



# Cisco USC 8000 Series OS Administrator Guide, Release 4.1

First Published: February 20, 2015

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



# Table of Contents

<b>Chapter 1 Overview .....</b>	<b>1</b>
1.1 About this Manual .....	1
1.2 Product Description .....	2
1.2.1 The USC 8088 Controller .....	2
1.2.1.1 Overview of the USC 8088 Controller Features .....	3
1.2.2 The Dual-Radio Small Cell .....	3
1.2.2.1 Overview of Small Cell Features .....	4
1.3 The Data Model .....	5
1.4 Data Model Managed Objects .....	5
1.5 Relationship between Small Cells, Radios, and Cells .....	6
1.6 Small Cell Boot Sequence .....	7
1.7 Provisioning Sequence .....	8
1.8 Configuration Sequence .....	8
1.9 Document Conventions .....	9
1.10 The Cisco USC 8000 Series Documentation Set .....	10
<b>Chapter 2 The OS CLI .....</b>	<b>11</b>
2.1 CLI Overview .....	11
2.2 System Components .....	12
2.3 Command Modes .....	13
2.3.1 The Candidate Configuration and the Commit Command .....	13
2.3.2 Operational Mode Commands in the Configuration Mode .....	13
2.4 Navigating the CLI .....	13
2.5 Command Hierarchy .....	14
2.5.1 Root Level Commands .....	15
2.6 Working in the Configuration Mode .....	16
2.6.1 Entering and Navigating the Configuration Mode .....	16
2.6.2 Entering Configuration Mode Commands .....	16
2.6.3 Using Show Commands as Provisioning Aids .....	17
2.6.4 Deleting Objects .....	18
2.6.5 Screen Display Truncation .....	18
2.7 Frequently Used Commands .....	19
2.8 Logging into the CLI .....	20
2.9 Show Commands .....	20

2.9.1 Processing Command Output . . . . .	20
2.9.2 Filtering Output with Regular Expressions. . . . .	21
2.10 The Fetch Command . . . . .	22
2.10.1 Indexes . . . . .	23
2.11 Configuring CLI Settings . . . . .	23
2.11.1 Viewing the Current CLI Settings. . . . .	23
2.11.2 Configuring the Display Banner. . . . .	24
2.11.3 Configuring the Idle Timeout . . . . .	24
2.11.4 Configuring CLI Session Parameters . . . . .	25
2.11.4.1 Configuring the Number of CLI Sessions per User . . . . .	25
2.11.4.2 Configuring the Total Number of CLI Sessions . . . . .	25
2.11.5 Viewing CLI Administrator Sessions . . . . .	25
2.11.6 Logging a User Off the System . . . . .	25
2.12 Managing the Configuration . . . . .	25
2.12.1 Displaying the Running Configuration . . . . .	26
2.12.2 Displaying the Candidate Configuration . . . . .	27
2.12.3 Displaying Changes in the Candidate Configuration . . . . .	27
2.12.4 Discarding Edits. . . . .	28
2.12.5 Saving the Running Configuration. . . . .	28
2.12.6 Backing Up the Running Configuration . . . . .	29
2.12.7 Loading and Merging a Configuration File. . . . .	29
<b>Chapter 3 Initial Configuration . . . . .</b>	<b>31</b>
3.1 Configuring the USC 8088 Controller for eRMS . . . . .	31
3.2 Configuring General System Parameters . . . . .	32
3.3 Setting the System Date and Time . . . . .	32
3.4 Configuring the USC 8088 Controller Time Zone . . . . .	33
3.4.1 Setting the USC 8088 Controller Time Zone . . . . .	33
3.4.2 Configuring a Custom USC 8088 Controller Time Zone . . . . .	33
3.5 Configuring Equipment Location . . . . .	34
3.5.1 Configuring the USC 8088 Controller Location . . . . .	35
3.5.1.1 Configuring GNSS Location Determination and Reporting . . . . .	35
3.5.1.2 Configuring the USC 8088 Controller Location Manually . . . . .	36
3.5.2 Small Cell Location . . . . .	36
<b>Chapter 4 IP Configuration . . . . .</b>	<b>39</b>
4.1 IP Networking. . . . .	39
4.1.1 Changing the Default IP Address . . . . .	39
4.1.2 Configuring an Ethernet Port IP Address. . . . .	40
4.1.3 Setting the Ethernet Port Speed . . . . .	40
4.1.4 Viewing IP Interface Configurations. . . . .	40
4.1.4.1 show Interface . . . . .	40
4.1.4.2 show Interface Detail. . . . .	41
4.1.4.3 show Interface Verbose. . . . .	42
4.1.5 Resetting Interface Statistics . . . . .	42

4.1.6 Configuring VLANs . . . . .	43
4.1.7 Configuring Ethernet Port Link Aggregation . . . . .	44
4.1.8 Configuring Static Routes . . . . .	45
4.1.9 Configuring the USC 8088 Controller DHCP Server . . . . .	46
4.1.9.1 Default Port 2 DHCP Server Settings . . . . .	46
4.1.9.2 Modifying DHCP Server Settings . . . . .	46
4.1.9.3 Default Port 4 DHCP Server Settings . . . . .	47
4.1.9.4 Disabling the DHCP Server on an IP Interface . . . . .	47
4.1.9.5 Configuring the DHCP Server for Third-Party Equipment . . . . .	48
4.1.10 Configuring IP Forwarding Groups . . . . .	48
4.1.11 SSH TCP Port Forwarding . . . . .	49
4.1.12 Configuring Network Time Synchronization . . . . .	49
4.1.13 Configuring DNS Lookup and Domain Search using a Name Server . . . . .	50
4.1.14 Configuring Static Name Resolution . . . . .	51
4.1.15 Configuring IP Routing . . . . .	51
4.1.15.1 Configuring Dynamic Routing to the Core Network . . . . .	51
4.1.15.2 Configuring Virtual Routing and Forwarding . . . . .	53
4.1.15.3 Configuring Static Route Metrics . . . . .	54
4.2 Configuring Certificate Revocation Policies . . . . .	55
4.3 Configuring IPsec to the Core Network . . . . .	56
4.3.1 Before You Begin . . . . .	58
4.3.2 Importing the Security Gateway Trusted Root Certificate . . . . .	58
4.3.3 Configuring the IPsec Tunnel for UMTS Traffic . . . . .	59
4.3.4 Configuring the IPsec Tunnel for LTE Traffic . . . . .	62
4.4 Configuring a 6in4 Tunnel to the Core Network . . . . .	66
4.4.1 Configuring a 6in4 Tunnel Using an IPsec Virtual Interface . . . . .	67
4.4.2 Configuring a 6in4 Tunnel Using a Local IP Address . . . . .	68
4.5 Configuring IPsec to the Small Cell . . . . .	68
4.6 Deployment Considerations with a Firewall . . . . .	69
4.6.1 USC 8088 Controller Deployed Outside the Enterprise Intranet . . . . .	70
4.6.2 USC 8088 Controller Deployed Inside the Enterprise Intranet . . . . .	71
4.6.3 Firewall Inside the Core Network . . . . .	72
4.6.3.1 UMTS Iu/IP Firewall Considerations . . . . .	72
4.6.3.2 UMTS Iuh Firewall Considerations . . . . .	73
4.6.3.3 LTE S1 Firewall Considerations . . . . .	74
4.6.3.4 Dual-Mode Firewall Considerations . . . . .	75
<b>Chapter 5 UMTS Radio Access Network . . . . .</b>	<b>77</b>
5.1 Configuring the Core UMTS Network . . . . .	77
5.1.1 Deleting the Existing Configuration . . . . .	79
5.1.2 Configuring UMTS Core Network Settings . . . . .	79
5.1.2.1 Configuring Core Network Iu Settings . . . . .	80
5.1.2.2 Configuring Core Network Iuh Settings . . . . .	81
5.1.2.3 UMTS Cell Provisioning Timer . . . . .	83

5.1.3 Configuring Home NodeB Gateway Redundancy . . . . .	83
5.2 Configuring UMTS Femto Access Point Service . . . . .	85
5.3 Configuring Small Cells and Cells . . . . .	86
5.3.1 Adding Small Cells and Cells with Auto Provisioning . . . . .	86
5.3.2 Adding a Small Cell and a Cell Manually . . . . .	89
5.3.3 Deleting a Small Cell and a Cell . . . . .	90
5.4 Disabling and Enabling Cell Transmission . . . . .	91
5.5 Configuring Multi-Operator Core Networks . . . . .	91
5.6 Enabling Optional Features . . . . .	93
5.6.1 Configuring High-Capacity Networks . . . . .	93
5.6.2 Enabling Enhanced Coverage . . . . .	94
5.6.3 Configuring Downlink Higher Order Modulation . . . . .	94
<b>Chapter 6 LTE Radio Access Network . . . . .</b>	<b>97</b>
6.1 Configuring the Core Network LTE Services . . . . .	97
6.1.1 Deleting the Existing Configuration . . . . .	99
6.1.2 Configuring Core Network Settings . . . . .	99
6.1.2.1 Configuring Core Network LTE Settings . . . . .	100
6.1.2.2 LTE Cell Provisioning Timer . . . . .	101
6.1.3 Configuring LTE S1 Load Redundancy and Load Balancing . . . . .	101
6.1.4 Enabling Dual-Band LTE Idle-Mode UE Load Balancing . . . . .	102
6.2 Configuring LTE Femto Access Point Service . . . . .	103
6.3 Configuring Small Cells and Cells . . . . .	104
6.3.1 Adding a Small Cell and a Cell Manually . . . . .	104
6.3.2 Deleting a Small Cell and a Cell . . . . .	106
6.4 Disabling and Enabling Cell Transmission . . . . .	106
<b>Chapter 7 UMTS RF Management . . . . .</b>	<b>107</b>
7.1 RF Management Configuration Overview . . . . .	108
7.2 Initial System Provisioning with the LCI . . . . .	108
7.3 Before You Begin . . . . .	108
7.4 Initial UMTS RF Management Provisioning . . . . .	108
7.4.1 Enabling UMTS RF Management . . . . .	108
7.4.2 Placing the USC 8088 Controller In Service . . . . .	109
7.5 Basic UMTS REM Scanning . . . . .	109
7.5.1 Configuring Basic and Periodic Scanning Parameters . . . . .	109
7.5.2 Configuring Primary Scrambling Codes . . . . .	110
7.5.2.1 Designating Primary Scrambling Codes for the small cell solution . . . . .	111
7.5.2.2 Configuring Alternate Primary Scrambling Codes . . . . .	111
7.5.3 Configuring the Power Transmission Range . . . . .	112
7.5.3.1 Configuring Periodic Power Reassignment . . . . .	113
7.5.4 Initial UMTS Self-Configuration . . . . .	113
7.5.5 Aborting a UMTS REM Scan . . . . .	113
7.6 The Maximum UMTS Cell Transmit Power . . . . .	114
7.6.1 Configuring the Maximum UMTS Cell Transmit Power . . . . .	114

7.6.2 Configuring Location-Based Power Allocation . . . . .	114
7.6.3 Configuring the Maximum Cell Power Level Delta . . . . .	115
7.7 Viewing UMTS RF Management Configurations . . . . .	116
7.7.1 Viewing the UMTS RF Management Configuration . . . . .	116
7.7.2 Viewing UMTS REM Scan Results . . . . .	116
7.8 Advanced RF Management . . . . .	118
7.8.1 Training the System to Set Cell Power Levels . . . . .	118
7.8.2 Provisioning UMTS Neighbor Lists . . . . .	119
7.8.3 Adding or Deleting a UMTS Cell from an Operational Network . . . . .	120
7.8.4 Excluding a Cell from all small cell solution Neighbor Lists . . . . .	121
7.8.5 Including and Excluding a Neighbor for a UMTS Single Cell . . . . .	121
7.8.6 Creating the Final UMTS Neighbor List . . . . .	122
7.8.7 Bypassing UMTS REM Scan Topology Components . . . . .	123
7.8.8 Manually Assigning Primary Scrambling Codes . . . . .	124
7.8.9 Manually Assigning Maximum Power Transmission Levels . . . . .	124
7.8.10 UMTS REM Scan Locking . . . . .	124
7.8.10.1 Locking System-Wide UMTS Cell RF Attributes During REM Scan	125
7.8.10.2 Locking Attributes of a Single Cell During a UMTS REM Scan . . .	125
7.8.10.3 Locking System-Wide Primary Scrambling Codes . . . . .	126
7.8.10.4 Locking Single Cell Primary Scrambling Codes . . . . .	126
7.8.10.5 Locking System-Wide Maximum Power Transmission Levels . . . .	126
7.8.10.6 Locking Single Cell Maximum Power Transmission Levels . . . .	126
7.8.10.7 Locking System-Wide UMTS Neighbor Lists . . . . .	127
7.8.10.8 Locking Single Cell Neighbor Lists . . . . .	127
7.8.11 Reinitializing the UMTS RF Management Suite . . . . .	127
7.9 Self-Configuration Zones . . . . .	128
7.9.1 Managing Zones . . . . .	129
7.9.1.1 Creating a Zone . . . . .	129
7.9.1.2 Adding a Cell to a Zone . . . . .	130
7.9.1.3 Enabling all Cells in a Zone . . . . .	130
7.9.1.4 Disabling all Cells in a Zone . . . . .	130
7.9.1.5 Deleting a Cell from a Zone . . . . .	130
7.9.1.6 Moving a Cell to a Different SONConfig Zone . . . . .	131
7.9.1.7 Creating a UMTS Zone Reference Neighborhood List . . . . .	131
7.9.1.8 Deleting a UMTS Zone Reference Neighborhood List . . . . .	131
7.9.1.9 Deleting a UMTS Zone Detected Neighborhood List . . . . .	132
7.9.1.10 Deleting a Zone . . . . .	132
7.9.1.11 Viewing the Zone Configuration . . . . .	132
7.9.1.12 Viewing the Default SONConfigAndScan Zone . . . . .	133
7.9.1.13 Executing a REM Scan on a Zone . . . . .	134
7.9.1.14 Assigning Cell Transmit Power Levels to a Zone . . . . .	135
7.9.1.15 Configuring Maximum Cell Transmit Power in a Zone . . . . .	135
7.9.2 Locking Cells in a Zone . . . . .	136
7.9.2.1 Locking Zone-Wide Cell RF Attributes During REM Scan . . . . .	137

7.9.2.2 Locking Zone-Wide Primary Scrambling Codes . . . . .	137
7.9.2.3 Locking Zone-Wide Maximum Power Transmission Levels . . . . .	137
7.9.2.4 Locking Zone-Wide Neighbor Lists . . . . .	137
7.9.3 Alternative RF Management Scenarios . . . . .	138
7.9.3.1 Turning up a Multi-Building Campus . . . . .	138
7.9.3.2 Initiating Fast Scanning for Changes in the External RF Environment	139
7.9.3.3 Detecting Changes in the GSM Environment . . . . .	141
<b>Chapter 8 LTE RF Management . . . . .</b>	<b>145</b>
8.1 LTE RF Management Configuration Overview . . . . .	145
8.2 Initial System Provisioning with the LCI . . . . .	146
8.3 Before You Begin . . . . .	146
8.4 Initial LTE RF Management Provisioning . . . . .	146
8.4.1 Enabling LTE RF Management . . . . .	146
8.4.2 Placing the USC 8088 Controller In Service . . . . .	146
8.5 Basic LTE REM Scanning . . . . .	147
8.5.1 Configuring Basic Scanning Parameters . . . . .	147
8.5.2 Configuring Physical Cell IDs . . . . .	148
8.5.2.1 Designating Physical Cell IDs for the small cell solution . . . . .	148
8.5.3 Initial LTE Self-Configuration . . . . .	148
8.5.4 Aborting an LTE REM Scan . . . . .	148
8.6 LTE Cell Transmit Power . . . . .	149
8.6.1 Configuring the Maximum LTE Cell Transmit Power for all Cells . . . . .	149
8.6.2 Configuring the Transmit Power for an Individual Cell . . . . .	149
8.6.3 Configuring REM Scan-Based LTE Power Assignments . . . . .	150
8.7 Viewing LTE RF Management Configurations . . . . .	150
8.7.1 Viewing the LTE RF Management Configuration . . . . .	150
8.7.2 Viewing LTE REM Scan Results . . . . .	151
8.8 Advanced RF Management . . . . .	152
8.8.1 Provisioning LTE Neighbor Lists . . . . .	152
8.8.2 Adding or Deleting an LTE Cell from an Operational Network . . . . .	154
8.8.3 Excluding a Cell from all small cell solution Neighbor Lists . . . . .	154
8.8.4 Creating the Final Neighbor List . . . . .	154
8.8.5 Bypassing LTE REM Scan Topology Components . . . . .	155
8.8.6 Manually Assigning Physical Cell IDs . . . . .	156
8.8.7 LTE REM Scan Locking . . . . .	156
8.8.7.1 Locking System-Wide LTE Cell RF Attributes During REM Scan . . . . .	156
8.8.7.2 Locking System-Wide Physical Cell IDs . . . . .	157
8.8.7.3 Locking System-Wide LTE Neighbor Lists . . . . .	157
8.8.9 Centrally-Coordinated Dynamic Fractional Frequency Reuse . . . . .	157
<b>Chapter 9 LTE Zones . . . . .</b>	<b>159</b>
9.1 Creating an LTE Zone . . . . .	159
<b>Chapter 10 Access Control Topics . . . . .</b>	<b>161</b>
10.1 Open Subscriber Groups . . . . .	161

10.2 Closed Subscriber Groups .....	161
10.2.1 Adding Users through the Web Interface .....	163
10.3 UMTS Admission Control .....	166
10.4 LTE Admission Control .....	168
10.4.1 Configuring the Maximum Number of UEs LTE Per-Cell .....	168
10.4.2 Configuring the LTE Emergency Priority Level .....	169
<b>Chapter 11 Regulatory Features .....</b>	<b>171</b>
11.1 Configuring Emergency Calls .....	171
11.1.1 Emergency Call Redirect .....	171
11.1.1.1 Redirecting Emergency Call Traffic .....	171
11.1.1.2 Assigning Emergency Call Priority Levels .....	172
11.1.2 Configuring ACCOLC .....	172
11.3 LTE Public Warning Systems .....	173
11.4 Restricting LTE Cell Access .....	174
11.5 Configuring UMTS Cell Broadcast Services .....	175
<b>Chapter 12 Session Management .....</b>	<b>177</b>
12.1 Overview .....	177
12.2 Configuring Policies .....	178
12.2.1 Configuring User Blacklists .....	181
12.3 Configuring Local Switching .....	182
12.4 Configuring UMTS Walled Garden Access .....	183
12.4.1 Configuring Classification Groups .....	183
12.4.2 Configuring Walled Garden DNS Support .....	185
12.4.2.1 Wildcard Support .....	186
12.5 User Configuration Examples .....	186
12.5.1 Defining Users in the RAN .....	187
12.5.1.1 UE1 (Guest) .....	187
12.5.1.2 UE2 (Engineer) .....	189
12.5.1.3 UE3 (Business) .....	192
12.5.1.4 UE4 (Engineer) .....	195
<b>Chapter 13 IP QoS and Filtering .....</b>	<b>199</b>
13.1 Configuring IP Quality of Service .....	199
13.1.1 Class of Service .....	199
13.1.2 Configuring Packet Queuing and Scheduling .....	199
13.1.3 Default CoS Markings for Output Traffic .....	201
13.1.4 Editing Default Control Plane CoS Markings .....	201
13.1.4.1 Configuring Control Plane CoS code point classifications .....	201
13.1.4.2 Configuring Control Plane Classification Groups .....	201
13.1.5 LTE QoS Differentiation .....	202
13.2 Configuring Egress IP Quality of Service .....	203
13.2.1 Configuring 802.1Q Priority Code Point Behavior .....	205

13.3 Configuring IP Interface Filtering .....	205
<b>Chapter 14 UMTS Mobility .....</b>	<b>207</b>
14.1 Cell Connection States .....	207
14.1.1 Enabling Fast Dormancy .....	208
14.1.2 CELL_FACH and Admission Control.....	209
14.2 Handover .....	209
14.3 Multiple Ingress Macro Hand-In.....	210
14.3.1 Disambiguation of Target Hand-in Cell .....	210
14.3.2 Configuring Multiple Ingress Hand-In .....	211
14.4 Target Cell ID-Based Hand-In .....	213
14.5 Cell Selection and Re-Selection .....	213
14.6 Enabling Cell Re-Selection from UMTS to LTE .....	215
14.7 Creating UMTS Proximity Detection Cells .....	216
<b>Chapter 15 LTE Mobility .....</b>	<b>217</b>
15.1 Handover .....	217
15.2 Cell Selection and Re-Selection .....	218
15.3 Enabling Cell Re-Selection from UMTS to LTE .....	219
15.4 Enabling LTE Idle Mode Cell Re-Selection .....	220
15.5 Creating LTE Proximity Detection Cells.....	222
<b>Chapter 16 System Scaling .....</b>	<b>225</b>
16.1 Configuring UMTS System Session Rates .....	225
16.1.1 Configuring UMTS Maximum Session Rates .....	225
16.1.2 Configuring UMTS System Session Transition Rates.....	226
16.2 Adjusting the UMTS TCP MSS .....	226
16.3 Adjusting the LTE TCP MSS .....	228
<b>Chapter 17 System Management .....</b>	<b>231</b>
17.1 Overview .....	231
17.2 The Local Configuration Interface .....	231
17.3 Fault Management.....	232
17.3.1 Events .....	233
17.3.1.1 Anatomy of an Event .....	234
17.3.2 Conditions .....	235
17.3.3 Alarms .....	235
17.4 User Administration .....	238
17.4.1 Enabling the Read-Only Administrator .....	240
17.4.2 Editing User Attributes .....	240
17.4.3 Changing User Passwords .....	241
17.5 SNMP .....	241
17.5.1 Supported Standard MIBs .....	242
17.5.2 Standard Supported Traps .....	242
17.5.3 Standard Trap Details .....	243

17.5.3.1 authenticationFailure . . . . .	243
17.5.3.2 coldStart . . . . .	243
17.5.3.3 linkDown . . . . .	243
17.5.3.4 linkUp . . . . .	244
17.5.3.5 warmStart . . . . .	244
17.5.4 Small Cell Solution Proprietary MIBs . . . . .	244
17.5.5 Small Cell Solution Traps Parameters . . . . .	245
17.5.6 Small Cell Solution Trap Messages . . . . .	245
17.5.7 Supported SNMP Operations . . . . .	246
17.5.8 Enabling SNMP and Setting the SNMP Version . . . . .	247
17.5.9 Configuring SNMP System Parameters . . . . .	247
17.5.10 Viewing SNMP Parameters . . . . .	247
17.5.11 Viewing the SNMP Configuration . . . . .	248
17.5.12 Trap Forwarding for Third-Party Devices . . . . .	248
17.5.13 Disabling and Reactivating the SNMP Agent . . . . .	248
17.5.14 Monitoring Ports and Interfaces . . . . .	248
17.5.15 Configuring SNMP Trap Targets . . . . .	249
17.5.16 Example Trap Target Configurations . . . . .	251
17.5.16.1 Example SNMP v2c Traps or Inform Targets . . . . .	251
17.5.16.2 Example SNMP v3 Trap Targets . . . . .	251
17.5.16.3 Example SNMP v3 Inform Targets . . . . .	252
17.5.17 Generating Test SNMP Traps . . . . .	252
17.5.17.1 Generating a Test SNMP Trap for All Trap Targets . . . . .	252
17.5.17.2 Generating a Test SNMP Trap to a Defined Trap Target . . . . .	252
17.5.17.3 Generating All SNMP Traps . . . . .	252
17.5.17.4 Generating SNMP Traps of a Defined Severity . . . . .	253
17.5.17.5 Clearing All SNMP Traps . . . . .	253
17.5.17.6 Clearing a Defined SNMP Trap . . . . .	253
17.5.17.7 Generating Standard Traps . . . . .	253
17.5.18 Configuring SNMP Source Address Filtering . . . . .	253
17.5.19 Viewing SNMP Inform Statistics . . . . .	254
17.5.20 Disabling SNMP Trap Notifications . . . . .	255
17.5.21 SNMP Authentication, Authorization, and Accounting . . . . .	255
17.5.22 SNMP Proxy . . . . .	256
17.6 Syslog . . . . .	257
17.6.1 Defining Syslog Filters . . . . .	258
17.6.2 Configuring Syslog Targets . . . . .	259
17.6.3 Viewing Configured Syslog Targets . . . . .	260
17.6.4 Resetting Syslog Counters . . . . .	260
17.7 Performance Management . . . . .	260
17.7.1 Configuring Data Collection . . . . .	261
17.7.2 Viewing PM Statistics . . . . .	262
17.7.3 Configuring Performance Management Reports . . . . .	263
17.7.4 Resetting PM Counters . . . . .	265

17.7.5 Deleting PM Statistics . . . . .	265
17.7.6 Viewing Real-Time Resource Usage . . . . .	265
17.7.7 Tracking Unique User Devices . . . . .	266
17.7.8 Tracking User Visit Duration . . . . .	267
<b>Chapter 18 System Maintenance . . . . .</b>	<b>269</b>
18.1 Managing Files . . . . .	269
18.1.1 Using the file list Command . . . . .	269
18.1.2 Using the file show Command . . . . .	270
18.1.3 Using the file match Command . . . . .	271
18.1.4 Using the file get Command . . . . .	272
18.1.5 Using the file put Command . . . . .	272
18.1.6 Using the file archive Command . . . . .	273
18.1.7 Using the file delete Command . . . . .	273
18.1.8 Using the file storage cleanup Command . . . . .	274
18.1.9 Rotating Debug Log Files . . . . .	274
18.1.10 Configuring a Remote Server for Log Files . . . . .	274
18.1.11 UMTS Call Performance Event Report Files . . . . .	275
18.1.12 LTE Call Performance Event Report Logs . . . . .	277
18.2 Backing Up and Restoring the Database . . . . .	278
18.2.1 Backing Up the Database . . . . .	279
18.2.2 Restoring the Database . . . . .	279
18.3 Downloading, Upgrading, and Reverting . . . . .	280
18.3.1 Displaying the Software Image Version . . . . .	280
18.3.2 Copying the Software Image and Update . . . . .	281
18.3.3 Reverting to the Previous Image . . . . .	282
18.4 Replacing a Small Cell . . . . .	282
18.5 Rebooting the System . . . . .	283
<b>Chapter 19 Troubleshooting . . . . .</b>	<b>285</b>
19.1 USC 8088 Controller Diagnostics . . . . .	285
19.1.1 Field Recovery User Overview . . . . .	286
19.1.2 Configuring the Field Recovery User . . . . .	286
19.1.2.1 Enabling the Field Recovery User . . . . .	286
19.1.2.2 Disabling the Field Recovery User . . . . .	286
19.1.2.3 Changing the Field Recovery User Password . . . . .	287
19.1.3 Configuring Console Access for the Field Recovery User . . . . .	287
19.1.4 Configuring Console Access for the Administrative User . . . . .	287
19.1.5 Resetting the USC 8088 Controller to the Factory Default . . . . .	288
19.2 Creating a Bundle of Error Log Files . . . . .	288
19.3 Small Cell LED Management . . . . .	289
19.4 Small Cell LED Boot Sequence . . . . .	290
19.5 Locating Small Cell . . . . .	291
19.6 Follow an IMSI . . . . .	292
19.7 Small Cell Link Test . . . . .	292

19.8 Service Affecting Actions .....	293
19.8.1 USC 8088 Controller Reboots .....	293
19.8.2 Small Cell Reboots .....	294
19.8.3 Non-Rebooting Events and Actions .....	294
19.8.4 Actions Requiring a Reboot .....	294
<b>Chapter A Operational States .....</b>	<b>295</b>
<b>Chapter B Miscellaneous Show Commands .....</b>	<b>297</b>
B.1 Sample Show Commands .....	298
B.1.1 show configuration .....	298
B.1.2 show Core .....	299
B.1.3 show FAPService 1 CellConfig UMTS RAN FDDFAP PagingRetryCount .....	299
B.1.4 show FAPService 1 CellConfig UMTS RAN FDDFAP PowerRampSetup .....	299
B.1.5 show FAPService 1 FAPControl UMTS HomeNodeB .....	299
B.1.6 show IP ARP .....	300
B.1.7 show IP Route .....	300
B.1.8 show IP Route Configured .....	300
B.1.9 show IP Route Configured Detail .....	300
B.1.10 show RadioNode .....	301
B.1.11 show RadioNode Radio .....	301
B.1.12 show RFMgmt UMTS .....	301
B.1.13 show ServicesNode .....	303
B.1.14 show Session .....	303
B.1.15 show Session Detail UEIPAddress .....	303
B.1.16 show Session Detail UENATIPAddress .....	304
B.1.17 show Session UMTS Detail SessionID .....	304
B.1.18 show Session UMTS Summary .....	305
B.1.19 show status .....	305
B.1.20 show System File Target .....	305
B.1.21 show System File Transfer History .....	306
B.1.22 show System UMTS Detail .....	306
B.1.23 show UE Location .....	306





# 1 Overview

This chapter contains the following sections:

- [Section 1.1, About this Manual](#) on page 1
- [Section 1.2, Product Description](#) on page 2
- [Section 1.3, The Data Model](#) on page 5
- [Section 1.4, Data Model Managed Objects](#) on page 5
- [Section 1.5, Relationship between Small Cells, Radios, and Cells](#) on page 6
- [Section 1.6, Small Cell Boot Sequence](#) on page 7
- [Section 1.7, Provisioning Sequence](#) on page 8
- [Section 1.8, Configuration Sequence](#) on page 8
- [Section 1.9, Document Conventions](#) on page 9
- [Section 1.10, The Cisco USC 8000 Series Documentation Set](#) on page 10

## 1.1 About this Manual

This guide provides a description of the key features and functionalities of the Cisco small cell solution and the operating system (OS) that manages it. The guide provides the high-level and detailed information with examples of provisioning and maintenance procedures using the OS Command Line Interface (CLI). Use this guide as a resource to assist you in provisioning, operating, and maintaining the system with the CLI.

