</td>
<td>“show kvstore verbose”</td>
</tr>
<tr>
<td>344</td>
<td>Disabled</td>
<td>“show kvstore kvclient”</td>
</tr>
<tr>
<td>345</td>
<td>Disabled</td>
<td>“show kvstore kvmgr”</td>
</tr>
<tr>
<td>346</td>
<td>Disabled</td>
<td>“show pcc-service all”</td>
</tr>
<tr>
<td>347</td>
<td>Disabled</td>
<td>“show pcc-service statistics all”</td>
</tr>
<tr>
<td>348</td>
<td>Disabled</td>
<td>“show pcc-policy service all”</td>
</tr>
<tr>
<td>349</td>
<td>Disabled</td>
<td>“show pcc-policy service statistics all”</td>
</tr>
<tr>
<td>350</td>
<td>Disabled</td>
<td>“show pcc-quota service all”</td>
</tr>
<tr>
<td>351</td>
<td>Disabled</td>
<td>“show pcc-quota service statistics all”</td>
</tr>
<tr>
<td>352</td>
<td>Disabled</td>
<td>“show pcc-af service all”</td>
</tr>
<tr>
<td>353</td>
<td>Disabled</td>
<td>“show pcc-af service statistics all”</td>
</tr>
<tr>
<td>354</td>
<td>Disabled</td>
<td>“show pcc-sp-endpoint all”</td>
</tr>
<tr>
<td>355</td>
<td>Disabled</td>
<td>“show pcc-sp-endpoint statistics all”</td>
</tr>
<tr>
<td>356</td>
<td>Disabled</td>
<td>“show event-notif server all”</td>
</tr>
<tr>
<td>357</td>
<td>Disabled</td>
<td>“show event-notif statistics”</td>
</tr>
<tr>
<td>358</td>
<td>Disabled</td>
<td>“show demux-mgr statistics bindmux all”</td>
</tr>
<tr>
<td>359</td>
<td>Disabled</td>
<td>“show congestion-control configuration”</td>
</tr>
<tr>
<td>360</td>
<td>Disabled</td>
<td>“show congestion-control statistics mme full”</td>
</tr>
<tr>
<td>361</td>
<td>Disabled</td>
<td>“show congestion-control statistics imsimgr all full”</td>
</tr>
<tr>
<td>365</td>
<td>Disabled</td>
<td>“show cli history”</td>
</tr>
<tr>
<td>367</td>
<td>Disabled</td>
<td>“show sls-service all”</td>
</tr>
<tr>
<td>368</td>
<td>Disabled</td>
<td>“show sls-service peers all”</td>
</tr>
<tr>
<td>369</td>
<td>Disabled</td>
<td>“show sls-service statistics all”</td>
</tr>
</tbody>
</table>

Notes:
- Enabled = Included in default record section
- Disabled = Not included in default record section