This guide is designed to be used in conjunction with the *Cisco 8000 Series OS Data Model Reference Guide*. Refer to the data model reference for details about objects and parameters that comprise the system configuration and operational state.

In addition to the text-based CLI, the OS system has two browser-based graphical interfaces. Refer to the *Cisco USC 8000 Series System Commissioning Guide* for information about initial system provisioning. Refer to the *Cisco eRMS Installation and Administration Guide* for information about provisioning and maintaining a functioning system.

The primary audience for this guide includes system administrators, network operators, and other personnel responsible for configuring, administering, and operating the small cell solution system. It assumes you have an understanding of the Internet, networking principles, networking configuration, and experience in radio networks.



**Note** The chapters and sections in this manual are grouped logically by topic rather than in strict provisioning sequence. Refer to [Section 1.7, Provisioning Sequence](#) on page 8 for the actual provisioning flow.

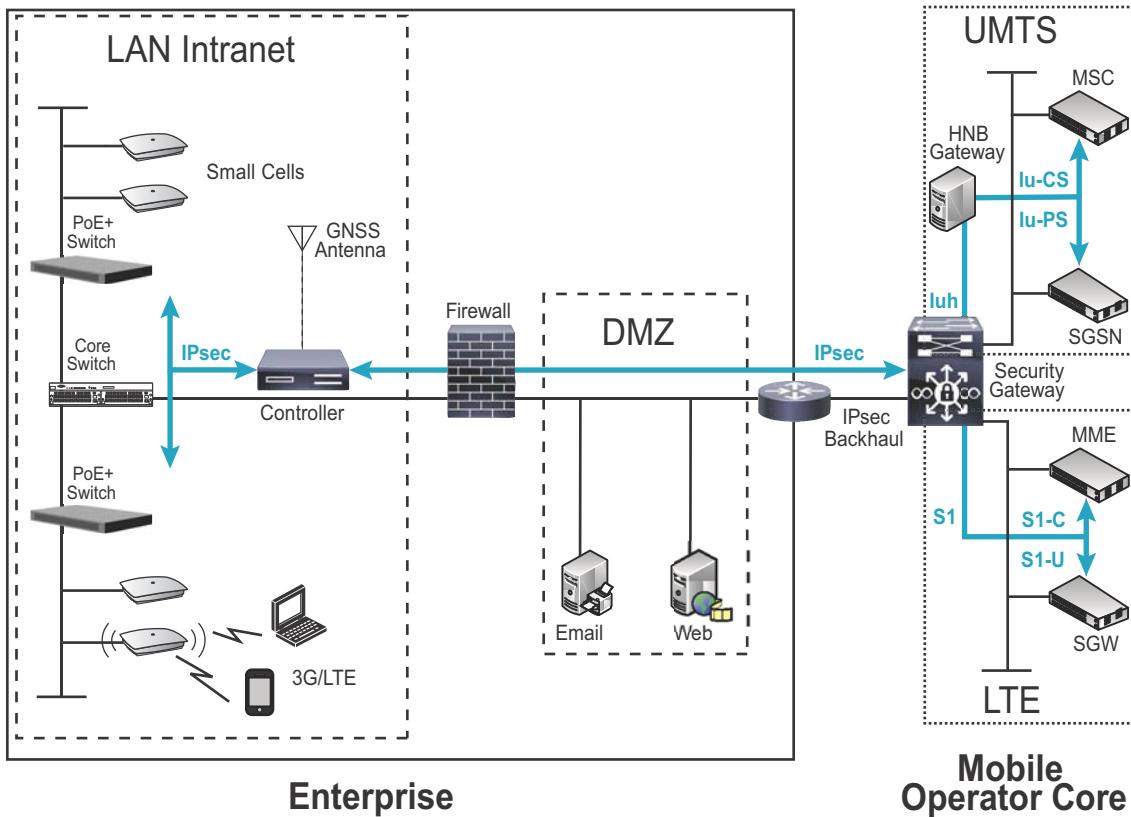
## 1.2 Product Description

The Cisco enterprise small cell network is the industry-first radio access network designed to provide coverage, capacity, and smart applications to enterprises. It not only seamlessly connects mobile devices to the mobile operator network, but also connects them to the enterprise intranet, enabling these devices to access both local and cloud-based applications. Further, it can provide a wealth of local intelligence that enables operators to deliver enterprise-specific services and smart applications.

The system is comprised of the USC 8088 Controller, which centrally controls up to 100 small cells operating in licensed 3G and LTE spectrum and deployed throughout an enterprise or a public space. OS offers a portfolio of small cells that offer 3G, LTE, and optionally Wi-Fi air interface capabilities. An enterprise installs the appropriate number of small cells in its building or campus and connects them to the LAN over Ethernet.

The controller aggregates the traffic from all small cells, connects them to mobile operator and enterprise networks, and ensures that end-users have a seamless experience as they move throughout the building or campus. [Figure 1](#) shows a logical view of the small cell solution.

All small cells utilize on-chip Trusted Platform Module (TPM) functions to implement secure boot and to establish secure IPsec tunnels to the controller. Small cells require an active network connection to the controller in order to operate.



**Figure 1** USC 8088 Controller in an Enterprise Network

### 1.2.1 The USC 8088 Controller

The controller is the central control point of the small cell solution. It provides overall traffic aggregation and session management for all mobile sessions delivered through the small cells. It is responsible for access control, small cell

management, auto configuration, self-optimization, interference management, mobility management, local data/voice offload logic, and core network integration functions for each small cell small cell solution.



**Figure 2** Cisco USC 8088 Controller

Using a single multi-access controller with UMTS and LTE functionalities, operators can deploy targeted coverage and capacity to enterprises within days. The unique architecture dramatically simplifies configuration and network optimization.

Using a common backhaul connection via any Ethernet LAN and an integrated network management system, operators can manage multiple access networks. The controller can also serve as a mobile service delivery platform while providing wireless session management across multiple radio access technologies without infrastructure changes.

### 1.2.1.1 Overview of the USC 8088 Controller Features

Key features of the controller include:

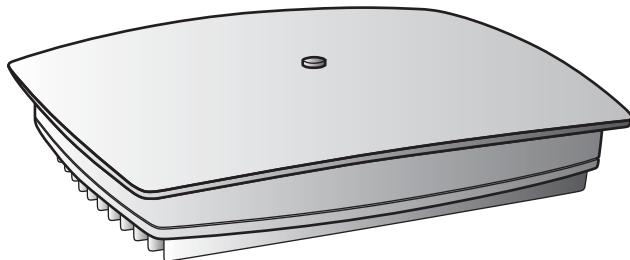
- multi-mode UMTS and LTE coverage
- enterprise optimized easy installation and integration with existing LAN infrastructure
- core network integration
- carrier grade security
- Self Optimizing Networks (SON)
- user and traffic prioritization
- automatic Radio Frequency (RF) planning
- ongoing RF optimization
- onboard applications and managed services

Refer to the *Cisco USC 8088 Controller Hardware Installation Guide* and datasheet for more information about the controller specifications and installation.

### 1.2.2 The Dual-Radio Small Cell

The Cisco dual-radio small cell is a small cell designed to address the 3G and LTE capacity requirements in dense in-building deployments. Small cells are centrally configured and managed by the Cisco USC 8088 local system controller, creating a coherent small cell solution system.

Cisco offers a portfolio of small cells that support UMTS and LTE radio interfaces and a range of frequency bands. Details on each small cell model are provided in the respective technical product description documents.



**Figure 3** Small Cell

Small cells come with internal antennas and can be installed on walls, ceilings, or above the ceiling. Both network connectivity and power are provided over Ethernet. Small cells support secure boot, and establish certificate-based IPsec tunnel to the controller for all control and user plane traffic.

When instructed, a small cell detects and provides the raw topology data points to the local system controller, which then makes RF self-organization decisions on behalf of the entire collection of small cell cells. This approach ensures the performance of the overall small cell solution system is maximized while interference to surrounding networks is minimized.

#### 1.2.2.1 Overview of Small Cell Features

The small cell:

- is designed from the ground up for large scale deployments
- is customized to support the Cisco small cell solution system architecture
- performs coordinated self-organization of RF characteristics that allows for rapid installation of Cisco small cell systems without special RF tools or skills
- integrates transparently into enterprise network environments
- is powered over Ethernet
- is available in multiple radio access technologies and frequency band combinations

Refer to the *Cisco USC 8738/8838 Hardware Installation Guide* and datasheet for more information about the specifications and installation requirements.

## 1.3 The Data Model

The Cisco small cell solution supports a rich data model with thousands of unique objects used to configure and monitor system operation, individual cell status, and user active and historical sessions. The data model expands upon data models defined in TR-096 and TR-198 by the Broadband Forum and 3GPP, and includes numerous extensions for Cisco small cell solution-specific functionalities and topologies.

The data model is protocol agnostic in that it can be accessed through standard management protocols, including TR-069, SNMP, and CLI. XML performance reports can be retrieved through FTP and SCP. A management client application can use the CLI to configure every aspect of the system, query all operational states, and display performance counters. An SNMP manager application can view all operational state and performance parameters.

In addition, asynchronous events may be delivered as SNMP traps. The controller can also be configured to collect 3GPP performance counters, generate TS32.405 compliant XML reports, and asynchronously upload them via FTP or SCP to a performance management server.

## 1.4 Data Model Managed Objects

The system is configured and maintained by manipulating physical and logical managed objects. [Table 1](#) shows the supported managed objects in the Cisco small cell solution (represented by the *System* in the object hierarchy):

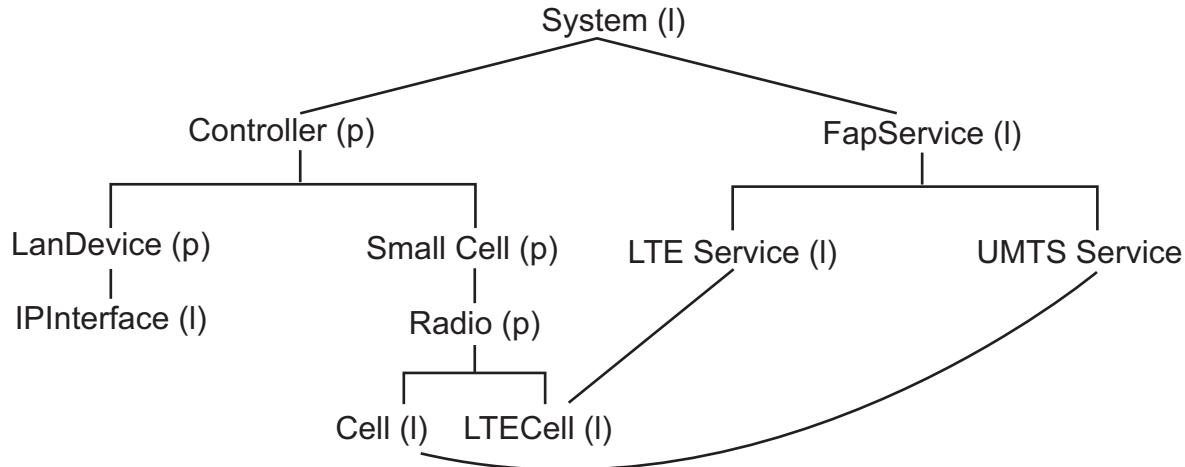
**Table 1: Managed Objects**

Manage Object Types	Managed Object Examples	Valid Options
Cell	Cell.57	1 through 2147483647, 100 total
FAPService	FAPService.1	1
Interface	LANDevice.2.IPInterface.10 ManagementDevice.1.IPInterface.1	1 through 4095, 501 total
LTECell	Cell.72	1 through 2147483647, 100 total
LTE Service	FAPService.1.FAPControl.LTE	LTE
Port	LANDevice.3 ManagementDevice	1 through 10 1
Radio	RadioNode.7.Radio.1	1 through 2
RadioNode	RadioNode.37	1 through 1024, 100 total
ServicesNode	ServicesNode.1025	1025
System	System	1
UMTS Service	FAPService.1.FAPControl.UMTS	UMTS

Each controller can support up to 100 small cells. Each small cell contains one UMTS or LTE radio, or one UMTS and one LTE radio. Each radio is associated with a single cell.

A LANDevice is the physical Gigabit Ethernet port in the controller. The controller can contain up to 512 logical IP Interfaces which correspond to VLANs.

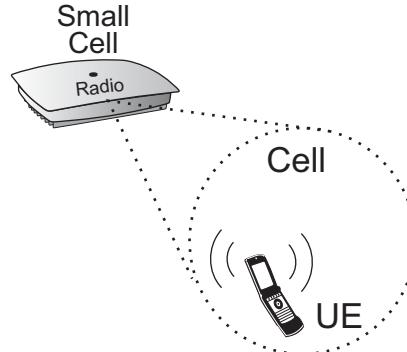
The controller, small cell, and radio are physical hardware elements in the Radio Access Network (RAN). Cells are logical entities associated with the radios. [Figure 4](#) shows the relationships between managed objects in the Cisco small cell solution. Physical objects are denoted by (p). Logical objects are denoted by (l).



[Figure 4](#) Managed Object Relationships

## 1.5 Relationship between Small Cells, Radios, and Cells

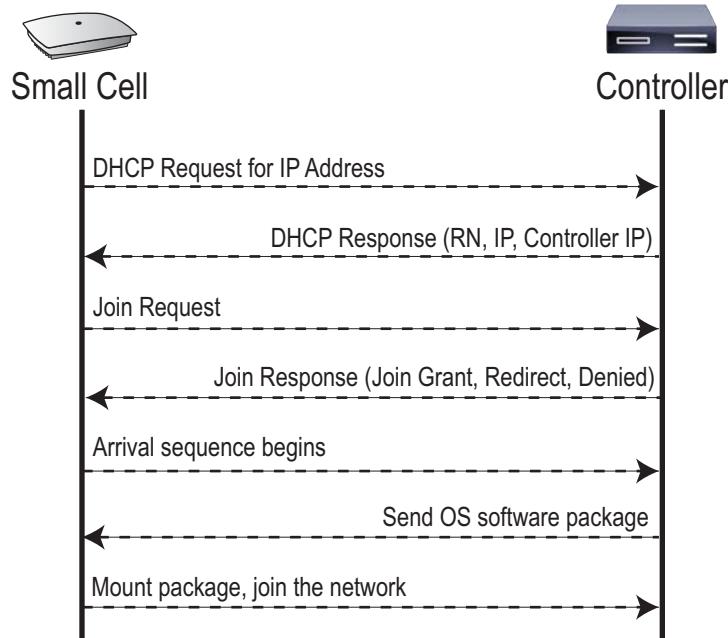
Both UMTS and LTE radios and their associated cells must be configured by the controller in order for those cells to become operational over the air. [Figure 5](#) illustrates the relationship of the small cells, radios, cells, and user equipment:



[Figure 5](#) Physical Small Cell, Radio, and UE with a Logical Cell

## 1.6 Small Cell Boot Sequence

On initial boot, the small cell performs the sequence illustrated in [Figure 5](#) and communicates with the controller. This sequence normally takes about one minute to complete. After the boot sequence, all devices are reachable.

**Figure 6** Small Cell Boot Sequence**Sequence description:**

- When the small cell is powered on, the device sends a DHCP Request to the controller DHCP server to get IP information. The DHCP server is configured in the controller to respond only to DHCP requests from Cisco USC 8000 Series small cells. Refer to [Section 4.1.9, Configuring the USC 8088 Controller DHCP Server](#) on page 46 for more information about the controller DHCP server configuration.
- The server responds with the IP addresses of the small cell and the controller (the master of the small cell).
- Using its own IP address, the small cell sends a Join Request message to the controller. The small cell seeks to join the cellular network.
- The controller responds with a Join Response message indicating whether the small cell is allowed to join the network or not.
- The arrival sequence begins. Based on the small cell configuration, the small cell joins the system and receives its configuration. The controller sends the Cisco software image and configuration settings to the small cell.
- The small cell reboots and mounts the Cisco software package as a RAM-based file system.
- The small cell contacts the controller and joins the network.

## 1.7 Provisioning Sequence

After the services and small cells have been installed and pre-provisioned as described in the *Cisco USC 8088 Controller Hardware Installation Guide* and *Cisco USC 8738/8838 Hardware Installation Guide*, provision the Cisco small cell solution in the following sequence:

- Configure IP networking parameters. Refer to [Section 4.1, IP Networking](#) on page 39.

2. Configure Femtocell Access Point (FAP) services. Refer to [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85.
3. Configure the IPsec tunnel to the provider core network, and optionally to the small cells. Refer to [Section 4.3, Configuring IPsec to the Core Network](#) on page 56.
4. Configure core network settings. Refer to [Section 5.1, Configuring the Core UMTS Network](#) on page 77.
5. Configure the RAN. Refer to [Section 5, UMTS Radio Access Network](#) on page 77.
6. Configure access to the system. Refer to [Chapter 10, “Access Control Topics”](#) on page 161.
7. Configure policies, local switching, and Quality of Service. Refer to [Chapter 12, “Session Management”](#) on page 177.
8. Configure handover and idle mode cell re-selection parameters. Refer to [Chapter 14, “UMTS Mobility”](#) on page 207.
9. Configure Fault, Configuration, Accounting, Performance, Security (FCAPS) capabilities. Refer to [Chapter 17, “System Management”](#) on page 231.
10. Configure Radio Frequency (RF) management. Refer to [Chapter 7, “UMTS RF Management”](#) on page 107.

## 1.8 Configuration Sequence

The following is a high-level overview of the initial provisioning sequence of the entire system. It assumes that the controller and all small cells have been properly installed, the controller has been initially provisioned, and that the small cells are properly cabled to the controller. Refer to the *Cisco USC 8088 Controller Hardware Installation Guide* and *Cisco USC 8738/8838 Hardware Installation Guide* for pre-provisioning information.

**Step 1** As each small cell is powered on, it registers itself with the controller. When auto provisioning is enabled, the system automatically provisions the small cell into the database and boots it in network monitor mode. At that point, the small cell is awaiting instruction from the controller. It is not radiating power.

**Step 2** Once all small cells are installed, the installation team instructs the controller to start network monitor measurements with the `request umts rem start` or `run request lte rem start` command. Upon receiving this command, the controller begins a process to auto-detect external macro cells on the same UMTS channel and to determine the internal topology of the system deployment.

This process takes anywhere from a few minutes to a few tens of minutes, depending on the number of small cells in the deployment. At the end of this process, each small cell is reprovisioned in Operational (NodeB) mode with an assigned primary scrambling code, a default maximum transmit power, and a fully populated neighbor list comprised of both external UMTS and LTE NodeB's and internal small cells. The system is now operational in that it can carry user traffic. However the small cell transmit powers have not yet been tuned.

**Step 3** (Optional) The installation team can perform a walk-through in the deployment area to gain topological information for manually tuning the small cell transmit powers.

Over time, the network will continue to gather UE measurements as devices use the enterprise system. When configured for periodic network scanning, the controller will use these measurements to tune the small cell power assignments over time, reacting to changes in the radio propagation environment and to changes in nearby external UMTS and LTE systems.

## 1.9 Document Conventions

This document uses the following typographical conventions:

- Monospaced text indicates CLI input or output. Input is in bold text, output in plain text. For example:  
`show Time NTPServer1`  
NTPServer1 10.1.11.200;
- **Bold text** also indicates a key pressed on a keyboard or other important element. **Bold monospaced** text indicates the name of a command or user screen input.
- *Italicized* text indicates a system element that can be configured in the procedure.
- Parameters for input commands are displayed by angle brackets (<parameter>). For example, `set IPInterfaceIPAddress <ip_address>`.

For the sake of brevity, some screen output will be truncated to remove repetitive and non-essential displays and blank lines. Refer to [Section 2.6.5, Screen Display Truncation](#) on page 18 for more information and an example.

## 1.10 The Cisco USC 8000 Series Documentation Set

The USC 8000 Series documentation set includes:

- The *Cisco USC 8000 Series System Description* provides an overview of how the USC 8000 Series system fits within an operator's network and in an enterprise, describes key features of the system, and provides specifications for the services and small cells.
- The *Cisco USC 8000 Series Feature Description* provides high-level descriptions of the small cell solution system features, their impact on the product components (controllers and small cells), manageability considerations, and feature benefits.
- The *Cisco USC 8000 Series OS Administrator Guide* provides procedures for configuring the software environment and internetworking between the controller and small cell devices.
- The *Cisco USC 8088 Controller Hardware Installation Guide* provides hardware specifications and installation instructions.
- The *Cisco USC 8738/8838 Hardware Installation Guide* provides hardware specifications and installation instructions.
- The *Cisco USC 8000 Series Deployment Planning Guide for Dual-Mode Systems* provides information about planning and dimensioning small cell solution systems.
- The *Cisco USC 8000 Series OS CLI User Guide* provides an introduction to the key features and functionalities of the Command Line Interface (CLI).
- The *Cisco 8000 Series OS Data Model Reference Guide* provides details about the objects and parameters that comprise the system configuration and operational state.
- The *Cisco 8000 Series OS Faults, Conditions, and Events Reference Guide* provides details about all alarms, conditions, and events in the system.
- The *Cisco USC 8000 Series System Commissioning Guide* provides information about turning up the small cell solution with the Local Configuration Interface (LCI) graphical user interface.
- The *Performance Measurements for Dual-Mode Small Cell Solution* provides a reference guide to Key Performance Indicators (KPI) that monitor the health and state of the small cell solution system.
- The *Cisco eRMS Installation and Administration Guide* provides information about installing the network management server and client and using it to remotely manage enterprise small cell deployments.
- The *Cisco USC 8000 Series Time Zone Reference Guide* provides the information required to configure the time zone for USC 8088 controller.
- The *Cisco USC 8000 Series Call Performance Event Reporting Guide* provides detailed information about call performance events files including the file format, reported events, and event parameters.
- The *Cisco eRMS NBI Integration Guide* provides information about integrating the eRMS network management system into operator's Northbound Interface (NBI) Operations Support Systems (OSSs) to surveil enterprise small cell networks.



## 2 The OS CLI

This chapter contains the following sections:

- [Section 2.1, CLI Overview](#) on page 11
- [Section 2.2, System Components](#) on page 12
- [Section 2.3, Command Modes](#) on page 13
- [Section 2.4, Navigating the CLI](#) on page 13
- [Section 2.5, Command Hierarchy](#) on page 14
- [Section 2.6, Working in the Configuration Mode](#) on page 16
- [Section 2.7, Frequently Used Commands](#) on page 19
- [Section 2.8, Logging into the CLI](#) on page 20
- [Section 2.9, Show Commands](#) on page 20
- [Section 2.10, The Fetch Command](#) on page 22
- [Section 2.11, Configuring CLI Settings](#) on page 23
- [Section 2.12, Managing the Configuration](#) on page 25

### 2.1 CLI Overview

The USC 8000 Series Command Line Interface (CLI) is an industry-standard hierarchical text interface for configuring the USC 8088 Controller and its subtended Cisco small cells to provide mobile broadband services. The single-lined commands execute when you press the **Enter** key.



All CLI commands are executed in the controller. Small cells are provisioned by the controller.

#### Note

The CLI has the following features:

- **Command help:** From any prompt or command, press the **Tab** key or type **?** (question mark) to display the list of valid commands or parameters.

```
admin% set FAPService 1 AccessMgmt?
Possible completions:
AccessMgmt - Access management configuration
admin% set FAPService 1 AccessMgmt
```

- **Command completion:** From any prompt or command, press the **Tab** key to complete a partially entered command. If there are more than one possible completion, it completes to the point of ambiguity. Press the **Tab** key again to see a list of valid completions. Command completion also applies to other strings such as file and user names.
- **Command memory:** From any prompt, press the **↑** (up arrow) to scroll through the most recently entered commands.

- **Command mobility:** From anywhere on an unexecuted command, use the ← (left arrow) or → (right arrow) to move the cursor on that line for command editing.

## 2.2 System Components

**Table 2** lists some of the important CLI objects in the system and shows their plain language equivalents:

**Table 2: System Objects**

CLI Object Name	Description
Airlink	Radio parameters
APN	Provider core network
Cell	Radio cell
CSDomain	Voice traffic
FAPService	Femto Access Point (FAP) service (radio services)
FDDFAP	Air interface cell related properties
HSDPA	Data downlink parameters
HSUPA	Data uplink parameters
IPInterface	IP interface of the controller Ethernet port
LANDevice	Controller port Ethernet port
LANHost	Small Cell
Layer3Forwarding	Data forwarding configuration
Layer3ForwardingGroup	Routing table
Layer3Routing	Routing configuration
PSDomain	Data traffic
QueueManagement	Class of Service
RadioBearer	Data traffic properties
RadioNode	Small cell, SCRN
ServicesNode	Controller, controller
UMTS	Radio
UTRAN	Radio network parameters
WLANSERVICE	Wi-Fi service parameters



Wi-Fi and WLAN objects are not currently supported.

Note

## 2.3 Command Modes

The CLI has two command modes, each with its own set of commands:

- **Operational Mode:** For monitoring the system and performing basic system administration, such as software upgrades. When you initially log into the controller, your CLI parser is automatically placed into the Operational Mode. A greater-than symbol (>) at the end of the hostname prompt indicates the Operational Mode:

```
admin@sn>
```

- **Configuration Mode:** For manipulating the system configuration. A percent symbol (%) at the end of the hostname prompt indicates the Configuration Mode. When in the Operational Mode, issue the **configure** command to enter the Configuration Mode:

```
admin@sn> configure
Entering configuration mode private
admin@sn%
```

### 2.3.1 The Candidate Configuration and the Commit Command

In the Configuration Mode, commands entered and text returned on the screen apply to the candidate configuration. The candidate configuration is not applied to the active system until the **commit** command is entered and validated. At this point it becomes the active configuration. Use the candidate configuration to build and modify the system without interfering with actual network operations.



**Note** Most command examples in this guide omit the **commit** command for brevity. Additionally, there are configurations that rely on other settings being properly configured before a commit can succeed. To focus the example commands specifically on the task described, the **commit** command is mostly omitted.

### 2.3.2 Operational Mode Commands in the Configuration Mode

Use the **run** command to issue an Operational Mode command in the Configuration Mode. The benefit of using the **run** command is that you can issue an Operational Mode command in the Configuration Mode. Therefore, you avoid having to commit a candidate configuration or toggle between the two modes to issue Operational Mode commands.

```
run show ServicesNode Time
ServicesNode 1025:
    CurrentTime: 2014-02-25T16:26:35Z
MezzanineCard 1025:
    ArriveTime: 2014-02-25T02:27:41Z
    UpTime:      13:58:54
```

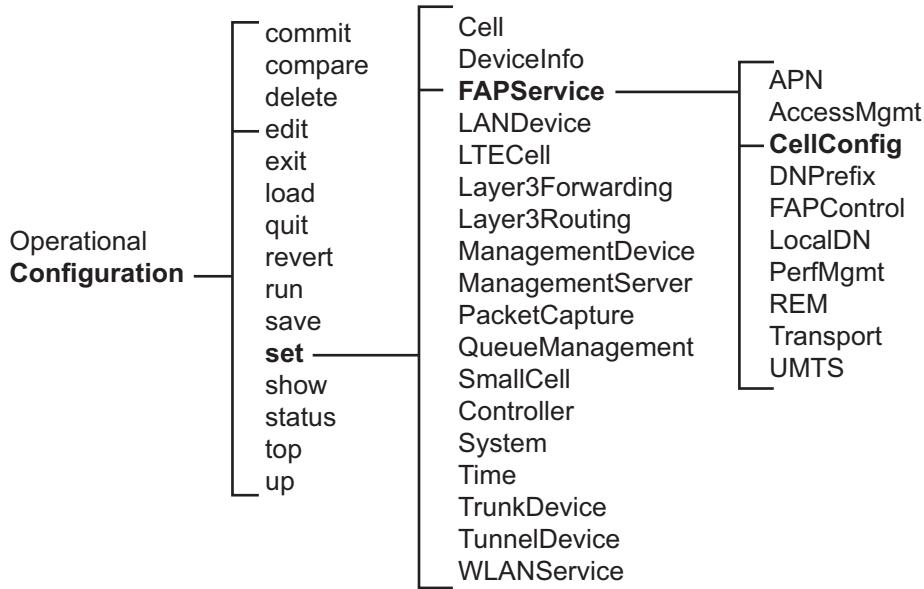
## 2.4 Navigating the CLI

The CLI integrates familiar navigational methods:

- Use the **Tab** key for auto-completion of a command or to display a list of possible command completions and help strings.
- Use the up or down arrows or the **Ctrl-p** or **Ctrl-n** key combinations to display command history.

## 2.5 Command Hierarchy

Commands within the CLI are organized in a hierarchy. Related commands are grouped together in sub-levels that may be acted upon by higher level commands. [Figure 7](#) shows an example of the CLI hierarchy. In this example from the Configuration Mode you navigate to the `set` level, then the *FAPService* (the small cell) level, and finally to the *CellConfig* level where you configure the cell parameters.



[Figure 7 Example of the CLI Hierarchy](#)

The current hierarchical level displays above the command prompt. For example, the root level of the Configuration Mode displays the following hierarchical level indicator and prompt:

```
[edit]
admin@(sn)%
```

Issue the `edit FAPService <ServiceNumber>` command to navigate to the *FAPService* level, and the level indicator changes to the following:

```
[edit FAPService 1]
admin@(sn)%
```



The current version of the OS software supports one FAPService. Therefore `<ServiceNumber>` is always 1 (one) in this release.

Note

Issue the `edit CellConfig` command to navigate to the *CellConfig* level, and the level indicator changes to the following:

```
[edit FAPService 1 CellConfig]
admin@(sn)%
```

Issue the `exit` command to navigate one level up the hierarchy to the *FAPService* level, and the level indicator returns to the following:

```
[edit FAPService 1]
admin@(sn)%
```

## 2.5.1 Root Level Commands

The sections below show the root level commands for each CLI mode.

Root-level Operational Mode commands:

- **configure**: Manipulate software configuration information
- **display**: Display operational state
- **exit**: Exit the management session
- **fetch**: Retrieve object attributes
- **file**: Perform file operations
- **id**: Show user ID information
- **ping**: Send ICMP ECHO\_REQUEST to network host
- **quit**: Exit the management session
- **request**: Make system-level requests
- **set**: Set CLI properties
- **show**: Show information about the system
- **source**: File to source
- **test**: Test configuration
- **wlan**: Show WLAN information on a local host (currently disabled)

Root-level Configuration Mode commands:

- **commit**: Commit current set of changes
- **compare**: Show configuration differences
- **delete**: Delete a data element
- **edit**: Edit a sub-element
- **exit**: Exit from this level
- **load**: Load configuration from an ASCII file
- **quit**: Exit from this level
- **revert**: Discard any outstanding edits
- **run**: Run an Operational Mode command
- **save**: Save configuration to an ASCII file
- **set**: Set a parameter
- **show**: Show a parameter
- **status**: Display users currently editing the configuration
- **top**: Exit to top level and optionally run command
- **up**: Exit one level of configuration

## 2.6 Working in the Configuration Mode

The Configuration Mode provides access to all read-write parameters of the OS data model. Use the Configuration Mode to provision the system and make changes to the system configuration.

### 2.6.1 Entering and Navigating the Configuration Mode

- From the Operational Mode, issue the **configure** command to enter the Configuration Mode:

```
admin@sn> configure
Entering configuration mode private
```

```
[edit]
admin@%
```

- Use the **edit** command to move to a hierarchy level. For example, the command **edit RadioNode 1 Radio 1** enters the [edit RadioNode 1 Radio 1] hierarchy level.

The **edit** command changes hierarchy levels in the CLI and operates like the **cd** command in UNIX. (Issuing CD in that environment moves you to a new directory level.)

```
[edit]
admin@sn% edit RadioNode 1 Radio 1
```

```
[edit RadioNode 1 Radio 1]
admin@sn%
```

- Use the **set** command to configure parameters at the current hierarchy level.

```
[edit RadioNode 1 Radio 1]
admin@sn% set Enable false
```

- Use the **exit** command to navigate to the previous hierarchy level.

```
[edit RadioNode 1 Radio 1]
admin@sn% exit
```

```
[edit]
admin@sn%
```

### 2.6.2 Entering Configuration Mode Commands

You can enter Configuration Mode commands individually or with one extended compound command. The following examples show how to define the two NTP servers for the controller using the **set** command. The **set** command modifies existing configuration attributes or creates them if they do not previously exist. Bolded text indicates user input. Entering the commands and parameters individually:

```
[edit]
admin@(sn)% set Time
[ok] [2011-01-04 21:35:39]
```

```
[edit Time]
admin@(sn)% set NTPServer1 10.202.1.1
[ok] [2011-01-04 21:36:31]
```

```
admin@(sn)% exit
[ok] [2011-01-04 21:36:52]
```

```
admin@(sn)% set NTPServer2 10.202.2.2
[ok] [2011-01-04 21:37:25]
```

```
[edit Time NTPServer2]
admin@(sn)% exit
[ok] [2011-01-04 21:37:33]
```

- Entering a single, compound command with the associated parameters:

```
admin@(sn)% edit Time NTPServer1 10.202.1.1 NTPServer2 10.202.2.2
```

## 2.6.3 Using Show Commands as Provisioning Aids

In the Configuration Mode, the **show** commands display the command hierarchy required to provision the system. For example, issuing the **show LANDevice** command returns the following:

```
show LANDevice
LANHostConfigManagement {
    IPInterface 1 {
        Enable          true;
        IPInterfaceIPAddress 10.1.192.10;
        IPInterfaceSubnetMask 255.255.255.0;
    }
    IPInterface 2 {
        Enable          true;
        IPInterfaceIPAddress 10.1.192.3;
        IPInterfaceSubnetMask 255.255.255.0;
        VLANID         2;
    }
}
LANEthernetInterfaceConfig 1 {
    Enable      true;
    MaxBitRate 1000;
    DuplexMode Full;
}
```

The same output displays from the Operational Mode by entering a **show configuration** command. In the example above, issue the **show configuration LANDevice** command.

From the output of the **show LANDevice** command above you can deduce the following:

- The *LANHostConfigManagement* object is the parent of *IPInterface* and *LANEthernetInterfaceConfig*. Therefore, *IPInterface* and *LANEthernetInterfaceConfig* are configured on the *LANHostConfigManagement* hierarchical level.
- IPInterface* is the parent of *Enable*, *IPInterfaceIPAddress*, and *IPInterfaceSubnetMask*. Therefore, *Enable*, *IPInterfaceIPAddress*, and *IPInterfaceSubnetMask* are configured on the *LANHostConfigManagement* | *IPInterface* hierarchical level.
- The *LANEthernetInterfaceConfig* object is the parent of *Enable*, *MaxBitRate*, and *DuplexMode*. Therefore, are configured on the *LANHostConfigManagement* | *LANEthernetInterfaceConfig* level.

The *LANHostConfigManagement* object is a child of the *LANDevice* object in the Configuration Mode. With this understanding, use the following commands to create the configuration that produces the example of the **show LANDevice** command above:

To create the sample configuration

- Step 1** From the Configuration Mode, issue the following commands to configure the LAN host:

```
admin@(sn)% set LANDevice 1 LANHostConfigManagement
[ok] [2011-01-05 01:03:02]

[edit LANDevice 1 LANHostConfigManagement]
admin@(sn)% edit IPInterface 1 Enable true IPInterfaceIPAddress 10.1.192.3
IPInterfaceSubnetMask 255.255.255.0
[ok] [2011-01-05 01:10:39]

admin@(sn)% exit
```

```
[ok] [2011-01-05 01:10:49]

[edit LANDevice 1 LANHostConfigManagement]
admin@(sn)% set LANEthernetInterfaceConfig 1 Enable true
[ok] [2011-01-05 01:12:17]

[edit LANDevice 1 LANEthernetInterfaceConfig 1 Enable]
admin@(sn)% exit
[ok] [2011-01-05 01:13:19]

[edit LANDevice 1]
admin@(sn)% commit
Commit complete.
```

## 2.6.4 Deleting Objects

Use the **delete** command to remove OS objects and their parameters from the candidate configuration. When you delete a parameter, the parameter value is reset to the default value in the candidate configuration. The following example deletes cell 66:

```
delete Cell 66
```

Issue the **show cell 66** command to validate the configuration:

```
show cell 66
-----^
syntax error: unknown element
```

## 2.6.5 Screen Display Truncation

For the sake of brevity and ease of reading, many of the repetitive and non-essential screen elements have been edited out of the example input and output in this manual. For example, the provisioning example above would be truncated to remove the screen prompts, hierarchical level indicators, and [ok] responses as follows:

```
configure
set LANDevice 1 LANHostConfigManagement
set IPInterface 1 Enable true IPInterfaceIPAddress 10.1.192.3 IPInterfaceSubnetMask
255.255.255.0
exit
edit LANEthernetInterfaceConfig 1 Enable true MaxBitRate 1000 DuplexMode full
exit
commit
```

A **show** command output examples similarly will not display information not relevant to the procedure. For example, [Section 14.1, Cell Connection States](#) on page 207 discusses setting timeout values. The **show** command returns the following output:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH
DCHInactivityTimer      50;
FACHInactivityTimer     100;
DisconnectInactivityTimer 600;
UE4aThreshold          256;
UE4aTimeToTrigger       100;
UE4aTxInterruption      500;
UE4aPendingTimeAfterTrigger 250;
RNC4aThreshold          512;
RNC4aTimeToTrigger       100;
MaxNumCellFACHUEs        16;
```

For brevity and clarity, the above output removes values irrelevant to the procedure, and is edited to:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH
DCHInactivityTimer      50;
FACHInactivityTimer     100;
DisconnectInactivityTimer 600;
MaxNumCellFACHUES       16;
```

## 2.7 Frequently Used Commands

Table 3 describes some of the frequently used CLI commands:

**Table 3: Frequently Used CLI Commands**

Command	Description	Mode
<b>commit</b>	Makes the candidate configuration the running configuration and saves the running configuration to persistent storage.	Configuration
<b>configure</b>	Accesses the Configuration Mode.	Operational
<b>delete</b>	Deletes an object or a parameter. When you delete an object, the object is removed from the candidate configuration.  When you delete a parameter, the parameter value is reset to the default value in the candidate configuration.	Configuration
<b>edit</b>	Sets edit context (location in configuration hierarchy) in the Configuration Mode.	Configuration
<b>exit</b>	From the Operational Mode, it exits the CLI. From the Configuration Mode, it returns to the Operational Mode.	Both
<b>file copy</b>	Copies a specified local file to a local destination (the administrator's controller home directory).	Operational
<b>file get</b>	Retrieves a file from a remote server and stores it locally in the administrator's controller home directory.	Operational
<b>file list</b>	Lists the contents of a directory.	Operational
<b>file match</b>	Displays every line in a text file that contains a specified text string.	Operational
<b>file put</b>	Takes a local file from a administrator's controller home directory and uploads it to a remote server.	Operational
<b>file show</b>	Displays the contents of the defined text file.	Operational
<b>set</b>	Sets a parameter.	Configuration
<b>show</b>	Displays the configuration or operational state.	Operational and Configuration
<b>show Version</b>	Displays the current software image.	Operational
<b>show Version Revert</b>	Displays the revert software image	Operational

## 2.8 Logging into the CLI

You can log into the CLI remotely through the Secure SHell (SSH) protocol. Log into the controller through the IP address 192.168.168.1. A default route is configured on Interface 1. Connect to this port in the controller and access the CLI over the network using SSH:

```
ssh admin@192.168.168.1
```

The factory default login is set to the following:

- Username is *admin*
- Password is *admin*

Example:

```
ssh admin@192.168.168.1
admin@192.168.0.1's password: admin
admin connected from 192.168.168.2 using ssh on (sn)
admin@sn>
```

## 2.9 Show Commands

Show commands are a valuable method for surveilling the state of the system and troubleshoot problems. You can process (filter) show commands as explained in [Section 2.9.1, Processing Command Output](#) on page 20. [Section 2.6.5, Screen Display Truncation](#) on page 18 explains how examples in this manual are edited for brevity and clarity.

### 2.9.1 Processing Command Output

Show command output can be verbose, much of which may not be relevant for your specific purpose. You can process the output of a commands such as *show* using an output redirect by entering the | (pipe) modifier. CLI commands support the following redirect targets:

**Table 4: Command Output Redirects**

Redirects	Description
count	Count the number of lines in the output
except	Show only text that does not matches a pattern
find	Search for the first occurrence of a pattern
linnum	Enumerate lines in the output
match	Show only text that matches a pattern
more	Paginate output
nomore	Suppress pagination
save	Save output text to a new or existing file



Text string searching is case sensitive. Enclose text strings containing special characters in quotation marks ("").

**Note**

The following example uses the output redirect to search for equipment that has been administratively placed out of service:

```
show System Event | match ADMIN_DISABLED
2011-01-01T06:36:50.803017Z W EVENT_ADMIN_DISABLED [MOI="LANDevice.2" ]
2011-01-01T06:36:50.716630Z W EVENT_ADMIN_DISABLED [MOI="Cell.30000" ]
2011-01-01T00:01:40.415149Z W EVENT_ADMIN_DISABLED [MOI="LANDevice.2" ]
2011-01-01T00:01:40.327636Z W EVENT_ADMIN_DISABLED [MOI="Cell.30000" ]
2011-06-06T22:20:11.607247Z W EVENT_ADMIN_DISABLED [MOI="LANDevice.2" ]
2011-06-06T22:20:11.525528Z W EVENT_ADMIN_DISABLED [MOI="Cell.30000" ]
2011-06-03T19:07:50.528407Z W EVENT_ADMIN_DISABLED [MOI="LANDevice.2" ]
2011-06-03T19:07:50.445971Z W EVENT_ADMIN_DISABLED [MOI="Cell.30000" ]
```

The following example saves the current configuration to a text file:

```
show configuration | save /configfiles/configfile.cfg
```

The following example displays the primary scrambling codes deployed in the network:

```
show Cell UMTS | match PrimaryScramblingCode
PrimaryScramblingCode      "[ 12 ]";
PrimaryScramblingCode      "[ 13 ]";
PrimaryScramblingCode      "[ 15 ]";
PrimaryScramblingCode      "[ 18 ]";
PrimaryScramblingCode      "[ 19 ]";
PrimaryScramblingCode      "[ 20 ]";
PrimaryScramblingCode      "[ 21 ]";
PrimaryScramblingCode      "[ 22 ]";
PrimaryScramblingCode      "[ 24 ]";
PrimaryScramblingCode      "[ 25 ]";
PrimaryScramblingCode      "[ 26 ]";
PrimaryScramblingCode      "[ 28 ]";
PrimaryScramblingCode      "[ 29 ]";
```

The following example displays session data for a specified International Mobile Subscriber Identity (IMSI):

```
show Session UMTS history | match <imsi>
```

## 2.9.2 Filtering Output with Regular Expressions

A regular expression is a text string describing a search pattern. Refine searches to target specific output by filtering with regular expressions. Search strings support multiple filters. Output of multiple search filters must pass the filter of each filter. Regular expressions are case-sensitive.

The CLI supports the following regular expressions:

**Table 5: Supported Regular Expressions**

Expression	Description
.	(period) Matches any character.
^	Matches the beginning of a string.
\$	Matches the end of a string.
[abc...]	Character class, which matches any of the characters "abc..." Character ranges are specified by a pair of characters separated by a -.
[^abc...]	Negated character class, which matches any character except "abc...".

**Table 5: Supported Regular Expressions (continued)**

Expression	Description
r1   r2	Alternation. It matches either r1 or r2.
r1r2	Concatenation. It matches r1 and then r2.
r <sup>+</sup>	Matches one or more r's.
r <sup>*</sup>	Matches zero or more r's.
r?	Matches zero or one r's.
(r)	Grouping. It matches r.

The following example searches for UMTS voice sessions that were disconnected due to failure, such as Abnormal Release, and displays a list of events that are both not normal and are voice-related:

```
show Session UMTS History | except Normal\ Release | match Voice
Session IMSI D V ConnectTime RRCState ConnectCause Cell DisconnectTime DisconnectCause
122048 001010123451354 1 1 2011-08-25T12:55:16.772242Z Cell_DCH Voice 14 - Still Active
122047 001010123451014 0 1 2011-08-25T12:53:27.355962Z Cell_DCH Voice 14 2011-08-25T12:53:30.820811Z All radiolinks failed
122041 001010123451351 0 1 2011-08-25T12:51:05.993090Z Cell_DCH Voice 14 -
122039 001010123456812 0 1 2011-08-25T12:51:02.60933Z Cell_DCH Voice 14 -
120156 001010123451264 - - - - Voice 14 -
ServicesNode Rebooted
```

## 2.10 The Fetch Command

The Operational Mode **fetch** command is an efficient method of retrieving first-level system configuration and status information. It follows the structure of the data model and returns the immediate attributes of the specified object path.

The fetch command syntax consists of a list of objects optionally followed by an attribute name and a list of object indexes. The fetch command allows for one omitted index for a list object in an object path. The omitted index must be the last one in the object path.

Data model objects are separated by a period (.). For example:

**QueueManagement.ControlPlaneCoS.**

Using the fetch command in the CLI, replace the period with a space:

```
fetch QueueManagement ControlPlaneCos
ControlPlaneClassificationGroup 0;
DefaultSignalingClassQueue 7;
DefaultOAMClassQueue 3;
```

The fetch command will retrieve attributes from multiple instances of an object domain. The following example returns the *EthernetID* of all provisioned small cells:

```
fetch RadioNode EthernetID
RadioNode 10 {
    EthernetID 11:22:33:44:55:66;
}
RadioNode 384 {
    EthernetID 00:24:48:01:2a:28;
}
```

## 2.10.1 Indexes

The lower-case *i* enclosed in curly braces ( {*i*} ) is an index that is a variable integer representing an array structure. For example:

**RadioNode.{i}.**

In the CLI, you can omit the index number and search for all of the specified objects and their first-level attributes:

```
fetch RadioNode
RadioNode 10 {
    Enable                      true;
    EthernetID                  11:22:33:44:55:66;
    SecurityMode                secure;
    OperState                   OOS-NOTPRESENT;
    LANDeviceNumberOfEntries    1;
    ForwardingEngineNumberOfEntries 1;
}
RadioNode 384 {
    Enable                      true;
    EthernetID                  00:24:48:01:2a:28;
    SecurityMode                open;
    OperState                   OOS-NOTPRESENT;
    LANDeviceNumberOfEntries    1;
    ForwardingEngineNumberOfEntries 1;
}
```

Each indexed object has an index attribute with the prefix of that object and a suffix of *Index*. For example: **RadioNode RadioNodeIndex**. Specify the unique object index number for a more targeted search. The following example searches for first-level information about small cell 10:

```
fetch RadioNode RadioNodeIndex 10
Enable                      true;
EthernetID                  11:22:33:44:55:66;
SecurityMode                secure;
OperState                   OOS-NOTPRESENT;
LANDeviceNumberOfEntries    1;
ForwardingEngineNumberOfEntries 1;
```

Refer to *Cisco 8000 Series OS Data Model Reference Guide* for complete details about objects and parameters that comprise the system configuration and operational state. Refer to the *Cisco USC 8000 Series OS CLI User Guide* for information about how to map the data model to the CLI hierarchy.

## 2.11 Configuring CLI Settings

The topics in this section explain how to configure CLI-specific session parameters.

### 2.11.1 Viewing the Current CLI Settings

Issue the **show cli** command from the Operational Mode to display the current CLI settings:

```
show cli
autowizard true;
complete-on-space true;
display-level 99999999;
history 100;
idle-timeout 600;
```

```

output {
    file terminal;
}
paginate true;
screen {
    length 50;
    width 80;
}
show {
    defaults false;
}
terminal xterm;

```

## 2.11.2 Configuring the Display Banner

You can optionally configure a text banner that displays immediately upon user log on to the CLI. The banner content can be entered directly into the CLI or uploaded from a text file. The banner displays upon the next user log into the system.

To enter a display banner through the CLI

**Step 1** From the Operational Mode, issue the **request system banner load Terminal** command and press the *Enter* key.

```
request system banner load Terminal
```

**Step 2** Enter the banner text. Carriage returns are permitted. Terminate the input by pressing *CTRL+D*. For example:

```
Welcome to the SpiderCloud CLI!
Press the Tab key or type ? (question mark) to display the list of valid commands or
parameters.
```

To create and load a display banner from a file

**Step 1** Create a text file and enter the contents of the display banner. Save the text file in the user home directory on the controller:

- For the administrator: /scw/data/home/admin
- For the read-only administrator: /scw/data/home/roadmin

**Step 2** From the Operational Mode, enter the **request system banner load <FileName>** command to load the text file. This example uses the file named *banner.txt*.

```
request system banner load banner.txt
```

**Viewing the display banner**

The banner displays automatically upon the next system log in. For example:

```
ssh admin@10.3.1.18
admin@10.3.1.18's password:
Welcome to the SpiderCloud CLI!
Press the Tab key or type ? (question mark) to display the list of valid commands or
parameters.
admin@>
```

## 2.11.3 Configuring the Idle Timeout

For security reasons you will automatically be logged out of your CLI session after 600 seconds (ten minutes) of inactivity. This time period is configurable from the Operational Mode on a per-user, per-session basis by issuing the **set idle-timeout** command and specifying the idle timeout period in seconds. Valid options are from 1 through

8192 (136.5 minutes). Specifying 0 (zero) disables the idle timeout and leaves your session active until the controller reboots, you manually log out, or you are logged out of the session by an administrative user.

The following example sets the idle timeout to 1800 seconds (30 minutes):

```
set idle-timeout 1800
```

## 2.11.4 Configuring CLI Session Parameters

As a security feature, system administrators can limit the number of CLI sessions per user and total number of all CLI sessions allowed on each controller.

### 2.11.4.1 Configuring the Number of CLI Sessions per User

An individual user can have multiple concurrent CLI sessions up to the maximum number of total CLI sessions per controller. Use the **set System CLI MaxSessionsPerUser** command from the Configuration Mode to change the maximum number of sessions allowed for each user up to the total number of CLI sessions allowed per controller. The following example sets the maximum number of sessions for each user to 1.

```
set System CLI MaxSessionsPerUser 1
```

### 2.11.4.2 Configuring the Total Number of CLI Sessions

By default, the controller supports up to four active CLI administrative user sessions in the controller at one time. If an individual user has multiple concurrent CLI sessions, each count against the total number of sessions. Use the **set System CLI MaxSessions** command from the Configuration Mode to change the maximum number of users allowed within the range of 1 through 4. The following example sets the maximum number of administrative user sessions to 1.

```
set System CLI MaxSessions 1
```

## 2.11.5 Viewing CLI Administrator Sessions

The controller supports customizable number active CLI administrative user sessions in the controller at one time. An individual CLI user can have multiple simultaneous sessions as long as the total number of all administrative user sessions does not exceed that number.

Issue the **show users** command from the Operational Mode to view the active CLI users. For example:

```
show users
SID USER  CTX FROM      PROTO LOGIN
 10 admin cli 10.3.254.34 ssh  04:49:42
 *8 admin cli 10.1.1.101  ssh  08:33:19
```

Your session is denoted with an \* (asterisk) before the session ID.

## 2.11.6 Logging a User Off the System

Use the **request system logout user** command from the Operational Mode to log an administrative user from a CLI session. The following example logs out user 10:

```
request system logout user 10
```

## 2.12 Managing the Configuration

Managing the configuration involves viewing the running and candidate configurations, editing the configuration file, saving the running configuration, and loading and merging configuration files. Refer to [Section 2.3.1, The Candidate](#)

[Configuration and the Commit Command](#) on page 13 for information about the difference between the running and candidate configurations.

This section contains the following topics:

- [Section 2.12.1, Displaying the Running Configuration](#) on page 26
- [Section 2.12.2, Displaying the Candidate Configuration](#) on page 27
- [Section 2.12.3, Displaying Changes in the Candidate Configuration](#) on page 27
- [Section 2.12.4, Discarding Edits](#) on page 28
- [Section 2.12.5, Saving the Running Configuration](#) on page 28
- [Section 2.12.6, Backing Up the Running Configuration](#) on page 29
- [Section 2.12.7, Loading and Merging a Configuration File](#) on page 29

## 2.12.1 Displaying the Running Configuration

You can display the running configuration from the Configuration Mode or the Operational Mode:

- To display the running configuration in the Operational Mode, use the **show configuration** command.
- To display the running configuration in the Configuration Mode, issue the **run show configuration** command, as shown below:

```
run show configuration
FAPService 1 {
    FAPControl {
        UMTS {
            SelfConfig {
                NeighborListSelfConfigEnable true;
                MeasIMSIList 123456789101001;
                MeasLoadingFactor 70;
                FAPCoverageTargetMinBase -900;
                FAPCoverageTargetValue1 50;
                FAPCoverageTargetValue2 -30;
                FAPCoverageTargetAdditionDelta 30;
                NumMeasUe 101;
                NumPstThresh 101;
                NumImsiThresh 101;
                NumValidRSThresh 101;
                rMeasDiscard 101;
                AutoProvisionEnable true;
            }
            Gateway {
                SecGWServer1 10.1.30.104;
                CNProtocol Iu/IP;
            }
        }
    }
}
[output truncated]
```

Note that the output of the **show configuration** command is quite verbose. For a more targeted response, add the **match** parameter as illustrated below:

```
show configuration | match FACHInactivityTimer
                    FACHInactivityTimer 0;
```

Refer to [Section 2.9.1, Processing Command Output](#) on page 20 for more information about filtering show command output.

## 2.12.2 Displaying the Candidate Configuration

Use the **show** command in the Configuration Mode to display the candidate configuration (the configuration with your edit changes included).

To display the candidate configuration

**Step 1** From the Configuration Mode, issue the command to modify the running configuration. This example sets the CN protocol to *Iu/IP*.

```
set FAPService 1 FAPControl UMTS Gateway CNProtocol Iu/IP
```

**Step 2** Issue the **show** command to display your changes and other settings for that hierarchical level. In this example, Step 1 set the *CNProtocol* parameter, so the **show** command below extends down to the **show FAPService <ServiceNumber> FAPControl UMTS Gateway CNProtocol** level.

```
show FAPService 1 FAPControl UMTS Gateway CNProtocol
CNProtocol Iu/IP;
```

The following example extends the **show** command to the **show FAPService <ServiceNumber> FAPControl UMTS Gateway** level to display the candidate configuration changes to the UMTS gateway hierarchy:

```
show FAPService 1 FAPControl UMTS Gateway
SecGWSERVER1 10.1.30.104;
CNProtocol Iu/IP;
FAPGWPort 29169;
```

## 2.12.3 Displaying Changes in the Candidate Configuration

To display outstanding changes in the candidate configuration before committing them, issue the **compare running** command in the Configuration Mode. New statements to be added to the configuration are flagged with a plus sign (+). Removed statements are flagged with a minus sign (-).

```
compare running
...
Cell 1 {
-   Enable true;
+   Enable false;
    RadioNode 1;
    Radio 1;
}
+Cell 2 {
+   Enable true;
+   RadioNode 2;
+   Radio 1;
+   CellConfig {
+     UMTS {
+       RAN {
+         FDDFAP {
+           MobilityLinkReservation 3;
+           RF {
+             UARFCNDL "[ 10700 ]";
+             PrimaryScramblingCode "[ 0 ]";
+             MaxFAPTxPower 0;
+           }
+         }
+       }
+     }
+   }
}
```

```
+}
...
RadioNode 1 {
-   Enable true;
+   Enable false;
  EthernetID 00:00:00:aa:aa:cc;
  SecurityMode open;
  Radio 1 {
    Enable true;
    Band umts-band-I;
  }
+RadioNode 2 {
+  Name "";
+  Description "";
+  Enable true;
+  EthernetID 00:00:00:aa:aa:bb;
+  SecurityMode open;
+  ServingController 0.0.0.0;
+  Radio 1 {
+    Enable true;
+    Band umts-band-I;
+  }
+}
[output truncated]
```

## 2.12.4 Discarding Edits

In the Configuration Mode, you can discard candidate configuration edits in one of two ways:

- Use the **exit** command to leave the Configuration Mode before executing the **commit** command. Exiting the Configuration Mode without committing changes discards all session edits.
- Use the **revert** command.

## 2.12.5 Saving the Running Configuration

You can save the current running configuration to a text file in the controller.

**To save the running configuration**

**Step 1** From the Configuration Mode, issue the **save <filename.cfg>** command. This example saves the running configuration to a file named *config-2011-08-10.cfg*.

```
save config-2011-08-10.cfg
```

**Step 2** Issue the **run file list** command to verify that the file was successfully saved:

```
run file list
cell-insert.txt
cell-test.txt
config-2011-08-10.cfg
error_incidents/
fg_200_list.txt
[output truncated]
```

**Step 3 (Optional)** Issue the **run file list Detail** command to verify the file timestamp:

```
run file list Detail
drwx----- 2 4096 Aug 31 21:22 .ssh/
-rw-r--r-- 1 2496 Aug 16 06:32 Cert-SCW_CA1-Self.pem
-rw-r--r-- 1 2468 Aug 16 06:33 Cert-db212s6.int.spidercloud.com-SCW_CA1.pem
-rw-r--r-- 1 7593 Aug 16 06:31 SpiderCloud-scsn-Cert.pem
-rw-r--r-- 1 18568 Aug 13 22:14 access_points_radios_insert_0000128.txt
-rw-r--r-- 1 6136 Aug 13 22:14 access_points_radios_iid_0000010.txt
-rw-r--r-- 1 35656 Sep 9 00:59 bc_add_cell_test_config
-rw-r--r-- 1 130 Aug 13 22:14 cell-delete.txt
-rw-r--r-- 1 217 Aug 13 22:14 cell-insert.txt
-rw-r--r-- 1 17782 Aug 10 23:19 config-2011-08-10.cfg
```

## 2.12.6 Backing Up the Running Configuration

After saving the running configuration to a file, you can back it up to an external device. Issue the **file put <local\_path> <destination-url>** command from the Operational Mode using the Secure Copy Protocol (SCP), File Transfer Protocol (FTP), or Trivial File Transfer Protocol (TFTP). If you do not specify the device password, you will be prompted for it. The password you enter is not echoed back to the terminal.

The following command backs up the file *backup.cfg* to the server with the IP address 10.20.10.1. Note that this example renames the *backup.cfg* file using the SCP to add the date 08/01/2011.

```
file put backup.cfg scp://admin@10.20.10.1/backup.08.01.2011.cfg
admin@10.20.10.1's password:
```

Enter the password to the remote server.

## 2.12.7 Loading and Merging a Configuration File

Issue the **load merge <filename.cfg>** command from the Configuration Mode to load a previously saved configuration file onto the controller and merge this with your current candidate configuration. It will overwrite the existing provisioning for those parameters whose values are different in the new configuration file.

Parameters that are part of the original configuration but not of the new one are maintained. Parameters that are in the new configuration but not in the original one are added to the merged configuration.



If the configuration file was saved from another controller, first use a text editor and change the IP address (in the *LANDevice 1* section) of the other controller to the one of the node you are importing it to.

**Note**

The following example loads the file named *config-2011-08-10.cfg* and then commits it, making it the running configuration.

```
load merge config-2011-08-10.cfg
commit
```





## 3 Initial Configuration

This chapter discusses the initial controller configuration. It contains the following sections:

- [Section 3.1, Configuring the USC 8088 Controller for eRMS](#) on page 31
- [Section 3.2, Configuring General System Parameters](#) on page 32
- [Section 3.3, Setting the System Date and Time](#) on page 32
- [Section 3.4, Configuring the USC 8088 Controller Time Zone](#) on page 33
- [Section 3.5, Configuring Equipment Location](#) on page 34

### 3.1 Configuring the USC 8088 Controller for eRMS

When using the eRMS network management system to manage multiple controllers, each controller must be configured to communicate with the eRMS server. After the controller boots it periodically sends notifications to the eRMS server advertising its availability. Refer to the *Cisco eRMS Installation and Administration Guide* for more information about the eRMS management system.

To configure the controller to communicate with the eRMS server

**Step 1** From the Configuration Mode, issue the **set ManagementServer** command to enter the controller eRMS management parameters. This example:

- the management server URL is 192.168.1.50. Note that this must be appended by :8080/acs.
- eRMS will manage OS upgrades
- the minimum number of seconds between active notifications is 0
- enables support for the CPE WAN Management Protocol (CWMP)
- the minimum number of seconds between messages from the controller to the eRMS server is 0
- the port the controller listens for connection request messages is 7547

```
set ManagementServer URL 192.168.1.50:8080/acs UpgradesManaged true
ManageableDeviceNotificationLimit 0 EnableCWMP true DefaultActiveNotificationThrottle 30
ConnectionRequestPort 7547
```

**Step 2** Issue the following command to verify the configuration:

```
show ManagementServer
URL                                http://192.168.1.50:8080/acs;
PeriodicInformEnable                 false;
UpgradesManaged                      true;
ManageableDeviceNotificationLimit    0;
EnableCWMP                           true;
DefaultActiveNotificationThrottle   30;
ConnectionRequestPort                7547;
```

## 3.2 Configuring General System Parameters

You can configure the controller name, description, and contact information.

### To configure system information

**Step 1** From the Configuration Mode, enter the following command to configure general system parameters.

This example sets the:

- description to *IT\_Room*
- contact to *jgonzalez@provider.net*
- name to *San\_Jose*

```
set System Description IT_Room Contact jgonzalez@provider.net name San_Jose
```

**Step 2** Issue the following command to verify the configuration:

```
show System
Description          IT_Room;
Contact             jgonzalez@provider.net;
Name                San_Jose;
```

## 3.3 Setting the System Date and Time

Use the **set system clock** command to set the controller date and time. The system uses the 24-hour clock format. Valid input formats are:

- YYYY-MM-DDTHH:MM:SS
- YYYY-MM-DDTHH:MM
- HH:MM:SS
- HH:MM.



When configured for NTP, the controller uses NTP for system timing and ignores this value.

### Note

### To set the system date and time

**Step 1** From the Operational Mode, issue the **set system clock** command to set the controller date and time. This example sets the date to December 12, 2011, and the time to 1:30 PM.

```
set system clock 2011-12-12T13:30:00
Mon Dec 12 13:30:00 UTC 2011
```

**Step 2** Issue the **show ServicesNode Time** command to display the current system time, the time the controller joined the small cell solution, and length of time that the controller has been active in the system. The time displays in ISO 8601 format.

```
show ServicesNode Time
ServicesNode 1025:
  CurrentTime: 2014-02-25T16:26:35Z
MezzanineCard 1025:
  ArriveTime: 2014-02-25T02:27:41Z
  UpTime:      13:58:54
```

## 3.4 Configuring the USC 8088 Controller Time Zone

The controller ships with a large number of pre-defined time zones that include parameters such as the zero meridian offset and optional daylight savings time configurations. You cannot edit or delete these time zones, but you can create a custom time zone and configure its optional offset parameters. For example you might create a custom time zone if the offset rules for a designated time zone change, such as if daylight savings time is enacted. Refer to the *Cisco USC 8000 Series Time Zone Reference Guide* for more information about time zone configuration.

### 3.4.1 Setting the USC 8088 Controller Time Zone

You can select a pre-defined controller time zone. Refer to [Section 3.4.2, Configuring a Custom USC 8088 Controller Time Zone](#) if you require offset parameters that are not defined with a pre-defined time zone. Note that if the controller has previously been configured with a custom time zone, you must use the *LocalTimeZoneName* parameter and set the value to null with "" (empty double parenthesis).

To set a pre-defined controller time zone

**Step 1** From the Configuration Mode, issue the following command to select a pre-defined time zone for the controller. This example selects *Europe\_London*, the zero median time zone centered in London.

```
set Time TimeZone Europe_London
```

**Step 2** Issue the following command to verify the configuration:

```
show Time
TimeZone Europe_London;
```

To change a custom time zone to a predefined time zone

**Step 1** From the Configuration Mode, issue the following command to select a predefined time zone for the controller. This example selects *Europe\_Madrid* which has a -1 hour offset from the zero median time zone.

```
set Time TimeZone Europe_Madrid LocalTimeZoneName ""
```

**Step 2** Issue the following command to verify the configuration:

```
show Time
LocalTimeZoneName      "";
TimeZone              Europe_Madrid;
```

### 3.4.2 Configuring a Custom USC 8088 Controller Time Zone

You can create a custom controller time zone if the offset rules for a designated time zone change. For example, if daylight savings time is enacted, or for any other reason pre-defined time zones are not applicable to your situation.

To configure a custom controller time zone

**Step 1** From the Configuration Mode, issue the following command to configure a custom controller time zone. This example:

- configures daylight savings time
- uses the code name *WET* when not in daylight savings time and *WEST* during daylight savings time
- begins daylight savings time on Sunday of the last week of March at 1 a.m.
- ends daylight savings time on Sunday of the last week of October at 2 a.m. (the default, not specified)

```
set Time TimeZone Custom LocalTimeZoneName WETWEST,M3.5.0/1,M10.5.0
```

**Step 2** Issue the following command to verify the configuration:

```
show Time
LocalTimeZoneName      WET0WEST,M3.5.0/1,M10.5.0;
TimeZone               Custom;
```

## 3.5 Configuring Equipment Location

The network implements the enhanced telecommunications-based system that automatically associates a physical location (latitude, longitude, and altitude), within a range of 300 meters (1000 feet), with the calling party's telephone number. This information can be used to support:

- emergency services
- third-party applications
- location locking and assurance

Each controller and small cell can have a defined physical location. When an emergency call is initiated inside the small cell solution, that call is associated with a specific small cell who's physical location is sent to the emergency operator when the call is received.

The system uses radio location to locate the user equipment. A small cell inherits the controller location by default or can be manually configured to override that setting. You can set the controller physical location either automatically through a GNSS antenna with the USC 8088 or manually enter the information.

The physical location information is entered in the following formats:

- **Altitude:** entered in meters in whole integers (no decimals).
- **Latitude:** The latitude in degrees expressed in TR-196-compliant format computed as shown below. A positive number indicates north of the equator, a negative number indicates south of the equator. The range is from 90°00.00' South (-90,000,000) to 90°00.00' North (90,000,000).
- **Longitude:** The longitude in degrees expressed in TR-196-compliant format as shown below. A positive number indicates east of the prime meridian, a negative number indicates west of the prime meridian. The range is from 180°00.00' West (-180,000,000) to 180°00.00' East (180,000,000).



There are numerous free online resource to determine a location's GPS coordinates. There are other online resources to convert these coordinates from the more commonly expressed degree, minute, second format to degree/minute format used in the determining the TR-196-compliant format.

To convert coordinates to TR-196-compliant format

**Step 1** Convert coordinates from degree/minute format to TR-196-compliant format as follows:

- The latitude converts to N 37° 23.75' in degree/minute format. To convert degree/minute format to TR-196-compliant format:  $(37 * 1,000,000) + ((23.75 * 1,000,000) / 60) = 37,000,000 + (23,750,000 / 60) = 37,000,000 + 395,833 = 37,395,833$ .
- The longitude converts to W 121° 55.5' in degree/minute format. To convert to TR-196-compliant format:  $(121 * 1,000,000) + ((55.5 * 1,000,000) / 60) = 121,000,000 + (55,500,000 / 60) = 121,000,000 + 925,000 = 121,925,000$ . Since California is west of the prime meridian, this is expressed as -121,925,000.



The commas in the example numbers above are for clarity and ease of reading only. Do not enter commas for location coordinates into the CLI.

#### Note

**Table 6** describes the location parameters. Refer to the *3GPP TS 23.032 V6.0.0* standard for a detailed description of these parameters.

**Table 6: Location Parameters**

Parameter	Description
Altitude	Altitude in meters.
AltitudeUncertainty	Uncertainty of the UE vertical location in meters. Small cell only.
Confidence	Percent certainty that the UE is in the area defined by the GeographicalAreaFormat parameter values, from 0 through 100. Small cell only.
GeographicalAreaFormat	Manner in which location parameters are specified (refer to <a href="#">Table 7</a> ). Small cell only.
HorizontalUncertainty	Uncertainty of the UE horizontal location in meters. Small cell only.
Latitude	Latitude in degrees times 1,000,000.
Longitude	Longitude in degrees times 1,000,000.
UncertaintyEllipseAxisOrientation	Angle orientation of the ellipse that defines the maximum distance of location uncertainty, in degrees measured clockwise from the north. From 0 through 179. Small cell only.
UncertaintyEllipseSemiMajor	Maximum length, in meters, of the major radius of the location uncertainty ellipse <sup>a</sup> . Small cell only.
UncertaintyEllipseSemiMinor	Maximum length, in meters, of the minor radius of the location uncertainty ellipse <sup>b</sup> . Small cell only.

a. The major radius is one half of the length of the diameter of the longer curve of an ellipse.

b. The minor radius is one half of the length of the diameter of the shorter curve of an ellipse.

## 3.5.1 Configuring the USC 8088 Controller Location

You can set the controller physical location either automatically through a GNSS antenna with the USC 8088 or manually enter the information.

### 3.5.1.1 Configuring GNSS Location Determination and Reporting

The USC 8088 controller contains an integrated Global Navigation Satellite System (GNSS) receiver that supports location determination and reporting when an external antenna is connected to its TNC port. It synchronizes with either GPS or GLONASS satellites to provide latitude, longitude, and altitude information about the location of the controller.

GNSS derived latitude and longitude information display in both TR-196-compliant and in degree, minute, and second format and is persistent after reboots or change in the location mode, with the last known information displayed until a new reading can be made. Altitude displays in meters.

To enable GNSS location determination

**Step 1** From the Configuration Mode, issue the following command to enable GNSS location determination. This example enables *GPS* scanning.

```
set ServicesNode 1025 Location ScanMode GPS
```

**Step 2** Issue the following command to verify the configuration.

```
show ServicesNode 1025 Location ScanMode
ScanMode GPS;
```

### 3.5.1.2 Configuring the USC 8088 Controller Location Manually

You can manually configure the controller physical location when there is no GNSS antenna available. This information is persistent across reboots with the last known information available. The controller scan mode must be set to *Manual* to set or modify the location manually.

Manual location is configured in TR-196 format. Refer to [Section 11.1, Configuring Emergency Calls](#) on page 171 for information about the TR-196 format. Altitude is configured in meters.

To manually configure the controller location

**Step 1** From the Configuration Mode, issue the following command to manually configure the controller location. This example uses a building at location of latitude 37395748, longitude -121924264, and altitude 15.

```
set ServicesNode 1025 Location Latitude 37395748 Longitude -121924264 Altitude 15 ScanMode
Manual
```

**Step 2** Issue the following command to verify the configuration:

```
show ServicesNode 1025 Location
Latitude 37395748;
Longitude -121924264;
Altitude 15;
ScanMode Manual;
```

### 3.5.2 Small Cell Location

When defining the small cell location, the *GeographicalAreaFormat* parameter defines which location coordinates must be entered. [Table 7](#) describes the valid *GeographicalAreaFormat* values and their required location components:

**Table 7: Geographical Area Format Values**

Value	Required Components
LocationNotAvailable	Location unspecified
Point	Latitude and longitude
PointAndAltitude	Latitude, longitude, and altitude (in meters)
PointAndAltitudeWithUncertainty	Latitude, longitude, and altitude with the horizontal and vertical location uncertainties of the UE (in meters)
PointWithUncertainty	Latitude and longitude with the horizontal location uncertainty of the UE (in meters)

## To define the small cell location

- Step 1** From the Configuration Mode, set the location coordinates for the small cell. This example ensures that the small cell not use the controller location, and defines the *PointAndAltitude* value of latitude, longitude, and altitude, and uses the coordinates of the building as discussed above. It assumes:
- a latitude and longitude uncertainty of 20 meters
  - a vertical uncertainty of 10 meters
  - with a confidence of 80%

```
set RadioNode 40 Location GeographicalAreaFormat PointAndAltitude Latitude 37660150
Longitude -121542123 HorizontalUncertainty 20 Altitude 20 AltitudeUncertainty 10
Confidence 80 InheritServicesNodeLocation false
```

- Step 2** Issue the `show RadioNode <ServicesNode> Location` command to verify the configuration:

```
show RadioNode 40 Location
GeographicalAreaFormat          PointAndAltitude;
Latitude                         37660150;
Longitude                        -121542123;
HorizontalUncertainty           20;
Altitude                          20;
AltitudeUncertainty              10;
Confidence                        80;
InheritServicesNodeLocation      false
```

- Step 3** This example defines the *GeographicalAreaFormat* as *PointAndAltitudeWithUncertainty* and defines all geographical area format values. It uses the coordinates of the building as discussed above. It assumes:

- a latitude and longitude uncertainty of 20 meters
- a vertical uncertainty of 10 meters
- a confidence of 90%
- an uncertainty ellipse 15 meters by 10 meters oriented 30 degrees clockwise from the north ( $30^\circ$  in azimuthal notation or N  $30^\circ$  E in quadrant notation)

```
set RadioNode 50 Location GeographicalAreaFormat PointAndAltitudeWithUncertainty Latitude
37660150 Longitude -121542123 HorizontalUncertainty 20 Altitude 20 AltitudeUncertainty 10
UncertaintyEllipseAxisOrientation 35 UncertaintyEllipseSemiMajor 15
UncertaintyEllipseSemiMinor 10 Confidence 90
```

- Step 4** Issue the following command to verify the configuration:

```
show RadioNode 50 Location
GeographicalAreaFormat          PointAndAltitudeWithUncertainty;
Latitude                         37660150;
Longitude                        -121542123;
HorizontalUncertainty           20;
Altitude                          20;
AltitudeUncertainty              10;
UncertaintyEllipseSemiMajor      15;
UncertaintyEllipseSemiMinor      10;

UncertaintyEllipseAxisOrientation 35;
Confidence                        90;
```





# 4 IP Configuration

This chapter contains the following sections:

- [Section 4.1, IP Networking](#) on page 39
- [Section 4.2, Configuring Certificate Revocation Policies](#) on page 55
- [Section 4.3, Configuring IPsec to the Core Network](#) on page 56
- [Section 4.4, Configuring a 6in4 Tunnel to the Core Network](#) on page 66
- [Section 4.5, Configuring IPsec to the Small Cell](#) on page 68
- [Section 4.6, Deployment Considerations with a Firewall](#) on page 69

## 4.1 IP Networking

IP network provisioning of the controller requires configuring one or more *LANDevice* objects, which correspond to its Gigabit Ethernet ports and *IPInterface* objects, which are one or more logical IP interfaces for each physical port. To enable the physical device, set the *Enable* attribute for the *LANDevice LANEthernetInterfaceConfig* to *true*.

### 4.1.1 Changing the Default IP Address

Ethernet port 4, used for administrative access to the CLI, is configured with the default IP address 192.168.168.1. If you change this IP address, the new IP address will take effect immediately after entering a successful **commit** command. Users connected through an SSH session will lose connectivity to the controller. Start a new session by connecting to the new IP address on port 22.

To change the default IP address

**Step 1** From the Configuration Mode, assign the new IP address and subnet mask of the Ethernet port 4. This example assigns the IP address 192.168.32.5 with a subnet mask of 255.255.255.0.

```
set LANDevice 4 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
192.168.32.5 IPInterfaceSubnetMask 255.255.255.0
```

**Step 2** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice
LANDevice 4 {
    LANHostConfigManagement {
        IPInterface 1 {
            Enable           true;
            IPInterfaceIPAddress 192.168.32.5;
            IPInterfaceSubnetMask 255.255.255.0;
        }
    }
}
```

**Step 3** Issue the **commit** command to commit the changes:

```
commit
```

**Step 4** Your SSH connection to the controller terminates. Log back into the system using the new IP address. Refer to [Section 2.8, Logging into the CLI](#) on page 20 for information about logging into the system.

## 4.1.2 Configuring an Ethernet Port IP Address

Assign an IP address to a controller Ethernet port by creating an `IPInterface` for the `LANDevice`.

To assign an Ethernet port an IP interface

**Step 1** From the Configuration Mode, assign the IP address and subnet mask of the port. In this example, Ethernet port 3 is assigned the IP address 10.22.1.1 with a subnet mask of 255.255.255.0.

```
set LANDevice 3 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
10.22.1.1 IPInterfaceSubnetMask 255.255.255.0
```

**Step 2** Enable the physical interface:

```
set LANDevice 3 LANEthernetInterfaceConfig 1 Enable true
```

**Step 3** Issue the `show LANDevice` command to verify the configuration.

```
show LANDevice
LANDevice 3 {
    LANHostConfigManagement {
        IPInterface 1 {
            Enable           true;
            IPInterfaceIPAddress 10.22.1.1;
            IPInterfaceSubnetMask 255.255.255.0;
        }
    }
}
```

## 4.1.3 Setting the Ethernet Port Speed

Each controller Ethernet port can be separately configured for 100 Mbps or 1 Gbps traffic. Separate ports can have different speeds in the controller.

To configure the controller Ethernet port speed

**Step 1** From the Configuration Mode, enter the `set LANDevice <number> LANEthernetInterfaceConfig` command to set the Ethernet port maximum bitrate, in megabits per second. This example sets the bitrate to 100 megabits per second on port 1.

```
set LANDevice 1 LANEthernetInterfaceConfig 1 Enable true MaxBitRate 100
```

**Step 2** Enter the `show LANDevice <number> LANEthernetInterfaceConfig` command to verify the configuration:

```
show LANDevice 1 LANEthernetInterfaceConfig
LANEthernetInterfaceConfig 1 {
    Enable   true;
    MaxBitRate 100;
}
```

## 4.1.4 Viewing IP Interface Configurations

The following three Operational Mode commands display increasingly detailed information about controller IP interfaces:

### 4.1.4.1 show Interface

Use the `show Interface` command to view information about the IP interfaces of the controller gigabit Ethernet ports:

```
show Interface
LANDevice 1:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 10.1.194.16,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL

LANDevice 2:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: NoLink

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 172.30.30.1,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL

LANDevice 4:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: NoLink

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 192.168.168.1,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL
```

#### 4.1.4.2 show Interface Detail

Use the **show Interface Detail** command to display detailed information about the IP interfaces of the controller gigabit Ethernet ports:

```
show Interface Detail
LANDevice 1:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up
  BytesSent:      3923169  BytesReceived:      2026575
  PacketsSent:    11310   PacketsReceived:    24860

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 10.1.194.16,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL,
    DHCPServerEnable: false
    BytesSent:      3756575  BytesReceived:      668140
    PacketsSent:    11008   PacketsReceived:    10980

LANDevice 2:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up
  BytesSent:      98231070  BytesReceived:      92848501
  PacketsSent:    196442   PacketsReceived:    185697

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 172.30.30.1,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL,
```

```
DHCPServerEnable: true
BytesSent:          9822695  BytesReceived:        8972731
PacketsSent:       19645    PacketsReceived:     17945

[output truncated]
```

#### 4.1.4.3 show Interface Verbose

Use the **show Interface Verbose** command to display all information about the IP interface to the controller gigabit Ethernet port:

```
show Interface Verbose
LANDevice 1:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up
  BytesSent:          3949752  BytesReceived:        2184485
  PacketsSent:       11596    PacketsReceived:     26527
  ErrorsSent:         0        ErrorsReceived:      0
  UnicastPacketsSent: 11584   UnicastPacketsReceived: 11685
  DiscardPacketsSent: 0        DiscardPacketsReceived: 0
  MulticastPacketsSent: 0        MulticastPacketsReceived: 10489
  BroadcastPacketsSent: 12     BroadcastPacketsReceived: 4353

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 10.1.194.16,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL,
    DHCPServerEnable: false
    BytesSent:          3778781  BytesReceived:        689281
    PacketsSent:       11261    PacketsReceived:     11275
    ErrorsSent:         0        ErrorsReceived:      0
    UnicastPacketsSent: 11261   UnicastPacketsReceived: 11275
    DiscardPacketsSent: 0        DiscardPacketsReceived: 0
    MulticastPacketsSent: 0        MulticastPacketsReceived: 0
    BroadcastPacketsSent: 0     BroadcastPacketsReceived: 0

[output truncated]
```

#### 4.1.5 Resetting Interface Statistics

Reset the Gigabit Ethernet port and IP interface statistics with the **request Interface Statistics reset** command. Resetting the statistics sets the counters of all controller Ethernet ports and IP interfaces to zero. The system does not maintain a history of reset statistics.

To reset IP interface statistics

**Step 1** From the Operational Mode, issue the **show Interface LANDevice <port\_number> Detail** command to view the current counters. This example uses Ethernet port 1.

```
show Interface LANDevice 1 Detail
LANDevice 1:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up
  BytesSent:          3958995  BytesReceived:        2201020
  PacketsSent:       11656    PacketsReceived:     26733

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 10.1.194.16,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL,
    DHCPServerEnable: false
```

```
BytesSent:          3786465  BytesReceived:      693677
PacketsSent:       11315    PacketsReceived:   11348
```

[output truncated]

**Step 2** Issue the **request Interface Statistics reset** command to reset the IP interface statistics of all Ethernet ports (LANDevice) and IP interfaces in the controller.

```
request Interface Statistics reset
status Done
```

**Step 3** Issue the **show Interface LANDevice <port\_number> Detail** command to verify the configuration:

```
show Interface LANDevice 1 Detail
LANDevice 1:
  Enable: true, MACAddress: 00:24:48:00:31:80, OperState: IS-NORMAL,
  Status: Up
  BytesSent:          791  BytesReceived:      1031
  PacketsSent:        7    PacketsReceived:   15

  IPInterface 1:
    Enable: true, IPInterfaceIPAddress: 10.1.194.16,
    IPInterfaceSubnetMask: 255.255.255.0, VLANID: 0,
    ForwardingGroupIndex: 0, IngressClassificationGroup: 0,
    EgressClassificationGroup: 0, OperState: IS-NORMAL,
    DHCPServerEnable: false
    BytesSent:          1283  BytesReceived:      680
    PacketsSent:        10   PacketsReceived:   13
```

[output truncated]

## 4.1.6 Configuring VLANs

An *IPInterface* can be configured to add a VLAN tag to outgoing packets, and to drop packets not suitably VLAN tagged, by specifying a VLAN ID value for the *IPInterface* object. VLAN IDs are integers from 0 through 4095. The system supports up to 512 total VLANs. The VLAN ID value 0 (zero) indicates that no VLAN tag will be added. You can apply one VLAN tag per *IPInterface* object. The same VLAN ID cannot be used on multiple *IPInterfaces* on the same *LANDevice*.

### To configure VLAN tags

**Step 1** From the Configuration Mode, configure and enable a VLAN ID for an IP interface. In this example:

- interface 2 is named *Engineering\_VLAN*
- it has the IP address 10.1.94.6 with a subnet mask of 255.255.255.0
- it creates VLAN 2

```
set LANDevice 3 LANHostConfigManagement IPInterface 2 Enable true IPInterfaceIPAddress
10.1.94.6 IPInterfaceSubnetMask 255.255.255.0 VLANID 2 Description Engineering_VLAN
```

**Step 2** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice 3
LANHostConfigManagement {
  IPInterface 2 {
    Enable           true;
    IPInterfaceIPAddress 10.1.94.6;
    IPInterfaceSubnetMask 255.255.255.0;
    Description      Engineering_VLAN;
    VLANID          2;
    ForwardingGroupIndex 0;
  }
}
```

}

## 4.1.7 Configuring Ethernet Port Link Aggregation

To improve throughput, you can combine multiple physical Ethernet ports to form a logical trunk port with a higher data rate than the individual physical ports. Also called link aggregation, port trunking load balances traffic across the physical ports to achieve aggregate bandwidth close to the sum of the throughput of the combined ports.

In addition to increased bandwidth, link aggregation offers resiliency in the event of a link failure. When a port member of a trunk group has a link failure, the trunk bandwidth may be reduced, but the traffic continues to pass through the remaining port members of the trunk.

The controller supports up to two trunk ports of as many as four Ethernet ports apiece. The destination switch must support link aggregation.

To configure Ethernet port aggregation

**Step 1** From the Configuration mode, issue the following command to create, configure and enable a trunk port. This example:

- creates trunk port 1 with IP interface 1
- assigns it the IP address 10.191.0.1 with a subnet mask 255.255.255.0

```
set TrunkDevice 1 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
10.191.1 IPInterfaceSubnetMask 255.255.255.0
```

**Step 2** Issue the following command to create and enable the trunk port.

```
set TrunkDevice 1 LANEthernetInterfaceConfig 1 Enable true
```

**Step 3** Issue the following command to verify the configuration:

```
show TrunkDevice 1
LANHostConfigManagement {
    IPInterface 1 {
        Enable           true;
        IPInterfaceIPAddress 10.191.0.1;
        IPInterfaceSubnetMask 255.255.255.0;
    }
}
LANEthernetInterfaceConfig 1 {
    Enable true;
}
```

**Step 4** Issue the following command to assign Ethernet port 7 to the trunk port:

```
set LANDevice 7 LANEthernetInterfaceConfig 1 Enable true TrunkDeviceIndex 1
```

**Step 5** Issue the following command to verify the configuration:

```
show LANDevice 7 LANEthernetInterfaceConfig
LANEthernetInterfaceConfig 1 {
    Enable           true;
    TrunkDeviceIndex 1;
}
```

**Step 6** Issue the following command to assign Ethernet port 8 to the trunk port:

```
set LANDevice 8 LANEthernetInterfaceConfig 1 Enable true TrunkDeviceIndex 1
```

**Step 7** Issue the following command to verify the configuration:

```
show LANDevice 8 LANEthernetInterfaceConfig
LANEthernetInterfaceConfig 1 {
    Enable           true;
    TrunkDeviceIndex 1;
```

```
}
```

## 4.1.8 Configuring Static Routes

The system allows you to configure static routes to reach networks not directly connected to the controller by creating forwarding entries. A forwarding entry can specify either an IP address as the gateway, or can specify an interface in order to rely on proxy ARP to reach the destination. If both are specified, the interface specification will be ignored. Cisco Systems recommends defining the default static route.

To configure the default route

**Step 1** From the Configuration Mode, issue the **set Layer3Forwarding** command to specify the default route. This example specifies a *DestIPAddress* value of *0.0.0.0* and a *DestSubnetMask* value of *0.0.0.0* out from interface 1.

```
set Layer3Forwarding Forwarding 1 DestIPAddress 0.0.0.0 DestSubnetMask 0.0.0.0 LANDevice 1 IPInterface 1 Enable true
```

**Step 2** Issue the **show Layer3Forwarding** command to verify the configuration:

```
show Layer3Forwarding
Forwarding 1 {
    Enable          true;
    DestIPAddress  0.0.0.0;
    DestSubnetMask 0.0.0.0;
    LANDevice      1;
    IPInterface    1;
}
```

To configure a static route as a gateway

**Step 1** From the Configuration Mode, specify the static route. This example specifies a *DestIPAddress* value of *10.1.2.0* and a *DestSubnetMask* value of *255.255.255.0* and the *GatewayIPAddress* *10.1.1.254* of the gateway.

```
set Layer3Forwarding Forwarding 2 DestIPAddress 10.1.2.0 DestSubnetMask 255.255.255.0
GatewayIPAddress 10.1.1.254 Enable true
```

**Step 2** Issue the **show Layer3Forwarding** command to verify the configuration:

```
show Layer3Forwarding
Forwarding 2 {
    Enable          true;
    DestIPAddress  10.1.2.0;
    DestSubnetMask 255.255.255.0;
    GatewayIPAddress 10.1.1.254;
}
```

To configure a static route using an interface and relying on proxy ARP

**Step 1** From the Configuration Mode, configure the static route. This example configures a route to the *10.1.2.0/24* subnet from Ethernet port 3 IP interface 3.

```
set Layer3Forwarding Forwarding 2 Enable true DestIPAddress 10.1.2.0 DestSubnetMask 255.255.255.0 LANDevice 3 IPInterface 1
```

**Step 2** Issue the **show Layer3Forwarding** command to verify the configuration:

```
show Layer3Forwarding
Forwarding 2 {
    Enable          true;
    DestIPAddress  10.1.2.0;
    DestSubnetMask 255.255.255.0;
```

```

LANDevice          3;
IPInterface       1;
}

```

## 4.1.9 Configuring the USC 8088 Controller DHCP Server

The controller contains an IPv4 DHCP server for assigning IP addresses to small cells and other equipment. The controller DHCP server is disabled by default except on Ethernet ports 2 and 4. It must be enabled individually on each other IP interface that will access it. Disable the feature by disabling it on each IP interface in the controller. By default, this server will not respond to requests from non-enterprise small cell equipment other than on port 4.

### 4.1.9.1 Default Port 2 DHCP Server Settings

The controller Ethernet port 2 is by default configured for small cells, and has the DHCP server enabled for small cells that identify themselves as Cisco small cell solution equipment via DHCP Option 60. Port 2 is configured with the following IP addresses:

- 172.30.30.0/24 = subnet
- 172.30.30.10 to 172.30.30.209 for the small cells

### 4.1.9.2 Modifying DHCP Server Settings

You can modify the default DHCP settings to utilize a different set of IP addresses. Before modifying the controller DHCP server settings:

- The enterprise network between the controller and small cells must be properly configured.
- The controller and all small cells are either on the same LAN or VLAN, or there must be a relay agent configured to forward DHCP packets from the small cells to the controller and back.
- A pool of IP addresses must be defined for each subnet that contains small cells.

To edit DHCP server settings for small cells on a directly-connected network

**Step 1** From the Configuration Mode, issue the **set System DHCPServer Subnet** command to configure and enable the controller DHCP server for small cells on a directly connected network. In this example:

- the server is on subnet 1
- the prefix of the subnet of the small cells is 172.17.2.0.
- there are 100 small cell IP addresses
- in the pool, ranging from 172.17.2.100 through 172.17.2.199 inclusive

```
set System DHCPServer Subnet 1 Enable true Prefix 172.17.2.0 Netmask 255.255.255.0
MinimumIPAddress 172.17.2.100 MaximumIPAddress 172.17.2.199
```

**Step 2** Issue the following command to enable the controller DHCP server on the IP interface. This example enables the IP interface 1 on Ethernet port 2.

```
set LANDevice 2 LANHostConfigManagement IPInterface 1 DHCPServerEnable true
```

**Step 3** Issue the **commit** command to commit the configuration:

```
commit
```

**Step 4** Issue the **show system DHCPServer** command to verify the configuration:

```
show system DHCPServer
Subnet 1 {
    Enable      true;
    Prefix      172.17.2.0;
    Netmask     255.255.255.0;
    MinimumIPAddress 172.17.2.100;
    MaximumIPAddress 172.17.2.199;
```

## To modify DHCP server settings for small cells on a remote network

**Step 1** From the Configuration Mode, issue the **set System DHCPServer Subnet** command to configure and enable a DHCP server to assign IP addresses to small cells on a remote network where the DHCP query is reaching the controller via a DHCP relay. This operation allows the configuration of IP routers (a list of 1 to 16 IP gateways) that will be presented to the DHCP client to use for routing. In this example:

- the server is on subnet 2
- the prefix of the subnet of the small cells is 172.18.14.0
- there are 100 small cell IP addresses in the pool, ranging from 172.18.14.100 through 172.18.14.199 inclusive
- the server will direct small cell requests to the router with the IP address 172.18.14.1

```
set System DHCPServer Subnet 2 Enable true Prefix 172.18.14.0 Netmask 255.255.255.0
MinimumIPAddress 172.18.14.100 MaximumIPAddress 172.18.14.199 IPRoutes [ 172.18.14.1 ]
```

**Step 2** Issue the following command to enable the controller DHCP server on the IP interface. This example enables the IP interface 1 on Ethernet port 2.

```
set LANDevice 2 LANHostConfigManagement IPInterface 1 DHCPServerEnable true
```

**Step 3** Issue the **commit** command to commit the configuration:

```
commit
```

**Step 4** Issue the **show system DHCPServer** command to verify the configuration:

```
show system DHCPServer
Subnet 2 {
    Enable          true;
    Prefix          172.18.14.0;
    Netmask         255.255.255.0;
    MinimumIPAddress 172.18.14.100;
    MaximumIPAddress 172.18.14.199;
    IPRoutes        "[ 172.18.14.1 ]";
}
```

### 4.1.9.3 Default Port 4 DHCP Server Settings

The controller Ethernet port 4 is by default configured for use with initial system commissioning with Local Configuration Interface (LCI) browser-based user interface. Port 4 has the default IP address 192.168.168.1 with the DHCP server enabled for all equipment. When the installation laptop connects to port 4, the DHCP server issues it one of the following IP addresses:

- 192.168.168.10
- 192.168.168.11
- 192.168.168.12

### 4.1.9.4 Disabling the DHCP Server on an IP Interface

Disable the DHCP server on an IP interface after you have no longer need to avoid configuration issues.

#### To disable the controller DHCP server on an IP interface

**Step 1** From the Configuration Mode, disable the DHCP server on the IP interface. This example disables the DHCP server on Gigabit Ethernet port 4, IP interface 1.

```
set LANDevice 4 LANHostConfigManagement IPInterface 1 DHCPServerEnable false
```

**Step 2** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice 4
LANHostConfigManagement {
    IPInterface 1 {
        DHCPServerEnable      false;
    }
}
```

#### 4.1.9.5 Configuring the DHCP Server for Third-Party Equipment

In some instances, equipment may require the controller DHCP server to issue an IP address.

To permit non-Cisco small cell solution equipment to receive an IP address from the controller

**Step 1** From the Configuration Mode, issue the following command to allow the controller DHCP server to issue equipment other than small cells IP addresses:

```
set System DHCPServer Subnet 1 AllowedEquipment All
```

**Step 2** Issue the following command to verify the configuration:

```
show System DHCPServer Subnet 1
Enable          true;
Prefix          172.16.0.0;
Netmask         255.255.255.0;
MinimumIPAddress 172.16.0.100;
MaximumIPAddress 172.16.0.150;
AllowedEquipment All
```

#### 4.1.10 Configuring IP Forwarding Groups

A forwarding group is the mechanism for configuring virtual routing and forwarding instances in the controller. Virtual routing and forwarding instances allow collections of interfaces to be associated with unique routing and forwarding tables in order to support overlapping IP network address spaces.

By default, all interfaces are in the default forwarding group 0. The interface connecting to the provider core network and the interfaces connecting to the small cell network can only be associated with the default forwarding group. Other forwarding groups can only be used for interfaces that are used for locally switched UE data sessions.

After creating an IP forwarding group, locally switched UE data sessions can be mapped to a specific forwarding group by configuring the appropriate Policy.

To configure a forwarding group

**Step 1** From the Configuration Mode, create the forwarding group. In this example the forwarding group is called VRF\_1.

```
set Layer3Forwarding ForwardingGroup 1 Description VRF_1
```

**Step 2** Issue the **show Layer3Forwarding ForwardingGroup** command to verify the configuration:

```
show Layer3Forwarding ForwardingGroup
ForwardingGroup 1 {
    Description VRF_1;
}
```

**Step 3** Assign an IP interface and subnet mask to the forwarding group and assign it group number. In this example, the IP interface is 1, its IP address is 10.2.2.13 with a subnet mask of 255.255.255.0 and a forwarding group index of 1.

```
set LANDevice 3 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
10.2.2.13 IPInterfaceSubnetMask 255.255.255.0 ForwardingGroupIndex 1
```

**Step 4** Enable the physical device:

```
set LANDevice 3 LANEthernetInterfaceConfig 1 Enable true
```

**Step 5** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice
LANDevice 3 {
    LANHostConfigManagement {
        IPInterface 2 {
            Enable          true;
            IPInterfaceIPAddress 10.2.2.13;
            IPInterfaceSubnetMask 255.255.255.0;
            ForwardingGroupIndex 1;
        }
    }
    LANEthernetInterfaceConfig 1 {
        Enable      true;
    }
}
```

**Step 6** Set the default route for forwarding group 1. In this example, the Gigabit Ethernet port 3 has the IP interface *0.0.0.0* with a subnet mask of *0.0.0.0*.

```
set Layer3Forwarding Forwarding 1 Enable true DestIPAddress 0.0.0.0 DestSubnetMask
0.0.0.0 LANDevice 3 IPInterface 1 ForwardingGroupIndex 1
```

**Step 7** Issue the **show Layer3Forwarding** command to verify the configuration:

```
show Layer3Forwarding
Forwarding 1 {
    Enable          true;
    DestIPAddress 0.0.0.0;
    DestSubnetMask 0.0.0.0;
    LANDevice       3;
    IPInterface     1;
    ForwardingGroupIndex 1;
}
```

## 4.1.11 SSH TCP Port Forwarding

The system supports TCP port forwarding of SSH traffic to allow ancillary network equipment, such as switches and PoE injectors, installed in the enterprise premises to be remotely managed from the core network. This feature allows secure and encrypted configuration and management of up to 16 devices such as switches and POE injectors, and does not require any modifications to firewall policies. TCP port forwarding is disabled by default. It must be manually enabled.

To configure TCP port forwarding

**Step 1** From the Configuration Mode, issue the following command to enable TCP port forwarding. This example enables a switch with the IP address *10.2.1.1* using port *80* (HTTP).

```
set System SSH TCPPortForwardingDestination [ 10.2.1.1:80 ] TCPPortForwardingEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show System SSH
TCPPortForwardingEnable      true;
TCPPortForwardingDestination "[ 10.2.1.1:80 ]";
```

## 4.1.12 Configuring Network Time Synchronization

The small cell solution uses Network Time Protocol (NTP) version 4 to synchronize the controller system clock with the system clock of another device reachable over the IPsec tunnel to the mobile core network. The system supports configuring a primary and secondary NTP server.

## To configure network timing

**Step 1** From the Configuration Mode, define the IP address of the primary NTP server. In this example, the server has the IP address 10.1.11.200.

```
set Time NTPServer1 10.1.11.200 Enable true
```

**Step 2** Issue the `show Time NTPServer1` command to verify the configuration:

```
show Time NTPServer1
NTPServer1 10.1.11.200;
```

**Step 3** (Optional) Define the IP address of the secondary NTP server. In this example, the server has the IP address 10.1.11.202.

```
set Time NTPServer2 10.1.11.202 Enable true
```

**Step 4** Issue the `show Time NTPServer2` command to verify the configuration:

```
show Time NTPServer2
NTPServer1 10.1.11.202;
```

## To configure network timing using a forwarding group

**Step 1** From the Configuration Mode, define the IP address of the primary NTP server. In this example, the server has the IP address 10.1.11.201 and uses forwarding group 2.

```
set time NTPServer1 10.1.11.201 Enable true ForwardingGroupIndex 2
```

**Step 2** (Optional) Define the IP address of the secondary NTP server. In this example, the server has the IP address 10.1.11.203.

```
set Time NTPServer2 10.1.11.203 Enable true ForwardingGroupIndex 2
```

**Step 3** Issue the `show Time` command to verify the configuration:

```
show Time
NTPServer1          10.1.11.201;
NTPServer2          10.1.11.203;
Enable              true;
ForwardingGroupIndex 2;
```

## 4.1.13 Configuring DNS Lookup and Domain Search using a Name Server

The controller provides Domain Name System (DNS) name resolution by configuring the DNS server IP address. The system supports up to three DNS servers.

It also supports domain name search for hostname lookup. When a non-fully qualified hostname is presented for resolution, each of up to six defined domains are appended to the presented hostname and resolution is attempted for each. Configuring the `NameServer` and the `DomainSearch` parameters allows the use of hostnames for the security gateway server and for file operations such as `file put` and `file get`.

## To configure DNS name resolution using an IP address

**Step 1** From the Configuration Mode, issue the `set System NameServer <ip_address>` command. This example uses the IP address 10.50.10.1.

```
set System NameServer 10.50.10.1
```

**Step 2** Issue the `show system NameServer` command to verify the configuration:

```
show system NameServer
NameServer "[ 10.50.10.1 ]";
```

To configure domain name search for hostname lookup

**Step 1** From the Configuration Mode, issue the **set System DomainSearch <Domains>** command to create a list of domains. This command creates a list with two domains: *bar.com* and *bar.net*, and one subdomain, *int.bar.com*.

```
set System DomainSearch [ bar.com int.bar.com bar.net ]
```

**Step 2** Issue the **show System DomainSearch** command to verify the configuration:

```
show System DomainSearch
DomainSearch "[ bar.com int.bar.com bar.net ]";
```

#### 4.1.14 Configuring Static Name Resolution

In instances where there is no DNS server or there is one but you wish to bypass it, you can configure the controller static name host to match fully qualified domain names with their static IP addresses. If both a static name lookup and one or more DNS servers are configured, the controller uses the IP address in the static name lookup to reach the host.

This is applicable to any controller application that uses a Fully Qualified Domain Name (FQDN), including IPsec, ping, SSH, file uploads, and CLI file copy. In the example below the mobile provider uses a private core network with a static IP address rather than a fully qualified domain name for the security gateway.

To configure static name resolution

**Step 1** From the Configuration Mode, issue the **set System StaticNameLookup Host** command to configure the static name and map it to the IP address of the security gateway. This example configures host 1 with the fully qualified domain name of *secgw.com*, with the alias *secgw1* and description *Provider Security Gateway 1*.

```
set System StaticNameLookup Host 1 HostName secgw.com IPAddress 10.1.11.5 Aliases [ secgw1 ] Description "Provider Security Gateway 1"
```

**Step 2** Issue the **show System StaticNameLookup host** command to verify the configuration:

```
show System StaticNameLookup host
Host 1 {
    HostName      secgw.com;
    IPAddress    10.1.11.5;
    Description   "Provider Security Gateway 1";
    Aliases      "[ secgw1 ]";
}
```

#### 4.1.15 Configuring IP Routing

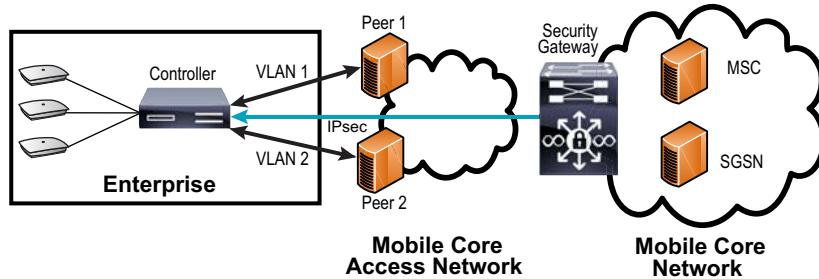
The Cisco small cell solution supports three types of IP routing:

- [Section 4.1.15.1, Configuring Dynamic Routing to the Core Network](#) on page 51
- [Section 4.1.15.2, Configuring Virtual Routing and Forwarding](#) on page 53
- [Section 4.1.15.3, Configuring Static Route Metrics](#) on page 54

##### 4.1.15.1 Configuring Dynamic Routing to the Core Network

The backhaul from the controller may have multiple routes to reach the security gateway in the core network. In configurations with two or more IP interfaces to reach the security gateway, dynamic routing can be used to determine which virtual circuit to use to reach the security gateway, by peering the controller with one or more Border Gateway Protocol (BGP) speakers in the core access network. This is useful for failover redundancy, as the controller can select an alternate path in case the active connection fails. BGP peering is assumed to be outside of the IPsec tunnel.

The controller implements limited support of BGP Version 4 such that the controller can learn routes to the security gateway. The system supports internal and external peers and exchange of IPv4 routing information. It can configure BGP peers and exchange routing information with them including TCP MD5 authentication. It supports a configurable maximum number of routes learned from its BGP peers and hold time, keepalive, and connect-retry timers. Figure 8 shows a logical view of dynamic routing to the core network.



**Figure 8** Dynamic Routing to the Core Network

### To configure dynamic routing to the core network

**Step 1** From the Configuration Mode, issue the following command to configure and enable BGP, and define a peer node. In this example peer 1 has the following attributes:

- description: *SecurityGateway1*
- IP address: 160.1.0.1
- autonomous system number: 22
- connectivity retry timer: 120 seconds (the default)
- hold time: 3 seconds (default is 180)
- keepalive interval: 1 seconds (default is 60)

```
set Layer3Routing BGPv4 88 Enable true Peer 1 Description SecurityGateway1 Address
160.1.0.1 Enable true RemoteAS 22 ConnectRetry 120 Holdtime 3 Keepalive 1
```

**Step 2** Issue the following command to define and enable peer 2. In this example peer 2 has the following attributes:

- description: *SecurityGateway2*
- IP address: 160.1.0.3
- autonomous system number: 22
- the MD5 password for this peer is *myPassword*
- connectivity retry timer: 120 seconds
- hold time: 3 seconds
- keepalive interval: 1 second

```
set Layer3Routing BGPv4 88 Enable true Peer 2 Description SecurityGateway2 Address
160.1.0.3 Enable true RemoteAS 22 Password myPassword ConnectRetry 120 Holdtime 3
Keepalive 3
```

**Step 3** Issue the following command to verify the configuration:

```
show Layer3Routing BGPv4
BGPv4 88 {
  Enable true;
  Peer 1 {
    Address      160.1.0.1;
    Description  SecurityGateway1;
    Enable       true;
    RemoteAS    22;
    Password    myPassword;
    ConnectRetry 120;
    Holdtime    3;
    Keepalive   1;
```

```

}
Peer 2 {
    Address      160.1.0.3;
    Description  SecurityGateway2;
    Enable       true;
    RemoteAS     22;
    ConnectRetry 120;
    Holdtime     3;
    Keepalive    1;
}
}

```

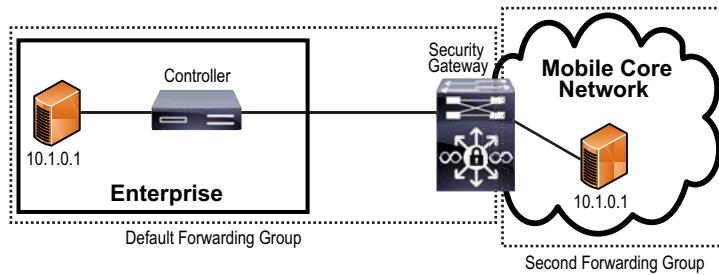
#### 4.1.15.2 Configuring Virtual Routing and Forwarding

The controller requires connectivity to two different routing domains: the provider core network and the enterprise network. As each of these networks is managed by different organizations there is an opportunity for IP address overlapping. The small cell solution supports virtual routing and forwarding to resolve overlapping IP addresses by implementing multiple forwarding groups.

The core network domain contains network elements that provide access to provider services such as the MSC and SGSN located behind the security gateway with which the controller maintains an IPsec tunnel. During IKE negotiations the security gateway provides a list of one or more protected subnets that the controller has access to. The controller assigns these routing entries to a new forwarding group to direct traffic to the appropriate element in the core network.

The controller also communicates with its small cell and other elements in the enterprise network. The enterprise network and the security gateway are in the default forwarding group and the IPsec tunnel is brought up using this forwarding group. Other elements of the core network are in a separate forwarding group. The NTP servers on the core network must be in the new forwarding group. The NTP server on the controller is always in the default forwarding group.

If there are elements with the core network with the same IP addresses as in the enterprise network, controller applications that interact with the core network will not be able to access enterprise elements with the same IP address. Figure 9 shows a logical view elements in the enterprise and core networks with identical IP addresses:



**Figure 9** Network Equipment with Identical IP Addresses

Once the new forwarding group has been created, the core network assigned to it, and the configuration committed, all traffic to the core network other than the security gateway and NTP will be routed using the new forwarding group. Any applications, such as SSH, IuH, SNMP, and Radio Access Network Application Part (RANAP) must accordingly be configured to use this forwarding group.

You must configure the correct core forwarding group for all controller management services. There are no restrictions or validation checks to verify the same forwarding group is used to configure the UMTS and LTE gateways.

This feature does not provide a complete virtual routing and forwarding. It should mainly be used in deployments when the protected subnet advertised by security gateway overlaps with the enterprise small cell networks.

This feature is orthogonal to the existing usage of forwarding groups in the UE flow context. The two should not be confused. Ensure the forwarding group index used for UMTS and LTE gateways is separate from the forwarding group used in Policy configuration used for user devices.



**Note** Creating and enabling a core network forwarding group affects other core network services such as SNMP, syslog, SSH, file transfers, and ping. Ensure that you account for forwarding groups when activating and accessing these other core network services.

To configure virtual routing and forwarding:

**Step 1** From the Configuration Mode, issue the following command to create a new forwarding group for all traffic inside the core network. This example creates forwarding group 2 with the description *CoreNetwork*.

```
set Layer3Forwarding ForwardingGroup 2 Description CoreNetwork
```

**Step 2** Issue the following command to verify the configuration:

```
show Layer3Forwarding ForwardingGroup
ForwardingGroup 2 {
    Description      CoreNetwork;
```

**Step 3** Issue the following command to direct UMTS core network traffic to the new forwarding group:

```
set FAPService 1 FAPControl UMTS Gateway CNForwardingGroupIndex 2
```

**Note:** The current version of the OS software supports one FAPService. Therefore <ServiceNumber> is always 1 (one) in this release.

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS Gateway
CNForwardingGroupIndex    2;
```

**Step 5** Issue the following command to direct LTE core network traffic to the new forwarding group:

```
set FAPService 1 FAPControl LTE Gateway CNForwardingGroupIndex 2
```

**Step 6** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE Gateway
S1ConnectionMode      One;
S1ConnectionEnable    false;
CNForwardingGroupIndex 2;
```

#### 4.1.15.3 Configuring Static Route Metrics

A method of implementing resilient backhaul without dynamic routing is to connect the controller to the security gateway with two independent Ethernet links and configure one as the primary link and the other as the secondary link. This essentially creates a floating static route. The route with the lowest metric carries the traffic. If that link fails its route is removed from the routing table and traffic switches to the secondary route as it would have the lowest (and only) metric.

To configure static route metrics

**Step 1** From the Configuration Mode, issue the following command to configure static route metrics on the primary backhaul link. This example:

- sets and enables the Layer 3 forwarding entry 3
- sets the destination IP address as 172.20.2.1 and subnet mask as 255.255.255.0
- sets the gateway IP address as 172.20.1.1
- uses Ethernet port 1 with IP interface 1
- sets the forwarding metric to 3
- adds the description *Primary*

```
set Layer3Forwarding Forwarding 3 Enable true DestIPAddress 172.20.2.1 DestSubnetMask
255.255.255.0 GatewayIPAddress 172.20.1.1 LANDevice 1 IPInterface1 ForwardingMetric 3
Description Primary
```

**Step 2** Issue the following command to configure static route metrics on the secondary backhaul link. This example:

- sets and enables Layer 3 forwarding entry 4
- sets the destination IP address as 172.20.0.0 and subnet mask as 255.255.255.0
- sets the gateway IP address as 172.20.2.1
- uses Ethernet port 3 with IP interface 1
- sets the forwarding metric to 4
- adds the description Secondary

```
set Layer3Forwarding Forwarding 4 Enable true DestIPAddress 172.20.0.0 DestSubnetMask
255.255.255.0 GatewayIPAddress 172.20.2.1 LANDevice 3 IPInterface1 ForwardingMetric 4
Description Secondary
```

**Step 3** Issue the following command to verify the configuration:

```
show Layer3Forwarding Forwarding
Forwarding 3 {
    Enable          true;
    DestIPAddress  172.20.2.1;
    DestSubnetMask 255.255.255.0;
    GatewayIPAddress 172.20.1.1;
    ForwardingMetric 3;
    Description     Primary;
    LANDevice       3;
    IPInterface     1;
}
Forwarding 4 {
    Enable          true;
    DestIPAddress  172.20.0.0;
    DestSubnetMask 255.255.255.0;
    GatewayIPAddress 172.20.2.1;
    ForwardingMetric 4;
    Description     Secondary;
    LANDevice       2;
    IPInterface     1;
```

## 4.2 Configuring Certificate Revocation Policies

The system has policies that define its behavior in the event that the security certificate revocation information is not available for a controller or small cell during IPsec tunnel establishment. The policies have the following options:

- **IfURISpecified:** The Online Certificate Status Protocol (OCSP) or Certificate Revocation Policy (CRL) must be available for the IPsec tunnel to come up, if OCSP or CRL Uniform Resource Identifier (URI) is specified.
- **NoCheck:** No revocation check is done during IPsec tunnel establishment.
- **NonStrict:** The revocation validation is not strict. The Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) need not be available for the IPsec tunnel to come up.
- **Strict:** The revocation validation is strict. The OCSP or CRL must be available for the IPsec tunnel to come up.

To configure a certificate policy for the controller-to-core tunnel

**Step 1** From the Configuration Mode, issue the following command to set the certificate policy for the connection between the controller and the core network. This example sets the policy to *Strict*.

```
set System CertManagement CoreCertRevocationPolicy Strict
```

**Step 2** Issue the following command to verify the configuration:

```
show System CertManagement CoreCertRevocationPolicy  
CoreCertRevocationPolicy Strict;
```

To configure a certificate policy for the controller-to-small cell tunnel:

**Step 1** From the Configuration Mode, issue the following command to set the certificate policy for the connection between the controller and the core network. This example sets the policy to *NonStrict*.

```
set System CertManagement RNCertRevocationPolicy NonStrict
```

**Step 2** Issue the following command to verify the configuration:

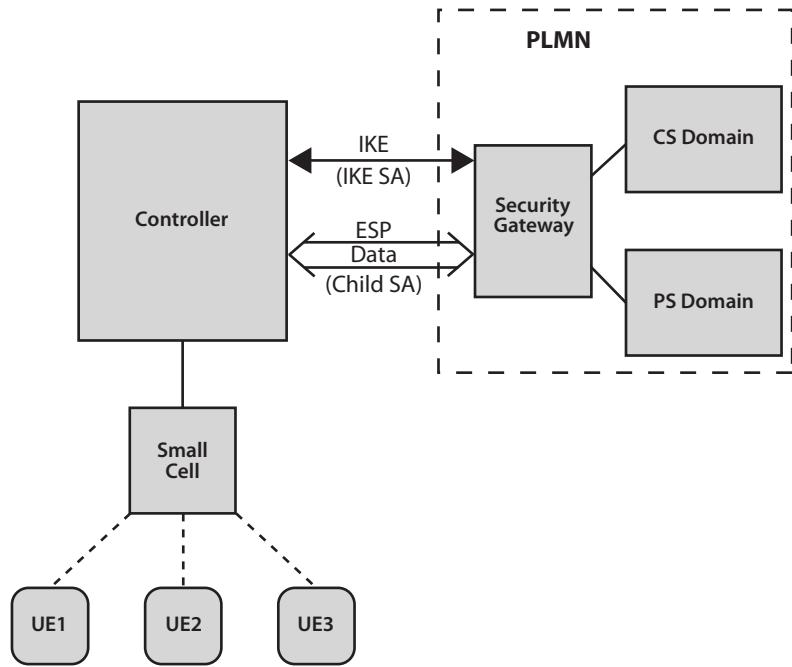
```
show System CertManagement RNCertRevocationPolicy  
RNCertRevocationPolicy NonStrict;
```

## 4.3 Configuring IPsec to the Core Network

The system uses the Internet Protocol Security (IPsec) standard to authenticate and encrypt traffic from the controller to the provider core network. It uses the Internet Key Exchange version 2 (IKEv2) protocol to negotiate keys and Encapsulating Security Payload (ESP) in tunnel mode to carry data.

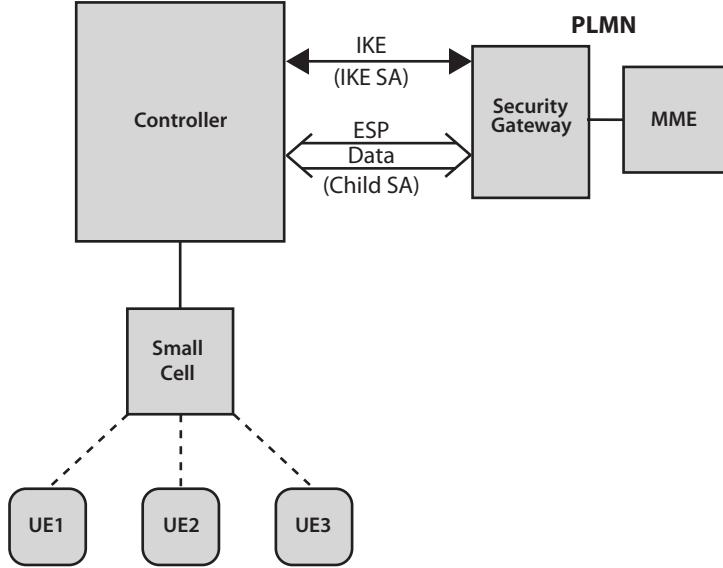
The controller either uses a Pre-Shared Key (PSK) or accepts a signed X.509 certificate to authenticate the security gateway. The security gateway may authenticate the controller using either a PSK or accepting a signed X.509 certificate from the controller.

To exchange voice and data traffic with the core network, the controller can dynamically obtain the IP address it uses for this traffic, the list of subnets behind the security gateway, and from the gateway itself using the IKEv2 configuration payload mechanism. Alternatively, this information can be statically configured through the CLI. [Figure 10](#) shows the IPsec tunnel to the provider core UMTS network.



**Figure 10** UMTS IPsec Tunnel Between the USC 8088 Controller and the Security Gateway

Figure 10 shows the IPsec tunnel to the provider core UMTS network.



**Figure 11** LTE IPsec Tunnel Between the USC 8088 Controller and the Security Gateway

Configuring IPsec to the provide core network in the controller consists configuring the IP address or DNS name of the security gateway, authentication credentials for the security gateway, and cryptographic parameters for the data passed in the tunnel. Refer to [Section 4.3.2, Importing the Security Gateway Trusted Root Certificate](#) on page 58, then [Section 4.3.3, Configuring the IPsec Tunnel for UMTS Traffic](#) on page 59.

## 4.3.1 Before You Begin

Before configuring IPsec to the core network, gather the following information for use in the configuration procedure:

- IP address(es) or fully qualified domain name(s) of the security gateway(s) to the core. Core security gateways are referred to as *SecGWServer* in the CLI. Up to three security gateways can be configured in the controller for redundancy. However the IPsec tunnel is established to only one of them.
- You can authenticate the security gateway with either:
  - **a certificate:** The trusted root certificate used to sign the certificate that the security gateway will send during authentication.
  - **PSK:** The PSK value used by both the security gateway and controller.
- (Optional) IKE parameters. If not specified, the controller will use the default values shown in parentheses.
  - Encryption Algorithm (AES-CBC)
  - Integrity Algorithm (HMAC-SHA1-96)
  - Diffie Hellman Group (2048)
  - Rekey interval (8 hours)
- (Optional) IPsec Parameters. If not specified, the controller will use the default values shown in parentheses.
  - Encryption Algorithm (AES-CBC)
  - Integrity Algorithm (HMAC-SHA1-96)
  - Rekey interval (7 hours)
- If the security gateway does not support the dynamic configuration:
  - Configure the controller the IP address for the virtual interface to the core network.
  - Configure the protected subnets behind the core security gateway such as circuit-switched and packet-switched domains that require IPsec access.

## 4.3.2 Importing the Security Gateway Trusted Root Certificate

For configurations using certificate authentication, import the trusted root certificate for the security gateway into the controller and add it to the IPsec trust store. The IPsec trust store can contain up to 16 certificates.

### To import the security gateway trusted root certificate

**Step 1** From the Operational Mode, get the security gateway trusted root certificate file. Use the **file get** command to copy it from whichever host is available with the Secure Copy Protocol (SCP), File Transfer Protocol (FTP), or Trivial File Transfer Protocol (TFTP). This example uses SCP.

```
file get scp://user@10.1.11.15/a/work/root-ca.pem root-ca.pem
user@10.1.11.15's password:
```

**Step 2** Add the trusted root certificate into the IPsec trust store. In this example, the certificate has the name *root-ca.pem*.

```
request system certificate CACert add Filename root-ca.pem
```

**Step 3** Issue the **show System Certificate CACert** command to verify the configuration:

```
show System Certificate CACert
CACert 1: root-ca.pem
  Description: root-ca.pem
  SerialNumber: C3B25D52709AF299
  Subject: C=US, ST=CA, L=Santa Clara, O=Operator,
            O=Engineering, OU=Development,
            CN=Engineering Root CA/ emailAddress=user@operator.com
  Issuer: C=US, ST=CA, L=Santa Clara, O=Operator,
            O=Engineering, OU=Development,
```

```
CN=Engineering Root CA/ emailAddress=user@operator.com
NotBefore: 2011-03-26T19:15:15Z,
NotAfter: 2021-03-23T19:15:15Z
```

### 4.3.3 Configuring the IPsec Tunnel for UMTS Traffic

IPsec tunnels can be authenticated with either a mutual certificate or mutual PSK.

#### Mutual Certificate Authentication

Configure the following to create an IPsec tunnel with mutual certificate authentication between the controller and the security gateway:

- One of the following:
  - The fully qualified domain name of the core security gateway. You must also configure either a system name server as described in [Section 4.1.13, Configuring DNS Lookup and Domain Search using a Name Server](#) on page 50 or using static name resolution as described in [Section 4.1.14, Configuring Static Name Resolution](#) on page 51.
  - The IP address of the security gateway server in the `SecGWServer<number>` field and the fully qualified domain name of the security gateway in the `SecGWServer<number>/IPsecId` field to authenticate the ID of the security gateway in its certificate.
- A *CryptoProfile* specifying the required IKE and IPsec parameters, and *PkeyIndex* (controller Pkey). The *PkeyIndex* must always be 1.
- A *VirtualInterface* specifying the *CryptoProfile* and *SecGWServerIndex*.

#### Mutual PSK Authentication

Configure the following to create an IPsec tunnel from the controller to the security gateway using mutual Pre-Shared Key (PSK) authentication:

- The IP address or fully qualified domain name of the core security gateway. When using a fully qualified domain name, you must also configure the system name server as described in [Section 4.1.13, Configuring DNS Lookup and Domain Search using a Name Server](#) on page 50.
- The pre-shared key used by both the security gateway and controller.
- A *Cryptoprofile* specifying the required IKE and IPsec parameters and security gateway pre-shared key index for the PSK.
- A virtual interface specifying the *Cryptoprofile* and security gateway server index.

#### To configure IPsec to the core network

- Step 1** From the Configuration Mode, configure the `SecGWServer` with the IP address or fully qualified domain name of the core security gateways. Here three security gateways are defined. Security gateway number 1 has the IP address 10.1.11.15. Security gateway number 2 has the fully qualified domain name *certificate.provider.net*. Security gateway number 3 with an IP address of 10.1.11.17 that has the fully qualified domain name *certificate3.provider.net*.

```
set FAPService 1 FAPControl UMTS Gateway SecGWServer1 10.1.11.15
set FAPService 1 FAPControl UMTS Gateway SecGWServer2 certificate.provider.net
set FAPService 1 FAPControl UMTS Gateway SecGWServer3 10.1.11.17 SecGWServer3IPSecId
certificate3.provider.net
```

- Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS Gateway
SecGWServer1          10.1.11.15;
```

```
SecGWServer2          certificate.provider.net;
SecGWServer3          10.1.11.17;
SecGWServer3IPSecId   certificate3.provider.net;
```

**Step 3** For static IP configuration, if the security gateway does not support the configuration payload:

- Configure the controller IP address of the virtual interfaces (up to eight) that connect to the protected subnetworks. In this example, the virtual interface has an IP address of 172.16.1.100 with a subnet mask of 255.255.255.0,

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 1 ConfigIPAddress
172.16.1.100 ConfigIPMask 255.255.255.0 enable true
    ◆ Configure the protected subnets of the circuit-switched domain. In this example, the circuit-switched domain is assigned to the static configuration 1, has the description Voice_Services, and has an IP address of 192.168.1.0 with a subnet mask of 255.255.255.0.
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 1 ProtectedSubnet 1
DestIPAddress 192.168.1.0 DestSubnetMask 255.255.255.0 Description Voice_Services Enable
true
    ◆ If needed, configure additional IP addresses to the protected subnets. This example configures the virtual interface 172.16.1.200:
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 2 ConfigIPAddress
172.16.1.200 ConfigIPMask 255.255.255.0 enable true
    ◆ Configure the protected subnets of the packet-switched domain. In this example, the packet-switched domain is assigned to the static configuration 2, has the description Data_Services, and has an IP address of 192.168.2.0 with a subnet mask of 255.255.255.0.
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 2 ProtectedSubnet 2
DestIPAddress 192.168.2.0 DestSubnetMask 255.255.255.0 Description Data_Services Enable
true
    ◆ Enable the static configuration of the IP address and protected core subnets:
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfigEnable true
```

**Step 4** For dynamic IP configurations, you may request that a specific IP address from the security gateway and optionally enforce that the IP address the security gateway assigned is the same as that requested. When enforced, the core IPsec tunnel will not come up unless the IP addresses match. If the *RequestedIPAddress* parameter is not configured, the security gateway may assign any IP address to the controller. This example requests address 172.16.1.100. This example does not require a specific IP address.

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfigEnable false
RequestedIPAddress 172.16.1.100 RequestedIPAddressEnforced false
```

**Step 5** Configure and enable a *VirtualInterface* by specifying the *CryptoProfile* and *SecGWServerIndex*.

```
set FAPService 1 Transport Tunnel VirtualInterface 1 SecGWServerIndex 1
CryptoProfileIndex 1 Enable true
```

**Step 6** Issue the `show FAPService <ServiceNumber> Transport Tunnel` command to verify the configuration:

```
show FAPService 1 Transport Tunnel
VirtualInterface 1 {
    Enable           true;
    DSCPMarkPolicy -1;
    CryptoProfileIndex 1;
    SecGWServerIndex 1;
}
SecGWServer 1 {
    RequestedIPAddress      0.0.0.0;
    RequestedIPAddressEnforced false;
    StaticConfigEnable       true;
    StaticConfig 1 {
        Enable           true;
```

```

ConfigIPAddress 172.16.1.100;
ConfigIPMask    255.255.255.0;
ProtectedSubnet 1 {
    Description   Voice_Services;
    Enable        true;
    DestIPAddress 192.168.1.0;
    DestSubnetMask 255.255.255.0;
}
}
StaticConfig 2 {
    Enable          true;
    ConfigIPAddress 172.16.1.200;
    ConfigIPMask    255.255.255.0;
    ProtectedSubnet 2 {
        Description   Data_Services;
        Enable        true;
        DestIPAddress 192.168.2.0;
        DestSubnetMask 255.255.255.0;
    }
}
}
}

```

**Step 7** Do one of the following

- For mutual certificate authentication: configure and enable a *CryptoProfile* specifying the required IKE and IPsec parameters. Here, no IKE and IPsec parameters are configured letting the controller use the defaults.

```
set FAPService 1 Transport Security CryptoProfile 1 SecGWPkeyIndex 1 PkeyIndex 1 Enable true
```

- For mutual PSK authentication: configure and enable the pre-shared key for the security gateway and controller. In this example, the PSK is set to *0x87f2540332abd7731c88a*.

```
set FAPService 1 Transport Security PreSharedKey 1 Enable true Password 0x87f2540332abd7731c88a
```

Configure and enable a *Cryptoprofile* specifying the required IKE and IPsec parameters and security gateway PSK index using the pre-shared key just added. Here, no IKE and IPsec parameters are configured, letting the controller use the defaults.

```
set FAPService 1 Transport Security CryptoProfile 1 SecGWPreSharedKeyIndex 1 Enable true
```

**Step 8** Issue the following command to verify the configuration:

```
show FapService 1 Transport Security
PreSharedKey 1 {
    Enable  true;
    Password 0x87f2540332abd7731c88a;
}
```

**Step 9** Configuration is complete. Commit the changes.

```
commit
```

**Step 10** From the Operational Mode, issue the **show Core IPSec** command to verify that the IPsec tunnel to the core has been established:

```
show Core IPSec
SecGWServer: 1 10.1.194.2 <-> 10.1.11.15 (Established)
    Status: Established
    LastTriedTime: 2011-12-06T18:45:18Z
    LocalIPAddress: 10.1.192.2
    IKESA: 1
        Status: Completed, CreationTime: 2011-12-06T18:45:19Z
        IPAddress: 172.16.200.1, SubnetMask: 255.255.255.0
```

```

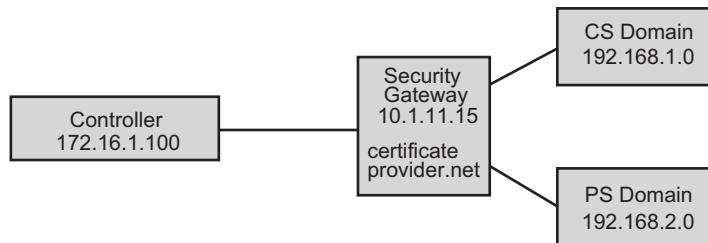
IKEEncryptInUse: AES-CBC, IKEPRFInUse: HMAC-SHA1, IKEIntegrityInUse: HMAC-SHA1-
96, IKEDHInUse: 1024
ChildSA: 29 (outbound)
    SPI: 3711271924, CreationTime: 2011-12-06T18:45:19Z
    ESPEncryptInUse: AES-CBC, ESPIntegrityInUse: HMAC-SHA1-96
    TrafficBytes: 0, TrafficPackets: 0
    IntegrityErrors: 0, ReplayErrors: 0, CryptErrors: 0, DecryptErrors: 0, SAErrors:
0, PolicyErrors: 0, SoftLifeErrors: 0
ChildSA: 30 (inbound)
    SPI: 3351559461, CreationTime: 2011-12-06T18:45:19Z
    ESPEncryptInUse: AES-CBC, ESPIntegrityInUse: HMAC-SHA1-96
    TrafficBytes: 49896, TrafficPackets: 1134
    IntegrityErrors: 0, ReplayErrors: 0, CryptErrors: 0, DecryptErrors: 0, SAErrors:
0, PolicyErrors: 0, SoftLifeErrors: 0

SecGWServer 2: - (Untried)

```

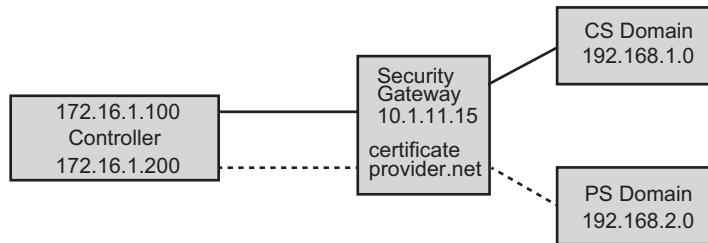
The number of *IKESA NumberOfEntries* should be 1. The number of *ChildSANumberOfEntries* should be 2 (one each for inbound and outbound traffic). The peer address and the subnet mask are assigned to the IKESA by the security gateway.

[Figure 12](#) shows a controller with one virtual interface to the core network with separate protected subnets for voice and data traffic:



**Figure 12** One Virtual IP Address to the Core Network

[Figure 13](#) shows a controller with two virtual interfaces to the core network, each with a separate protected subnet:



**Figure 13** Two Virtual IP Addresses to the Core Network

#### 4.3.4 Configuring the IPsec Tunnel for LTE Traffic

IPsec tunnels can be authenticated with either a mutual certificate or mutual PSK.

##### Mutual Certificate Authentication

Configure the following to create an IPsec tunnel with mutual certificate authentication between the controller and the security gateway:

- One of the following:

- The fully qualified domain name of the core security gateway. You must also configure either a system name server, as described in [Section 4.1.13, Configuring DNS Lookup and Domain Search using a Name Server](#) on page 50 or using static name resolution as described in [Section 4.1.14, Configuring Static Name Resolution](#) on page 51
- The IP address of the security gateway server in the `SecGWServer<number>` field and the fully qualified domain name of the security gateway in the `SecGWServer<number>/IPsecId` field to authenticate the ID of the security gateway in its certificate.
- A *CryptoProfile* specifying the required IKE and IPsec parameters, and *PkeyIndex* (controller Pkey). The *PkeyIndex* must always be 1.
- A *VirtualInterface* specifying the *CryptoProfile* and *SecGWServerIndex*.

### Mutual PSK Authentication

Configure the following to create an IPsec tunnel from the controller to the security gateway using mutual Pre-Shared Key (PSK) authentication:

- The IP address or fully qualified domain name of the core security gateway. When using a fully qualified domain name, you must also configure the system name server.
- The pre-shared key used by both the security gateway and controller.
- A *Cryptoprofile* specifying the required IKE and IPsec parameters and security gateway pre-shared key index for the PSK.
- A virtual interface specifying the *Cryptoprofile* and security gateway server index.

### To configure IPsec to the core network

**Step 1** From the Configuration Mode, configure the `SecGWServer` with the IP address or fully qualified domain name of the core security gateways. Here three security gateways are defined:

- Security gateway number 1 has the IP address 10.2.11.15.
- Security gateway number 2 has the fully qualified domain name `certificate.provider.net`.
- Security gateway number 3 with an IP address of 10.2.11.17 that has the fully qualified domain name `certificate3.provider.net`.

```
set FAPService 1 FAPControl LTE Gateway SecGWServer1 10.2.11.15
set FAPService 1 FAPControl LTE Gateway SecGWServer2 certificate.provider.net
set FAPService 1 FAPControl LTE Gateway SecGWServer3 10.2.11.17 SecGWServer3IPSecId
certificate3.provider.net
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE Gateway
SecGWServer1          10.2.11.15;
SecGWServer2          certificate.provider.net;
SecGWServer3          10.2.11.17;
SecGWServer3IPSecId   certificate3.provider.net;
```

**Step 3** Issue the following command to associate the tunnel security gateway server to the security gateway server with the LTE FAPService gateway server. The example associates the FAPControl security gateway server 1 to the transport tunnel security gateway server 1.

```
set FAPService 1 Transport Tunnel SecGWServer 1 FAPServiceType LTE FAPSecGWServer 1
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel SecGWServer 1
FAPServiceType        LTE;
FAPSecGWServer       1;
```

**Step 5** For static IP configuration, if the security gateway does not support the configuration payload:

- Configure the controller IP address of the virtual interfaces (up to eight) that connect to the protected subnetworks. In this example, the virtual interface has an IP address of 172.16.1.100 with a subnet mask of 255.255.255.0,

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 1 ConfigIPAddress
172.16.1.100 ConfigIPMask 255.255.255.0 enable true
  ◆ Configure the protected subnets of the circuit-switched domain. In this example, the circuit-switched domain is assigned to the static configuration 1, has the description LTE_Services, and has an IP address of 192.168.1.0 with a subnet mask of 255.255.255.0.
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 1 ProtectedSubnet 1
DestIPAddress 192.168.1.0 DestSubnetMask 255.255.255.0 Description LTE_Services Enable
true
  ◆ If needed, configure additional IP addresses to the protected subnets. This example configures the virtual interface 172.16.1.200:
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 2 ConfigIPAddress
172.16.1.200 ConfigIPMask 255.255.255.0 enable true
  ◆ Configure the protected subnets of the packet-switched domain. In this example, the packet-switched domain is assigned to the static configuration 2, has the description Data_Services, and has an IP address of 192.168.2.0 with a subnet mask of 255.255.255.0.
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfig 2 ProtectedSubnet 2
DestIPAddress 192.168.2.0 DestSubnetMask 255.255.255.0 Description Data_Services Enable
true
  ◆ Enable the static configuration of the IP address and protected core subnets:
```

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfigEnable true
```

**Step 6** For dynamic IP configurations, you may request that a specific IP address from the security gateway and optionally enforce that the IP address the security gateway assigned is the same as that requested. When enforced, the core IPsec tunnel will not come up unless the IP addresses match. If the *RequestedIPAddress* parameter is not configured, the security gateway may assign any IP address to the controller. This example requests address 172.16.1.100. This example does not require a specific IP address.

```
set FAPService 1 Transport Tunnel SecGWServer 1 StaticConfigEnable false
RequestedIPAddress 172.16.1.100 RequestedIPAddressEnforced false
```

**Step 7** Configure and enable a *VirtualInterface* by specifying the *CryptoProfile* and *SecGWServerIndex*.

```
set FAPService 1 Transport Tunnel VirtualInterface 1 SecGWServerIndex 1
CryptoProfileIndex 1 Enable true
```

**Step 8** Issue the `show FAPService <ServiceNumber> Transport Tunnel` command to verify the configuration:

```
show FAPService 1 Transport Tunnel
VirtualInterface 1 {
    Enable           true;
    DSCPMarkPolicy -1;
    CryptoProfileIndex 1;
    SecGWServerIndex 1;
}
SecGWServer 1 {
    FAPServiceType      LTE;
    FAPSecGWServer     1;
    RequestedIPAddress 0.0.0.0;
    RequestedIPAddressEnforced false;
    StaticConfigEnable true;
    StaticConfig 1 {
        Enable           true;
        ConfigIPAddress 172.16.1.100;
        ConfigIPMask     255.255.255.0;
    }
}
```

```

ProtectedSubnet 1 {
    Description    LTE_Services;
    Enable         true;
    DestIPAddress 192.168.1.0;
    DestSubnetMask 255.255.255.0;
}
}
StaticConfig 2 {
    Enable         true;
    ConfigIPAddress 172.16.1.200;
    ConfigIPMask   255.255.255.0;
    ProtectedSubnet 2 {
        Description    Data_Services;
        Enable         true;
        DestIPAddress 192.168.2.0;
        DestSubnetMask 255.255.255.0;
    }
}
}
}

```

**Step 9** Do one of the following

- For mutual certificate authentication: configure and enable a *CryptoProfile* specifying the required IKE and IPsec parameters. Here, no IKE and IPsec parameters are configured letting the controller use the defaults.

```
set FAPService 1 Transport Security CryptoProfile 1 SecGWPkeyIndex 1 PkeyIndex 1 Enable true
```

- For mutual PSK authentication: configure and enable the pre-shared key for the security gateway and controller. In this example, the PSK is set to *0x87f2540332abd7731c88a*.

```
set FAPService 1 Transport Security PreSharedKey 1 Enable true Password 0x87f2540332abd7731c88a
```

Configure and enable a *Cryptoprofile* specifying the required IKE and IPsec parameters and security gateway PSK index using the pre-shared key just added. Here, no IKE and IPsec parameters are configured, letting the controller use the defaults.

```
set FAPService 1 Transport Security CryptoProfile 1 SecGWPreSharedKeyIndex 1 Enable true
```

**Step 10** Issue the following command to verify the configuration:

```
show FapService 1 Transport Security
PreSharedKey 1 {
    Enable     true;
    Password   0x87f2540332abd7731c88a;
}
```

**Step 11** Configuration is complete. Commit the changes.

```
commit
```

**Step 12** From the Operational Mode, issue the **show Core IPSec** command to verify that the IPsec tunnel to the core has been established:

```
show Core IPSec Detail
SecGWServer: 1 (10.2.11.15)
FAPServiceType: LTE, FAPSecGWServer: 1
Status: Established
LastTriedTime: 2014-02-10T16:49:21Z
LocalIPAddress: 10.1.192.2
IKESA: 96
    Status: Completed, CreationTime: 2014-02-10T16:49:21Z, NextRekeyTime: 2014-02-10T23:46:21Z, ExpirationTime: 2014-02-11T00:49:21Z
    IPAddress: 172.16.200.100, SubnetMask: 255.255.255.0
```

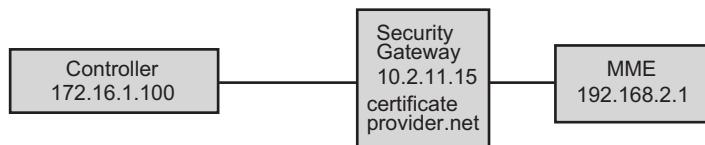
```

IKEEncryptInUse: AES-CBC, IKEPRFInUse: HMAC-SHA1, IKEIntegrityInUse: HMAC-SHA1-
96, IKEDHInUse: 1024
    ChildSA: 697 (outbound)
        SPI: 3416429826, CreationTime: 2014-02-10T16:49:21Z, NextRekeyTime: 2014-02-
10T22:25:21Z, ExpirationTime: 2014-02-10T23:49:21Z
        ESPEncryptInUse: Null, ESPIntegrityInUse: HMAC-SHA1-96
        TrafficBytes: 0, TrafficPackets: 0
        IntegrityErrors: 0, ReplayErrors: 0, CryptErrors: 0, DecryptErrors: 0, SAErrors:
0, PolicyErrors: 0, SoftLifeErrors: 0
    ChildSA: 698 (inbound)
        SPI: 3321205803, CreationTime: 2014-02-10T16:49:21Z, NextRekeyTime: 2014-02-
10T22:46:21Z, ExpirationTime: 2014-02-10T23:49:21Z
        ESPEncryptInUse: Null, ESPIntegrityInUse: HMAC-SHA1-96
        TrafficBytes: 0, TrafficPackets: 0
        IntegrityErrors: 0, ReplayErrors: 0, CryptErrors: 0, DecryptErrors: 0, SAErrors:
0, PolicyErrors: 0, SoftLifeErrors: 0

```

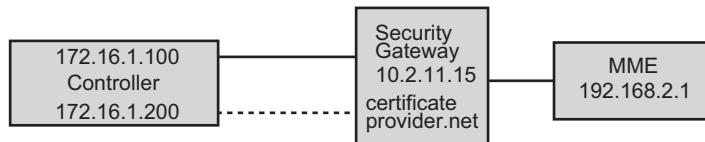
The number of *IKESANumberOfEntries* should be 1. The number of *ChildSANumberOfEntries* should be 2 (one each for inbound and outbound traffic). The peer address and the subnet mask are assigned to the IKESA by the security gateway.

[Figure 12](#) shows a controller with one virtual interface to the core network with separate protected subnets for voice and data traffic:



**Figure 14** One Virtual IP Address to the Core Network

[Figure 13](#) shows a controller with two virtual interfaces to the core network, each with a separate protected subnet:



**Figure 15** Two Virtual IP Addresses to the Core Network

## 4.4 Configuring a 6in4 Tunnel to the Core Network

The controller supports connecting to an IPv6 Evolved Packet Core (EPC) over a 6in4 tunnel (RFC 4213) that encapsulates IPv6 packets in IPv4 for transmission over an IPv4 network. This feature requires that either the security gateway can terminate the 6in4 tunnel or that a separate device (such as a multi-protocol router) in the security gateway's protected subnet can terminate the 6in4 tunnel. Traffic from the core network to the controller can be directed to either an IPv4 or IPv6 address.

Use of 6in4 tunneling allows the following to be access through IPv6:

- SNMP trap servers and targets
- syslog trap targets
- file uploads
- file get and put transfers
- NTP servers

- DNS servers
- eRMS management system servers

Encapsulating traffic in a 6in4 tunnel adds 20 bytes of overhead to each packet. Consider the implications of the additional packet size and adjust the TCP Maximum Segment Size (MSS) as needed. Refer to [Section 16.3, Adjusting the LTE TCP MSS](#) on page 228 for more information about LTE TCP MSS.

#### 4.4.1 Configuring a 6in4 Tunnel Using an IPsec Virtual Interface

To configure a 6in4 tunnel to the core network using an IPsec virtual interface

- Step 1** If it has not been previously created, from the Configuration Mode issue the following command to create and enable an IPsec virtual interface to associate an IPsec transport tunnel. This example assumes that IPsec has been configured on the controller using virtual interface 1 and it shows the enabling of the virtual interface to bring up the IPsec tunnel.

```
set FAPService 1 Transport Tunnel VirtualInterface 1 Enable true
```

- Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface 1
Enable          true;
```

- Step 3** Issue the following command to verify that the tunnel is up:

```
show Core IPSec Detail
SecGWServer: 1 (10.2.11.15)
  FAPServiceType: LTE, FAPSecGWServer: 1
  Status: Established
  LastTriedTime: 2014-02-10T16:49:21Z
  LocalIPAddress: 10.1.192.2
  IKESA: 96
    Status: Completed, CreationTime: 2014-02-10T16:49:21Z, NextRekeyTime:

[output truncated]
```

- Step 4** Issue the following command to create and enable a 6in4 tunnel from the controller to the core network security gateway or device in its protected subnet that can terminate a 6in4 tunnel connection. This example:

- creates and enables 6in4 tunnel 1
- with the controller IPv6 local virtual interface provided by the security gateway of 1. The inner IP address or virtual IP address of the controller terminates the 6in4 tunnel on the controller.
- with the remote IPv4 address that is part of the core subnet protected by the IPsec tunnel of 210.3.0.1. The device at 210.3.0.1 terminates the 6in4 tunnel in the core network.
- the controller will use an IPv6 IP address fd0c:d934:f30d::0002:2 with a prefix length of 112 bits to reach the IPv6 core network

```
set TunnelDevice 1 Enable true Type 6in4 LocalVirtualInterface [ 1 ] RemoteIPAddress
210.3.0.1 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
fd0c:d934:f30d::0002:2 IPInterfacePrefixLength 112
```

- Step 5** Issue the following command to validate the configuration:

```
show TunnelDevice 1
Enable          true;
Type            6in4;
LocalVirtualInterface "[ 1 ]";
RemoteIPAddress 210.3.0.1;
LANHostConfigManagement {
  IPInterface 1 {
    Enable          true;
```

```

    IPIInterfaceIPAddress      fd0c:d934:f30d::0002:2;
    IPIInterfacePrefixLength 112;
}
}

```

## 4.4.2 Configuring a 6in4 Tunnel Using a Local IP Address

The controller does not support the configuration of an IPv6 address on Ethernet interfaces or the configuration of IPv6 static routes. It does support configuring an IPv6 default route through a 6in4 tunnel. Cisco Systems recommends this configuration for installations using a 6in4 tunnel to reach an IPv6 core network.

To configure a 6in4 tunnel to the core network using a local IP address

**Step 1** From the Configuration Mode, issue the following command to enable an IPv6 default route:

**Step 2** Issue the following command to create and enable a 6in4 tunnel from the controller to the core network security gateway or device in its protected subnet that can terminate a 6in4 tunnel connection. This example:

- creates and enables 6in4 tunnel 1
- with the controller local IPv4 address provided by the security gateway 172.19.0.69
- with the remote IPv4 address that is part of the core subnetwork protected by the IPsec tunnel of 210.3.0.1

```
set TunnelDevice 1 Enable true Type 6in4 LocalIPAddress 172.19.0.69 RemoteIPAddress
210.3.0.1 LANHostConfigManagement IPIInterface 1 Enable true IPIInterfaceIPAddress
fd0c:d934:f30d::0002:2 IPIInterfacePrefixLength 112
```

**Step 3** Issue the following command to validate the configuration:

```
show TunnelDevice 1
Enable                  true;
Type                   6in4;
LocalIPAddress        172.19.0.69;
RemoteIPAddress       210.3.0.1;
IPv6AutoDefaultRouteEnable true;
LANHostConfigManagement {
    IPIInterface 1 {
        Enable              true;
        IPIInterfaceIPAddress fd0c:d934:f30d::0002:2;
        IPIInterfacePrefixLength 112;
    }
}
```

## 4.5 Configuring IPsec to the Small Cell

The traffic between the controller and a small cell can be in one of two security modes:

- **Secure mode:** packets between the controller and a small cell are authenticated and encrypted. Secure is the default mode, and the recommended operating mode.
- **Open mode:** packets are authenticated, but not encrypted. Open mode exists for easier debugging of the traffic flow between the controller and a small cell with packet capture. Cisco Systems does not recommend using open mode other than for debugging purposes.

By default, small cells boot up in secure mode. When configuring a small cell from an unprovisioned state, the radio automatically reboots with the configured security mode. If the small cell has previously been provisioned, you must manually reboot it after modifying the security mode.

## To configure the IPsec tunnel in secure mode between the services and small cells

When a small cell is created and enabled, it is in secure mode by default. The procedure below is only required if the small cell has been placed in an open security mode.

- Step 1** From the Configuration Mode, enable secure mode between the controller and small cell. This example uses small cell 68.

```
set RadioNode 68 SecurityMode secure Enable true
```

- Step 2** Issue the `show RadioNode <Number>` command to verify the configuration after the small cell reboots:

```
show RadioNode 68
RadioNode 68 {
    Enable                      true;
    SecurityMode                secure;
}
```

## To configure the IPsec tunnel in open mode between the services and small cells



Cisco Systems does not recommend using the open security mode as traffic between the controller and the small cell is not encrypted, and is sent in the clear. Only enable open mode to perform debugging for traffic packet capture.

- Step 1** From the Configuration Mode, disable encryption on traffic between the controller and the small cell: This example uses small cell 57.

```
set RadioNode 57 SecurityMode open Enable true
```

- Step 2** Issue the `show RadioNode <Number>` command to verify the configuration after the small cell reboots:

```
show RadioNode 57
Enable                      true;
SecurityMode                open;
```

## 4.6 Deployment Considerations with a Firewall

The system can be placed in various locations in the network topology. Select the appropriate deployment scenario based upon the enterprise IT infrastructure, the backhaul type, and the mobile network architecture. This section discusses various deployment models and the recommended firewall settings for optimal operation.

If the firewall is doing address translation, any protocols that carry IP addresses can fail if the Network Address Translation (NAT) does not have specific application layer gateway support for that protocol. If the small cell is in the inside network, then any protocol message from the small cell that carries the small cell's address will be incorrect when it reaches the controller unless the firewall is properly configured.

There are two types of NAT:

- **Basic NAT:** The simplest type of NAT provides a one-to-one translation of IP addresses. In this type of NAT, only the IP addresses and checksums are changed. For basic TCP/UDP functionality, the rest of the packet can be left untouched. Basic NAT can be used to interconnect two IP networks with incompatible addressing.

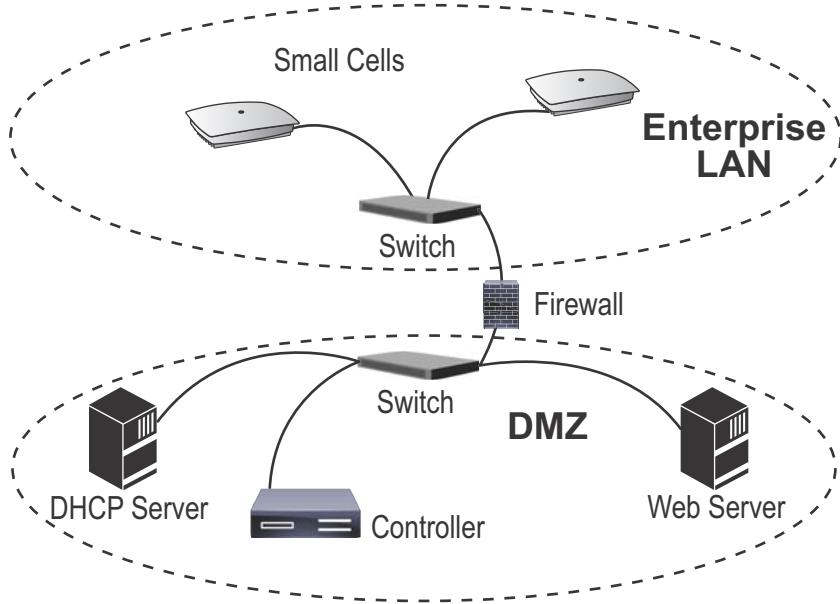
- **NAT with Port Translation (NAPT):** An entire IP address space, usually consisting of private IP addresses, is hidden behind a single or small group of IP address in another address space. NAPT is also known as Port Address Translation (PAT), IP masquerading, and NAT Overload. To avoid ambiguity in the handling of returned packets, a one-to-many NAT must alter higher level information such as TCP/UDP ports in outgoing communications and must maintain a translation table so that return packets can be correctly translated back.

## 4.6.1 USC 8088 Controller Deployed Outside the Enterprise Intranet

In some configurations the controller will be deployed within the enterprise DMZ. This allows it to connect directly with the mobile core without any firewall restrictions from the enterprise. It also keeps it outside the enterprise's LAN/intranet, providing added security.

A VLAN can then be used to connect all of the small cells to the controller. All traffic between the controller and small cells in such a topology will have to traverse a firewall, which in many cases could be configured to perform NAT functions.

**Figure 16** shows the topology of the small cell network with the small cells inside the corporate intranet:



**Figure 16** Firewall between Enterprise LAN and Intranet

If the deployment has a firewall between the controller and the small cells with the small cells inside the enterprise LAN, configure the firewall as per the information shown in [Table 8](#) to allow the small cell to communicate with the controller.

**Table 8: Required Open Firewall Ports**

Direction	Source	Destination	Protocol	Detail
RN → DHCP Server	68	67	UDP	DHCP (bootp)
DHCP Server → RN	67	68	UDP	DHCP (bootp)
DHCP Relay Agent ↔ DHCP Server	67	67	UDP	DHCP (bootp)
RN ↔ SN	62000	62000	UDP	Cisco booting
RN ↔ SN	500	500	UDP	IKE

**Table 8: Required Open Firewall Ports**

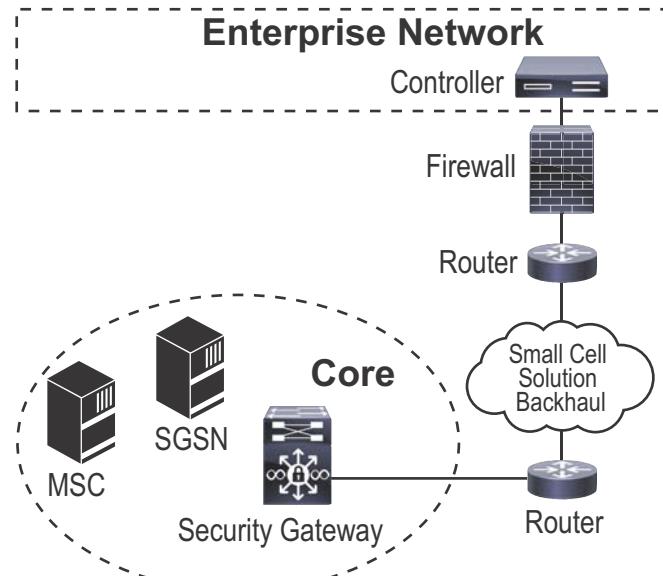
Direction	Source	Destination	Protocol	Detail
RN ↔ SN	4500	4500	UDP	NAT traversal
RN ↔ SN	N/A	N/A	ESP	IPsec
RN ↔ SN	319	319	UDP	PTP
SN → Core	179	179	TCP	BGP Routing



While the IPsec tunnel between a radio node and the services node is establishing, the X.509 certificates that are exchanged may be large enough to produce IP fragments. The firewall should also be configured to pass fragments if the radio node is not able to move past the OOS\_AUTHENTICATING state.

#### 4.6.2 USC 8088 Controller Deployed Inside the Enterprise Intranet

Figure 17 shows the topology of the network with the firewall between the enterprise network and the provider core network:



**Figure 17** Firewall between Enterprise Network and Core Provider Network

If the deployment has a firewall between the controller and the core provider network, configure the firewall as per the information shown in [Table 9](#) to allow the controller to communicate with the core network.

**Table 9: Required Open Firewall Ports**

Direction	Source	Destination	Protocol	Detail
SN $\leftrightarrow$ Core	N/A	N/A	ESP	IPsec
SN $\leftrightarrow$ Core	500	500	UDP	IKE
SN $\leftrightarrow$ Core	4500	4500	UDP	NAT traversal
SN $\rightarrow$ Core	any	53	UDP	DNS

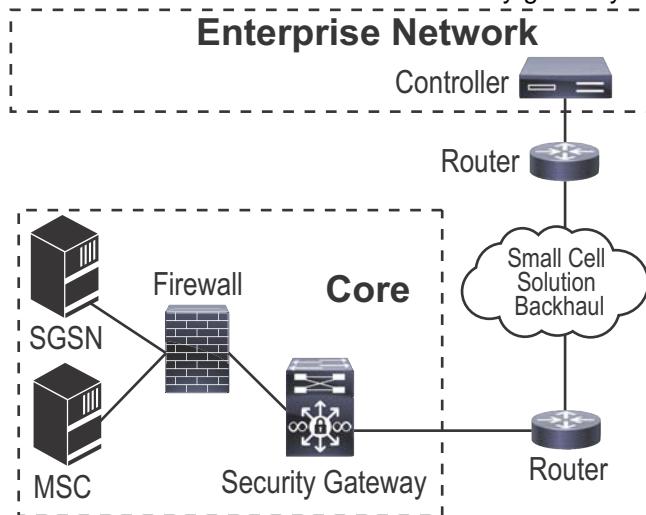
### 4.6.3 Firewall Inside the Core Network

Some configurations place a firewall inside the provider core network after the security gateway. Cisco supports configurations with Iu/IP, Iuh, S1, and dual-mode connections between the controller and the core network security gateway. The four connections require different firewall configurations.

- [Section 4.6.3.1, UMTS Iu/IP Firewall Considerations](#) on page 72
- [Section 4.6.3.2, UMTS Iuh Firewall Considerations](#) on page 73
- [Section 4.6.3.3, LTE S1 Firewall Considerations](#) on page 74
- [Section 4.6.3.4, Dual-Mode Firewall Considerations](#) on page 75

#### 4.6.3.1 UMTS Iu/IP Firewall Considerations

[Figure 18](#) shows the logical connection between the controller and security gateway with an Iu/IP connection:



**Figure 18** Firewall in the Provider Core Network after the Security Gateway with an Iu/IP Connection

If the deployment has a firewall inside the provider core network after traffic has traversed the security gateway and has been decrypted:

**Table 10: Required Open Firewall Ports with Iu/IP Connections**

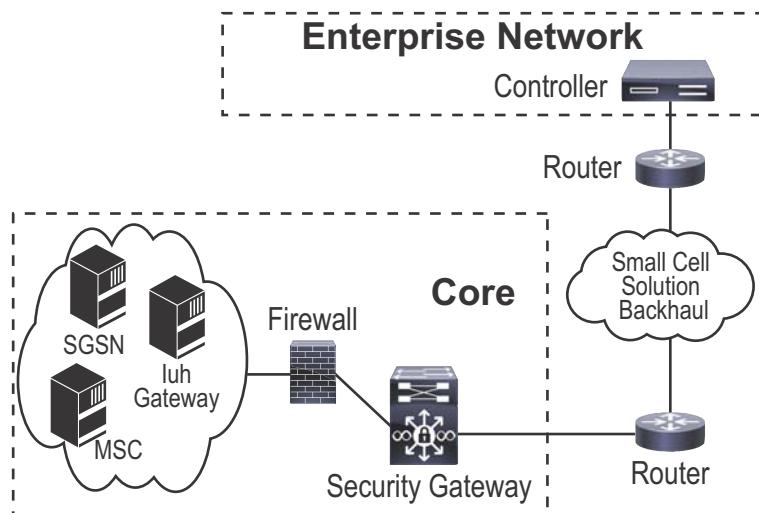
Direction	Source	Destination	Protocol	Detail	Traverses
SN ↔ Core	123	123	UDP	NTP	Management plane
SN ↔ Core	*A	*B	SCTP	CS domain	Control plane
SN ↔ Core	*C	*D	SCTP	PS domain	Control plane
SN → Core	any	*E	UDP (RTP)	CS domain	User plane
SN → Core	any	*F	UDP (GTP)	PS domain	User plane
SN → Core	any	162	UDP	SNMP trap	Management plane
Core → SN	any	161	UDP	SNMP query	Management plane
Core ↔ SN	any	22	TCP	SSH	Management plane

Several port numbers correspond to Signaling Transport (SIGTRAN) configuration parameters that are defined in \*A through \*D below:

- \*A: The port number of the SCTP endpoint of the controller in a circuit-switched domain.
- \*B: The port number of the SCTP endpoint of the mobile switching center in a circuit-switched domain.
- \*C: The port number of the SCTP endpoint of the controller in a packet-switched domain.
- \*D: The port number of the SCTP endpoint of the Serving GPRS Support Node (SGSN) in a packet-switched domain.
- \*E: The port number is managed by the provider core network.
- \*F: The port number is managed by the provider core network. (A commonly used port number is 2152.)

#### 4.6.3.2 UMTS Iuh Firewall Considerations

Figure 19 shows the logical connection between the controller and security gateway with an Iuh connection:



**Figure 19** Firewall in the Provider Core Network after the Security Gateway with an Iuh Connection

If the deployment has a firewall inside the provider core network after traffic has traversed the security gateway and has been decrypted:

**Table 11: Required Open Firewall Ports with an Iuh Connection**

Direction	Source	Destination	Protocol	Detail	Traverses
SN ↔ Core	123	123	UDP	NTP	Management plane
SN ↔ Core	*A	*B	SCTP	Iuh	Control plane
SN → Core	any	*C	UDP (RTP)	CS domain	User plane
SN → Core	any	*D	UDP (GTP)	PS domain	User plane
SN → Core	any	162	UDP	SNMP trap	Management plane
Core → SN	any	161	UDP	SNMP query	Management plane
Core ↔ SN	any	22	TCP	SSH	Management plane

Several port numbers correspond to Signaling Transport (SIGTRAN) configuration parameters that are defined in \*A and \*B below:

\*A: The configured port number (default 1024) of the SCTP endpoint of the controller for Iuh. This object is *FAPService.{i}.FAPControl.UMTS.Gateway.FAPLocalPort* in the data model.

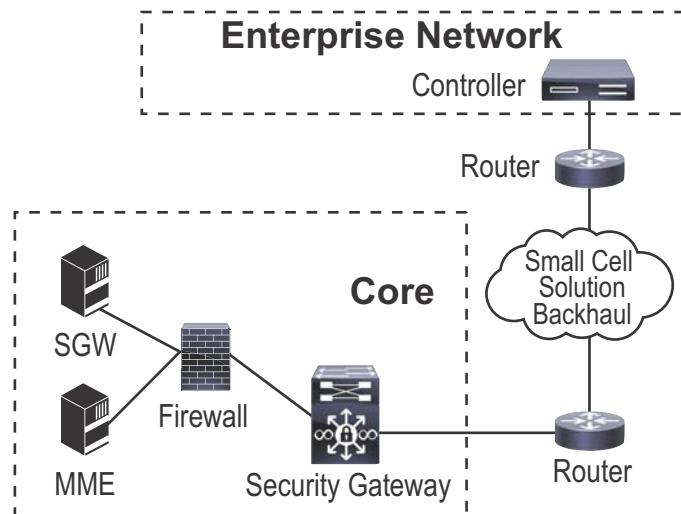
\*B: The configured port number (default 29169) of the SCTP endpoint of the controller for the Iuh gateway. This object is *FAPService.{i}.FAPControl.UMTS.Gateway.FAPGWPort* in the data model.

\*C: The port number is managed by the provider core network.

\*D: The port number is managed by the provider core network. (A commonly used port number is 2152.)

#### 4.6.3.3 LTE S1 Firewall Considerations

Figure 20 shows the logical connection between the controller and security gateway with an S1 connection:



**Figure 20** Firewall in the Provider Core Network after the Security Gateway with an S1 Interface

If the deployment has a firewall inside the provider core network after traffic has traversed the security gateway and has been decrypted:

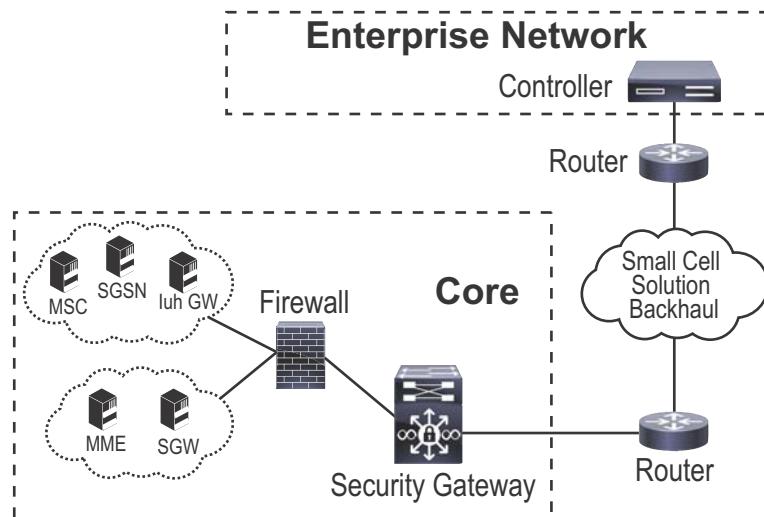
**Table 12: Required Open Firewall Ports with an S1 Interface**

Direction	Source	Destination	Protocol	Detail	Traverses
SN ↔ Core	36412	36412	SCTP	S1 control	Control plane
SN → Core	any	*A	UDP (GTP)	S1 data	User plane

\*A: The port number is managed by the provider core network.

#### 4.6.3.4 Dual-Mode Firewall Considerations

Figure 19 shows the logical connection between the controller and security gateway with a in a system supporting UMTS and LTE services:



**Figure 21** Firewall in the Provider Core Network after the Security Gateway In a Dual-Mode System

If the deployment has a firewall inside the provider core network after traffic has traversed the security gateway and has been decrypted:

**Table 13: Required Open Firewall Ports in a Dual-Mode System**

Direction	Source	Destination	Protocol	Detail	Traverses
SN ↔ Core	123	123	UDP	NTP	Management plane
SN ↔ Core	*A	*B	SCTP	Iuh	Control plane
SN → Core	any	*C	UDP (RTP)	UMTS CS domain	User plane
SN → Core	any	*D	UDP (GTP)	UMTS PS domain	User plane
SN → Core	any	162	UDP	SNMP trap	Management plane
Core → SN	any	161	UDP	SNMP query	Management plane

**Table 13: Required Open Firewall Ports in a Dual-Mode System**

Direction	Source	Destination	Protocol	Detail	Traverses
Core ↔ SN	any	22	TCP	SSH	Management plane
SN ↔ Core	36412	36412	SCTP	LTE S1 control	Control plane
SN → Core	any	*E	UDP (GTP)	LTE S1 data	User plane

Several port numbers correspond to Signaling Transport (SIGTRAN) configuration parameters that are defined in \*A and \*B below:

\*A: The configured port number (default 1024) of the SCTP endpoint of the controller for Iuh. This object is *FAPService.{i}.FAPControl.UMTS.Gateway.FAPLocalPort* in the data model.

\*B: The configured port number (default 29169) of the SCTP endpoint of the controller for the Iuh gateway. This object is *FAPService.{i}.FAPControl.UMTS.Gateway.FAPGWPort* in the data model.

\*C: The port number is managed by the provider core network.

\*D: The port number is managed by the provider core network. (A commonly used port number is 2152.)

\*E: The port number is managed by the provider core network.



# 5 UMTS Radio Access Network

This chapter contains the following sections:

- [Section 5.1, Configuring the Core UMTS Network](#) on page 77
- [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85
- [Section 5.3, Configuring Small Cells and Cells](#) on page 86
- [Section 5.4, Disabling and Enabling Cell Transmission](#) on page 91
- [Section 5.5, Configuring Multi-Operator Core Networks](#) on page 91
- [Section 5.6, Enabling Optional Features](#) on page 93

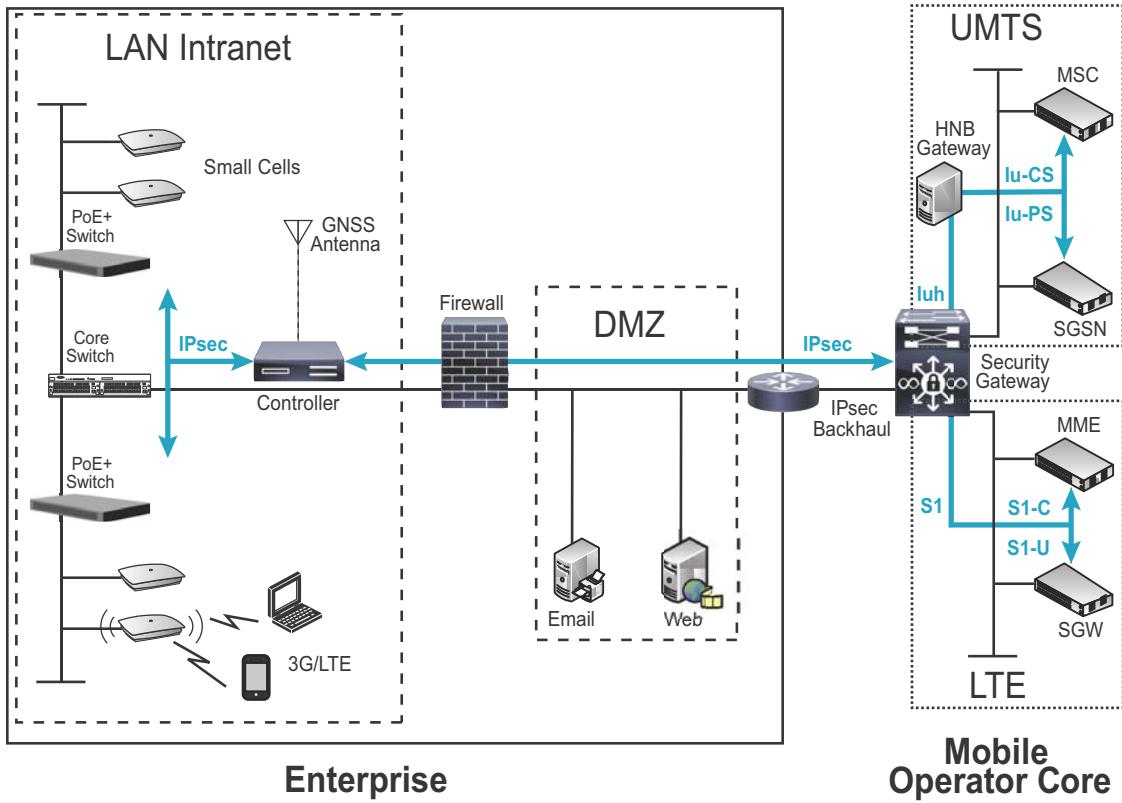
## 5.1 Configuring the Core UMTS Network

On the data plane, the controller uses the Real-time Transport Protocol (RTP) for Circuit-Switched (CS) communication (voice traffic) and the GPRS Tunnelling Protocol (GTP) for Packet-Switched (PS) communication (data traffic). On the control plane, the controller uses standard Iu/IP or Iuh protocols to communicate between the controller and the Mobile Switching Center (MSC) node and Serving GPRS Support Node (SGSN) in the provider core network.

[Figure 22](#) on page 78 provides a logical view of the Cisco small cell architecture. Refer to [Section 5.1.2.1, Configuring Core Network Iu Settings](#) on page 80 and [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85 for information about configuring network settings.

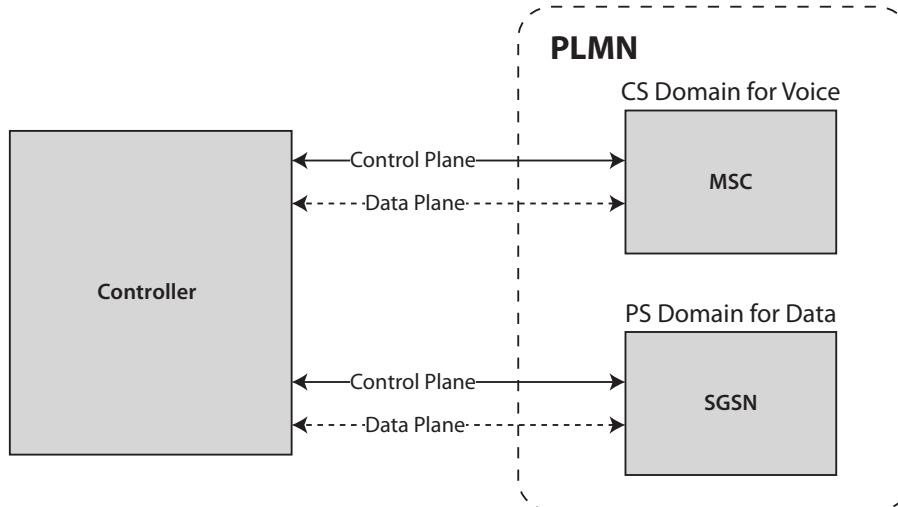
A Public Land Mobile Network (PLMN) is uniquely identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each operator providing mobile services is assigned its own PLMN. The system supports up to six PLMNs for each UMTS and LTE service.

Each user device has a unique International Mobile Subscriber Identity (IMSI) that identifies the administrator's core network. It consists of a three digit Mobile Country Code (MCC), a two or three digit Mobile Network Code (MNC), and a ten digit Mobile Subscription Identification Number (MSIN).



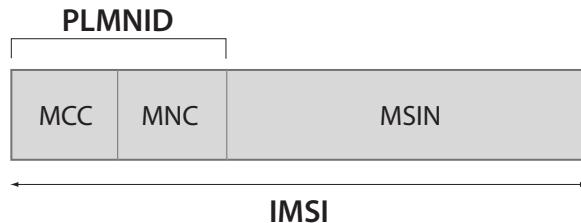
**Figure 22** Small Cell Solution Logical Architecture

[Figure 23](#) illustrates communications between the controller and the provider core network.



**Figure 23** Communications Between the USC 8088 Controller and the Provider Core Network

The MCC and MNC are predefined within a UTRAN. [Figure 24](#) shows the relationship of the PLMNID components.



**Figure 24** IMSI Components

### 5.1.1 Deleting the Existing Configuration

The Radio Access Network (RAN) is the equipment and related services that manage voice and data traffic between the provider core network and the mobile user. The network implements a RAN in an enterprise environment. Before configuring the core network and RAN, delete any existing RAN configuration to avoid configuration errors and start with a fresh RAN configuration.

To delete the RAN configuration:

**Step 1** From the Configuration Mode, issue the following commands to delete the RAN configuration:

```
delete FAPService
delete RadioNode
delete Cell
```

**Step 2** Issue the **show FAPService** command to verify the configuration:

```
show FAPService
No entries found.
```

### 5.1.2 Configuring UMTS Core Network Settings

The Signaling Transport (SIGTRAN) is an IP-based series of protocols used to configure voice and data traffic to the provider core network. You must define the following SIGTRAN parameters for UMTS service:

**Table 14: SIGTRAN Parameters**

Parameter	Description
CNIPAddress	IP address of SCTP endpoint of core device
CNIPPort	Port number of SCTP endpoint of core device
CNM3UANA	M3UA Network Appearance of core device
CNM3UANAIncluded	Whether M3UA Network Appearance should be included in messages to peer
DPC	SCCP Destination Point Code
M3UARoutingContext	M3UA Routing Context Value
OPC	SCCP Originating Point Code
RNCIPPort	Port number of SCTP endpoint of FAP
RNCM3UAASPID	M3UA Application Server Process Identifier
RNCM3UAPSPType	Type of M3UA Peer Server Process



**Note** Cells do not radiate without a connection to the core network. If an existing connection to the core network goes down, all cells are deprovisioned and stop radiating. Cells begin radiating again when the connection to the core network is reestablished.

### 5.1.2.1 Configuring Core Network Iu Settings

In this configuration, the controller connects directly to the mobile core network through an IPsec tunneled Iu/IP interface. It establishes an Iu-CS connection to the MSC and an Iu-PS connection to the SGSN. On the user plane, voice traffic is encapsulated using Real-time Transport Protocol (RTP), data traffic is encapsulated using GPRS Tunneling Protocol (GTP).

All control and user traffic between the controller and the core network is then encapsulated into a single IPsec tunnel. The controller can authenticate with, and connect directly to, existing mobile core security gateways using factory provisioned digital certificates.

#### To configure the core network Iu settings

**Step 1** From the Configuration Mode, configure the Core Network (CN) protocol to be used in the SIGTRAN. Here, the protocol specified is *Iu/IP*.

```
set FAPService 1 FAPControl UMTS Gateway CNProtocol Iu/IP
```

**Step 2** Specify the PLMN type, PLMNID, the Location Area Code, Routing Area Code (LACRAC), and Service Area Code (SAC) values. Refer to TR-196 for information about LACRAC formatting. Refer to 3GPP-TS.23.003 for information about SAC formatting.

```
set FAPService 1 CellConfig UMTS CN PLMNTYPE GSM-MAP PLMNID 00103 LACRAC
[ 4660:86 ] SAC 122
```

**Step 3** Issue the **show FAPService <ServiceNumber> CellConfig UMTS CN** command in to verify the security gateway and the CN protocol configurations:

```
show FAPService 1 CellConfig UMTS CN
PLMNTYPE GSM-MAP;
PLMNID 00103;
SAC 122;
LACRAC "[ 4660:86 ]";
```

**Step 4** Configure the SIGTRAN protocol parameters for the circuit-switched domain:

```
set FAPService 1 Transport SIGTRAN CSDomain CNIPAddress 10.20.10.5 CNIPPort 1705 RNCIPPort
1024 RNCM3UAPSPType IPSP RNCM3UAASPID 0 M3UARoutingContext 47 CNM3UANA 2 CNM3UANAIIncluded
true OPC 100 DPC 200
```

**Step 5** Configure the SIGTRAN protocol parameters for the packet-switched domain:

```
set FAPService 1 Transport SIGTRAN PSDomain CNIPAddress 10.20.10.8 CNIPPort 1702 RNCIPPort
1024 RNCM3UAPSPType IPSP RNCM3UAASPID 0 M3UARoutingContext 48 CNM3UANA 4 CNM3UANAIIncluded
true OPC 100 DPC 250
```

**Step 6** Issue the **show FAPService <ServiceNumber> Transport SIGTRAN** command to verify the SIGTRAN configuration for the circuit-switched domain and the packet-switched domain:

```
show FAPService 1 Transport SIGTRAN
SCCPAddrType ITU;
CSDomain {
    CNIPAddress 10.20.10.5;
    CNIPPort 1705;
    RNCIPPort 1024;
    RNCM3UAPSPType IPSP;
    RNCM3UAASPID 0;
    M3UARoutingContext 47;
```

```

CNM3UANA          2;
CNM3UANAIIncluded true;
OPC              100;
DPC              200;
}
PSDomain {
    CNIPAddress      10.20.10.8;
    CNIPPort         1702;
    RNCIPPort        1024;
    RNCM3UAPSPType  IPSP;
    RNCM3UAASPID   0;
    M3UARoutingContext 48;
    CNM3UANA          4;
    CNM3UANAIIncluded true;
    OPC              100;
    DPC              250;
}

```

**Step 7** Enable the connection to the core network:

```
set FAPService 1 FAPControl UMTS Gateway CNConnectionEnable true
```

**Step 8** Issue the `show FAPService <ServiceNumber> FAPControl` command to verify the configuration:

```
show FAPService 1 FAPControl UMTS Gateway
CNConnectionEnable true;
CNProtocol       Iu/IP;
```

**Step 9** Commit the configuration:

```
commit
```

**Step 10** After a successful commit, issue the `run show Core Control` command to verify the state information for the circuit-switched and packet-switched domains:

```
run show Core Control
Protocol: Iu/IP
CSDomain (Connected):
    SCTP Peering: Local 192.168.30.128:1024 <-> Remote 10.20.10.5:1075 (Connected)
    M3UA Peering: RC 47, NA 2 (Connected:Ready)
    SCCP Peering: ITU, OPC 100 <-> DPC 200 (Connected)
PSDomain (Connected):
    SCTP Peering: Local 192.168.30.128:1024 <-> Remote 10.20.10.8:1702 (Connected)
    M3UA Peering: RC 48, NA 4 (Connected:Ready)
    SCCP Peering: ITU, OPC 100 <-> DPC 250 (Connected)
```

### 5.1.2.2 Configuring Core Network luh Settings

In this configuration, each controller connects using an IPsec tunneled luh interface to a Home NodeB (HNB) gateway. The HNB gateway aggregates multiple controllers and connects to the core network using Iu-CS and Iu-PS over IP link.

To configure the core network luh settings

**Step 1** From the Configuration Mode, specify the PLMN type, PLMNID, the Location Area Code, Routing Area Code (LACRAC), and Service Area Code (SAC) values. Refer to TR-196 for information about LACRAC formatting. Refer to 3GPP-TS.23.003 for information about SAC formatting. The SAC setting is mandatory in luh configurations.

```
set FAPService 1 CellConfig UMTS CN PLMNType GSM-MAP PLMNID 00103 LACRAC
[ 4660:86 ] SAC 122
```

**Step 2** Issue the `show FAPService <ServiceNumber> CellConfig UMTS CN` command to verify the security gateway and the CN protocol configurations:

```
show FAPService 1 CellConfig UMTS CN
```

```
PLMNType GSM-MAP;
PLMNID 00103;
SAC 122;
LACRAC "[ 4660:86 ]";
```

**Step 3** Configure the Core Network (CN) protocol to be used in the SIGTRAN. Here, the protocol specified is *Iuh*.

```
set FAPService 1 FAPControl UMTS Gateway CNProtocol Iuh
```

**Note:** The current version of the OS software supports one FAPService. Therefore <ServiceNumber> is always 1 (one) in this release.

**Step 4** Configure the IP address of the security gateway. This example uses IP address 10.1.194.29.

```
set FAPService 1 FAPControl UMTS Gateway SecGWServer1 10.1.194.29
```

**Step 5** Configure the IP address of the HNB gateway. This example uses IP address 10.3.254.4.

```
set FAPService 1 FAPControl UMTS Gateway FAPGWSERVER1 10.3.254.4
```

**Step 6** Configure the SCTP port of the HNB gateway. This example uses port 29169.

```
set FAPService 1 FAPControl UMTS Gateway FAPGWPort 29169
```

**Step 7** Configure the controller SCTP port number. This example uses port 1024.

```
set FAPService 1 FAPControl UMTS Gateway FAPLocalPort 1024
```

**Step 8** Configure the controller registration retry timer, in seconds. This example uses 1 second.

**Step 9** Enable the connection to the core network:

```
set FAPService 1 FAPControl UMTS Gateway CNConnectionEnable true
```

**Step 10** Issue the `show FAPService <ServiceNumber> FAPControl` command to verify the configuration:

```
show FAPService 1 FAPControl UMTS Gateway
SecGWServer1          10.1.194.29;
FAPGWSERVER1          10.3.254.4;
FAPGWPort              29169;
CNConnectionEnable     true;
FAPLocalPort            1024;
CNPProtocol             Iuh;
```

**Step 11 (Optional)** Issue the following command for gateways supporting 3GPP release 9 and greater, and which require the R9 extension IE of cell-access-mode in registration requests:

```
Set configuration FAPService 1 FAPControl UMTS HomeNodeB SendCellAccessMode
SendCellAccessMode true
```

**Step 12** Issue the following command to verify the configuration:

```
show configuration FAPService 1 FAPControl UMTS HomeNodeB SendCellAccessMode
SendCellAccessMode true;
```

**Step 13** Commit the configuration:

```
commit
```

**Step 14** After a successful commit, issue the `run show Core Control` command to verify the state information for the *Iuh* gateway:

```
run show Core Control
Protocol: Iuh
Iuh gateway (Connected):
    Peering: Local 192.168.30.128:1024 <-> Remote 10.20.10.5:1075 (Connected)
```

### 5.1.2.3 UMTS Cell Provisioning Timer

To prevent cell provisioning and de-provisioning during a core connection flapping due to network issues, configure a cell provisioning timer to delay the time from the instance core network connection is established to when the system provisions the cells. The timer sets the provisioning delay in seconds from 0 through 300, with the default of 0.

To create a cell provisioning timer

**Step 1** From the Configuration Mode, issue the `set FAPService <ServiceNumber> FAPControl UMTS Gateway CNConnectionHoldDownTime` command to create a cell provisioning timer. This example sets the timer for 20 seconds.

```
set FAPService 1 FAPControl UMTS Gateway CNConnectionHoldDownTime 20
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS Gateway CNConnectionHoldDownTime  
CNConnectionHoldDownTime 20;
```

### 5.1.3 Configuring Home NodeB Gateway Redundancy

The eRMS system supports an intra- and inter-HNB gateway redundant architecture to provide failover in the event of two types of HNB gateway failure:

- **Intra-gateway failure:** In a gateway chassis with multiple HNB gateway line cards, when the active blade fails, all registered controllers failover to the standby blade.
- **Inter-gateway failure:** In topologies with geographic redundancy where two security gateways and their HNB gateways are in different locations, failure of the first HNB gateway, all controller traffic fails over to the secondary security gateway and its HNB gateway.

Figure 25 shows the logical architecture of the HNB gateway redundancy feature:

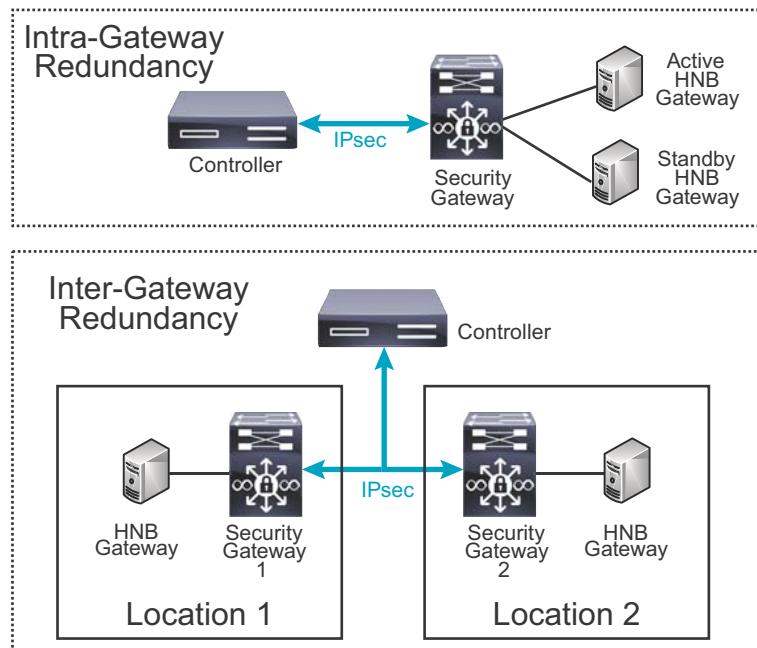


Figure 25 NodeB Gateway Redundancy Logical Architecture

Each controller supports connection to up to three security gateways, though it maintains at most one IPsec tunnel to a security gateway at one time. Each security gateway must have a separate virtual interface.

The controller supports configuring one HNB gateway IP address. If the connection to the HNB gateway fails, the DNS server behind the security gateway directs controller traffic to failover HNB gateways when configured. Controller-to-HNB gateway failures are traffic-affecting. All active sessions are dropped with a connection failure.

HNB gateways are identified by their fully qualified domain name that is provided to the controller by the security gateway. In the event of an HNB switchover, the DNS server resolves the IP address of the standby HNB gateway.

Each HNB gateway is assigned a primary and secondary LACRAC. Upon switchover the secondary LACRAC is advertised to user devices triggering a location update event.

When a controller boots, it attempts the following sequence:

- It attempts to establish an IPsec tunnel with the primary security gateway server, and then its primary HNB gateway.
- If it connects to the primary security gateway but fails to connect with the primary HNB gateway in the allotted number of tries, it attempts to connect with the secondary HNB gateway.
- If it fails to connect with the secondary HNB gateway, or fails to establish an IPsec connection to the primary security gateway, it follows the same procedure with the secondary security gateway,
- Failing all of the above, the controller repeats the procedure with the tertiary security gateway and its HNB gateways.

## To configure Home NodeB redundancy

**Step 1** From the Configuration Mode, issue the following command to configure and enable the primary security gateway. This example:

- configures and enables security gateway 1, with an IP address of 10.1.215.1
- configures the fully qualified domain name of *example.com*
- sets the core network connection retry to 10 attempts
- sets the number of times a switchover is triggered in if the core network cannot be established

```
set FAPService 1 FAPControl UMTS Gateway SecGWServer1 10.1.215.1 FAPGWSERVER1 example.com
CNConnectionEnable true CNConnectionMaxRetry 10 CNConnectionMaxSwitchover 5
```

**Step 2** Issue the following command to do configure and enable the secondary security gateway. This example:

- configures and enables security gateway 1, with an IP address of 10.2.215.1
- sets the core network connection retry to 10 attempts
- sets the number of times a switchover is triggered in if the core network cannot be established

```
set FAPService 1 FAPControl UMTS Gateway SecGWServer2 10.2.215.1 CNConnectionEnable true
CNConnectionMaxRetry 10 CNConnectionMaxSwitchover 5
```

**Step 3** Issue the following command to verify the configuration

```
show FAPService 1 FAPControl UMTS Gateway
SecGWServer1          10.1.215.1;
SecGWServer2          10.2.215.1;
FAPGWSERVER1          example.com;
FAPGWPort              29169;
CNConnectionEnable     true;
CNConnectionMaxRetry   10;
CNConnectionMaxSwitchover 5;
```

**Step 4** Issue the following command to configure and enable the primary security gateway virtual interface:

```
set FAPService 1 Transport Tunnel VirtualInterface 1 Enable true SecGWServerIndex 1
```

**Step 5** Issue the following command to configure and enable the secondary security gateway virtual interface:

```
set FAPService 1 Transport Tunnel VirtualInterface 2 Enable true SecGWServerIndex 2
```

**Step 6** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface
VirtualInterface 1 {
    Enable                      true;
    SecGWServerIndex            1;
}
VirtualInterface 2 {
    Enable                      true;
    SecGWServerIndex            2;
}
```

**Step 7** Issue the following command to set the primary and secondary LACRAC for the Iuh gateway. This example sets

```
set FAPService 1 CellConfig UMTS CN LACRAC [ 1252:52 1253.53 ]
```

**Step 8** Issue the following command to verify the configuration

```
show FAPService 1 CellConfig UMTS CN LACRAC
LACRAC "[ 1252:52 1253.53 ]";
```

## 5.2 Configuring UMTS Femto Access Point Service

Femto Access Point (FAP) Service is an instance of a Broadband Forum TR-196 object, and associated Cisco extensions. It contains configuration, operational state, and performance counters pertaining to the small cell solution. The FAPService object includes information about the following:

- core network connection configuration and operational state
- options for auto provisioning and self configuration of small cells and cells
- access policies
- system configuration, operational state, and performance monitoring statistics

You must specify the following mandatory parameters to create a FAPService:

- Radio Frequency (RF) and RAN Settings
- UTRA Absolute Radio Frequency Channel Number (UARFCN)
- maximum transmission power (MaxFAPTxPower) in units of 0.1 dBm
- Radio Network Controller ID (RNCID) of the controller

To configure UMTS FAP service

**Step 1** From the Configuration Mode, configure the channel number and maximum power settings. In this example, the frequency channel number is 1937 and the maximum transmission power rate range is from -100 through 200 (in units of 0.1 dBm). Extended coverage small cells have a maximum transmission power rate range from -100 through 240 (in units of 0.1 dBm).

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF UARFCNDL [ 1937 ] MaxFAPTxPower -100..100
```

**Step 2** For Iu/IP configurations, set the RNCID of the controller. In this example, the ID is 1000.

```
set FAPService 1 CellConfig UMTS RAN RNCID 1000
```

**Step 3** Issue the **show FAPService <ServiceNumber> CellConfig UMTS RAN** command to display the RAN configuration:

```
show FAPService 1 CellConfig UMTS RAN
```

```
RNCID          1000;
FDDFAP {
    RF {
        UARFCNDL      "[ 1937 ]";
        MaxFAPTxPower -100..100;
    }
}
```

**Step 4** Enable the network to serve UMTS traffic:

```
set FAPService 1 FAPControl AdminState true UMTS AdminState true
```

**Step 5** Issue the `show FAPService <ServiceNumber> FAPControl AdminState` command to verify the configuration:

```
show FAPService 1 FAPControl AdminState
AdminState true;
UMTS {
    AdminState true;
}
```

## 5.3 Configuring Small Cells and Cells

Configuring small cells requires setting parameters such as the Media Access Control (MAC) address and the UMTS transmission band. Configuring cells requires setting parameters such as the channel number, maximum transmit power, the cell operational mode, and primary scrambling code. Small cells and cells can be configured automatically with a feature called auto provisioning, or they can be configured manually.

Active UMTS cells can be in one of three operational modes:

- **GSMNetmon:** GSM scan mode
- **UMTSNetmon:** UMTS scan mode
- **UMTSNodeB:** operational mode

Cells in *GSMNetmon* or *UMTSNetmon* mode do not transmit power.

### 5.3.1 Adding Small Cells and Cells with Auto Provisioning

After an unprovisioned small cell completes the small cell boot sequence, configure auto provisioning to enable the controller to automatically configure the small cell, radio, and the associated cell with default parameters. This enables the system to become operational with minimal end-user input.

Auto provisioning:

- creates small cells, radios, and logical cell objects
- binds each logical cell object to a physical radio inside a small cell

Cells can be set to power up in one of three operational modes during auto provisioning:

- When a cell boots up in *UMTSNodeB* mode, it scans for GSM and UMTS neighbor cells and begins transmitting.
- When a cell boots up in *GSMNetmon* or *UMTSNetmon* mode, it monitors for neighbor cells but does not transmit radio signals.

First verify the operating states of small cells in the network. Then configure auto provisioning.



Auto provisioning by itself does not configure the cells using any knowledge of the RF environment.

#### Note



The provisioning instructions assume that small cell devices are mounted and powered on in the wireless environment. Additionally, the UARFCN must be configured before auto provisioning can be enabled. Refer to [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85.

#### Note

To display the state of the small cells before provisioning

**Step 1** From the Operational Mode, issue the **show RadioNode** command to display their operating state. Note their unprovisioned state in the output below:

```
show RadioNode
RN      Name          Enable   EthernetID           IPAddress        OperState
-----  -----
1001    RN1001-B001-F001  false    00:00:00:aa:aa:cc  10.1.214.101  OOS-UNPROVISIONED
1002    RN1002-B001-F001  false    00:00:00:aa:aa:bb  10.1.214.102  OOS-UNPROVISIONED
```

The *OperState* field shows that the small cells are unprovisioned.

To configure auto provisioning

**Step 1** (Optional) From the Configuration Mode, configure the set of local cell identifier values for auto provisioning. This is the set of 16 bit local cell identifiers allocated by the service provider for cells in the network. This example sets local cell identifiers 23100 through 23110 and 23200 through 23210.

```
set FAPService 1 CellConfig UMTS RAN AutoProvCIDList [ 23100..23110 23200..
23210 ]
```

Note that if *AutoProvCIDList* is empty, auto provisioning will select local cell identifiers starting from 1.

**Step 2** From the Configuration Mode, configure the set of primary scrambling codes for the network. Valid options are 0 through 511. This example uses primary scrambling codes 100 through 120 and 200 through 220.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCode
[ 100..120 200..220 ]
```

**Step 3** Issue the following command to set the initial cell operational mode. This example sets the cell to the *UMTSNodeB* transmitting mode.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF InitialMode UMTSNodeB
```

**Step 4** Configure the range of maximum cell transmit power for cells in the network. Auto provisioning will assign cells the smallest value in this range. The valid and default ranges are -100 through 200. The extended coverage small cell has a valid range of 011 through 240. This example sets the range from -50 through 200. Note that values are in 0.1 dBm increments.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower -50..200
```

**Step 5** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF
PrimaryScramblingCode      "[ 100..120 200..220 ]";
MaxFAPTxPower              -50..200;
InitialMode                UMTSNodeB;
```

**Step 6** Enable auto provisioning:

```
set FAPService 1 FAPControl UMTS SelfConfig AutoProvisionEnable true
```

**Step 7** Issue the **run show RadioNode** and **run show Cell** commands to verify the configuration:

**run show RadioNode**

RN	Name	Enable	EthernetID	IPAddress	OperState
1001	RN1001-B001-F001	true	00:00:00:aa:aa:cc	10.1.214.101	OOS-INDETERMINATE
1002	RN1002-B001-F001	true	00:00:00:aa:aa:bb	10.1.214.102	OOS-INDETERMINATE

**run show RadioNode**

RN	Name	Enable	EthernetID	IPAddress	OperState
1001	RN1001-B001-F001	true	00:00:00:aa:aa:cc	10.1.214.101	OOS-INIT
1002	RN1002-B001-F001	true	00:00:00:aa:aa:bb	10.1.214.102	OOS-INIT

**run show Cell**

CellHandle	Name	RN	Radio	ModeInUse	ConfState	OperState
<hr/>						

**run show RadioNode**

RN	Name	Enable	EthernetID	IPAddress	OperState
1001	RN1001-B001-F001	true	00:00:00:aa:aa:cc	10.1.214.101	OOS-SYNCING
1002	RN1002-B001-F001	true	00:00:00:aa:aa:bb	10.1.214.102	OOS-SYNCING

**run show Cell**

CellHandle	Name	RN	Radio	ModeInUse	ConfState	OperState
<hr/>						

**run show RadioNode**

RN	Name	Enable	EthernetID	IPAddress	OperState
1001	RN1001-B001-F001	true	00:00:00:aa:aa:cc	10.1.214.101	OOS-DEGRADED
1002	RN1002-B001-F001	true	00:00:00:aa:aa:bb	10.1.214.102	OOS-DEGRADED

**run show Cell**

CellHandle	Name	RN	Radio	ModeInUse	ConfState	OperState
1	-	1	1	UMTSNodeB	CONFIGURED	IS-NETMON
2	-	2	1	UMTSNodeB	CONFIGURED	IS-NETMON

**Step 8** Issue the **show RadioNode** command to see the resulting small cell and radio configuration created by auto provisioning. In this example, Radio 1 of both RadioNode 1 and RadioNode 2 are enabled on UMTS band IV.

```
show RadioNode
RadioNode 1 {
    Enable           true;
    Radio 1 {
        Enable true;
    }
}
RadioNode 2 {
    Enable           true;
    Radio 1 {
        Enable true;
    }
}
```

**Step 9** Issue the **show Cell** command to see the resulting cell configuration created by auto provisioning. In this example, Cell 1 is provisioned to Radio 1 of RadioNode 1. Cell 2 is provisioned to Radio 1 of RadioNode 2.

```
show Cell
Cell 1 {
    Enable      true;
    RadioNode 1;
    Radio      1;
    CellConfig {
        UMTS {
            RAN {
                CellID 1;
                FDDFAP {
                    MobilityLinkReservation 3;
                    RF {
                        UARFCNDL          "[ 1937 ]";
                        PrimaryScramblingCode "[ 0 ]";
                        MaxFAPTxPower      0;
                        Mode               UMTSNodeB;
                    }
                }
            }
        }
    }
}
Cell 2 {
    Enable      true;
    RadioNode 2;
    Radio      1;
    CellConfig {
        UMTS {
            RAN {
                CellID 2;
                FDDFAP {
                    MobilityLinkReservation 3;
                    RF {
                        UARFCNDL          "[ 1937 ]";
                        PrimaryScramblingCode "[ 1 ]";
                        MaxFAPTxPower      0;
                        Mode               UMTSNodeB;
                    }
                }
            }
        }
    }
}
```

### 5.3.2 Adding a Small Cell and a Cell Manually

Manually add a cell to the network by creating a small cell then creating a cell within it. To manually create the small cell you must know the Media Access Control (MAC) address and the UMTS transmission band.

To manually create a cell, you must know the channel number, maximum transmit power, the cell operational mode, and primary scrambling code. Auto provisioning must be disabled to manually add small cells and cells.

#### To add a cell to the network manually

**Step 1** From the Configuration Mode, validate that auto provisioning is disabled:

```
show FAPService 1 FAPControl UMTS SelfConfig AutoProvisionEnable
AutoProvisionEnable false;
```

**Step 2** If the value of `AutoProvisionEnable = true`, issue the following command to disable auto provisioning:

```
set FAPService 1 FAPControl UMTS SelfConfig AutoProvisionEnable false
```

**Step 3** Enter the `set RadioNode <Number>` command to create the small cell in the system. This example creates small cell 55 with a MAC address of `00:24:48:00:00:3e` transmitting on UMTS band IV.

```
set RadioNode 55 Enable true EthernetID 00:27:48:00:00:3e Radio 1 Band umts-band-IV Enable true
```

**Step 4** Issue the `show RadioNode` command to verify the configuration:

```
show RadioNode
RadioNode 55 {
    Enable           true;
    EthernetID      00:27:48:00:00:3e;
    Radio 1 {
        Enable true;
        Band   umts-band-IV;
    }
}
```

**Step 5** Enter the `set Cell <Number>` command to create the cell in the small cell. This example creates cell 55 on radio 1 of small cell 55, names it *Kitchen*, and gives it the description *Cell\_55*. It uses channel 1937, with a maximum transmit power of 0.9 dBm (in units of 0.1), primary scrambling code 222, in the operational mode (*UMTSNodeB*).

```
set Cell 55 Description Kitchen Name Cell_55 Enable true Radio 1 RadioNode 55 CellConfig
UMTS RAN FDDFAP RF UARFCNDL [ 1937 ] MaxFAPTxPower 90 UseSelfConfigAlternatePSC false
PrimaryScramblingCode [ 222 ] Mode UMTSNodeB
```

**Step 6** Issue the `show Cell` command to verify the configuration:

```
show Cell
Cell 55 {
    Enable     true;
    Name       Cell_55;
    Description Kitchen;
    RadioNode 55;
    Radio     1;
    CellConfig {
        UMTS {
            RAN {
                CellID 55;
                FDDFAP {
                    RF {
                        UARFCNDL          "[ 1937 ]";
                        PrimaryScramblingCode "[ 222 ]";
                        MaxFAPTxPower      90;
                        UseSelfConfigAlternatePSC false;
                        Mode               UMTSNodeB;
                    }
                }
            }
        }
    }
}
```

### 5.3.3 Deleting a Small Cell and a Cell

To delete a small cell, delete the cell and small cell from the configuration.

### To delete a cell and small cell

**Step 1** From the Configuration Mode, issue the `delete Cell <Number>` command to delete the cell from the network. This example deletes cell 66.

```
delete Cell 66
```

**Step 2** Issue the `show Cell <Number>` command to verify the configuration:

```
show cell 66
-----^
syntax error: unknown element
```

**Step 3** Issue the `delete RadioNode <Number>` command to delete the small cell. This example deletes small cell 66.

```
delete RadioNode 66
```

**Step 4** Issue the `show RadioNode <Number>` command to verify the configuration

```
show RadioNode 66
-----^
syntax error: unknown element
[error] [2011-08-30 17:59:36]
```

## 5.4 Disabling and Enabling Cell Transmission

It is often useful to temporarily disable all cell transmission in the system for administrative or diagnostic purposes. Issue the `request umts cell disable all` command to remove all cells from service. Issue the `request umts cell enable all` command to restart transmission on all cells in the system.

### To disable all cell transmission

**Step 1** From the Operational Mode, issue the `request umts cell disable all` command to disable all cell transmission:

```
request umts cell disable all
status OK
```

### To enable cell transmission on all cells

**Step 1** From the Operational Mode, issue the `request umts cell enable all` command to re-enable transmission on all cells in the system:

```
request umts cell enable all
status OK
```

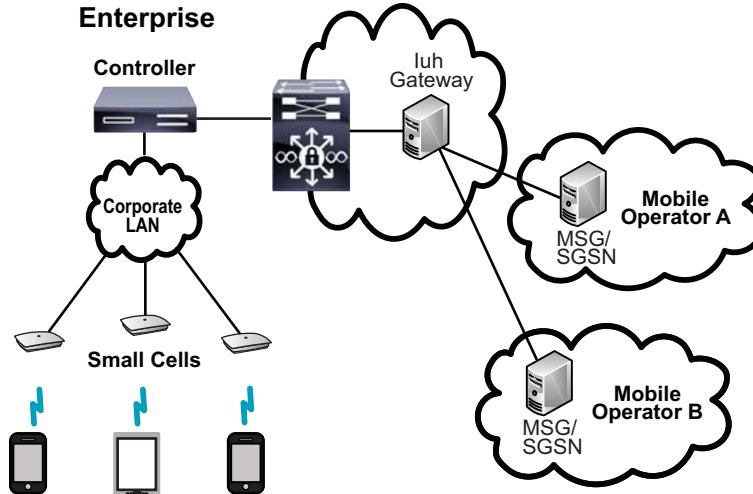
## 5.5 Configuring Multi-Operator Core Networks

The Cisco small cell solution supports the equipment sharing with multiple mobile providers. Each small cell solution can support up to five mobile providers operating on the same UMTS frequency band. All cells in the small cell solution operate with a single configuration that is shared by all mobile providers. The cells broadcast all the PLMN IDs corresponding to the mobile providers sharing the network to user devices.

User devices that support multiple core networks identify each core network independently. Devices that do not support this feature ignore the network-sharing signaling.

Multi-operator core networks must share a common Iuh gateway which can be maintained by one mobile provider, jointly maintained between two or more providers, or maintained by a third party. The Iuh gateway routes traffic to the

proper core network. Figure 26 shows the logical architecture of a multi-core network:



**Figure 26** Multi-Operator Network Logical Architecture

### To configure a multi-operator core network

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> CellConfig UMTS CN** command to configure the basic parameters of the core network. In this example:

- the PLMN type is GSM-MAP
- the PLMN ID is 00101
- the LACRAC is 73:73
- the core network ID is 0
- the common PLMN ID is part of the multiple PLMN list
- the circuit-switched domain periodic location update is 3600 seconds (one hour)
- the IMSI attach and detach procedure is enabled

```
set FAPService 1 CellConfig UMTS CN PLMNTYPE GSM-MAP PLMNID 00101 CNID 0 LACRAC [ 73:73 ]
] CommonPLMNIDInMultiplePLMNLIST true CSDomain T3212 3600 IMSIAttachDetachEnable true
```

**Step 2** Issue the following command to add the second mobile provider. This example adds PLMN ID 11122, bars access classes 1 and 2 from circuit-switched traffic and 3 and 4 from packet-switched traffic.

```
set FAPService 1 CellConfig UMTS CN MultiplePLMNsList 1 PLMNID 11122
AccessClassBarredListCS [ 1 2 ] AccessClassBarredListPS [ 3 4 ]
```

**Step 3** Issue the following commands to add the additional mobile providers. This example adds PLMN IDs 11133, 11144, and 11155.

```
set FAPService 1 CellConfig UMTS CN MultiplePLMNsList 2 PLMNID 11133
set FAPService 1 CellConfig UMTS CN MultiplePLMNsList 3 PLMNID 11144
set FAPService 1 CellConfig UMTS CN MultiplePLMNsList 3 PLMNID 11155
```

**Step 4** Issue the **show FAPService <ServiceNumber> CellConfig UMTS CN** command to validate the configuration:

```
show FAPService 1 CellConfig UMTS CN
PLMNTYPE                      GSM-MAP;
PLMNID                         00101;
LACRAC                          "[ 73:73 ]";
CNID                           0;
CommonPLMNIDInMultiplePLMNLIST true;
CSDomain {
    T3212                         3600;
```

```

    IMSIAttachDetachEnable true;
}
MultiplePLMNsList 1 {
    PLMNID          11122;
    AccessClassBarredListCS "[ 1 2 ]";
    AccessClassBarredListPS "[ 3 4 ]";
}
MultiplePLMNsList 2 {
    PLMNID          11133;
}
MultiplePLMNsList 3 {
    PLMNID          11155;
}

```

## 5.6 Enabling Optional Features

Cisco has a number of optional features that can be configured:

- [Section 5.6.1, Configuring High-Capacity Networks](#) on page 93
- [Section 5.6.2, Enabling Enhanced Coverage](#) on page 94
- [Section 5.6.3, Configuring Downlink Higher Order Modulation](#) on page 94

### 5.6.1 Configuring High-Capacity Networks

By default each cell supports 16 UMTS radio links. In small cell solutions requiring higher capacity traffic loads, cells can be configured to support 32 UMTS radio links. The number of radio links per cell and the associated link reservation parameters are configured globally. All cells in an small cell solution share these same properties. The number of radio links per cell can be any combination of:

- Circuit-switched R99 users
- Packet-switched R99 users (depending on Orthogonal Variable Spreading Factor code usage)
- Packet-switched high-speed downlink packet access users (3GPP Release 5)
- Packet-switched high-speed downlink packet access users (3GPP Release 6 and above)
- Multi-RAB combinations of the above (3 packet-switched RABs maximum)

As part of this configuration you can dedicate a number of radio links to mobility reservation, registration, and RACH reservation. [Table 15](#) shows the default access control settings and the recommended settings when changing from 16 to 32 radio links or back again to 16 radio links:

**Table 15: Access Control Settings**

Parameter	Default	Recommended for 16 Users	Recommended for 32 Users
Mobility link reservation	3	3	5 (range 0 through 10)
RACH link reservation	0	0	1 (range 0 through 6)
Registration link reservation	1	1	1 (range 0 through 6)

To configure a high capacity network

- Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> AccessMgmt AdmissionControl** command to configure a high-capacity network. This example uses:
- 32 radio links

- 5 mobility reservation links
- 1 RACH reservation links reservations
- 1 registration links reservations

```
set FAPService 1 AccessMgmt AdmissionControl Enable true MaxNumberOfRadioLinks 32
MobilityLinkReservation 5 RACHLinkReservation 1 RegistrationLinkReservation 1
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt AdmissionControl
Enable true;
MaxNumberOfRadioLinks 32;
MobilityLinkReservation 5;
RACHLinkReservation 1;
RegistrationLinkReservation 1;
```

## 5.6.2 Enabling Enhanced Coverage

To enable the optional extended coverage small cells, assign a higher maximum transmit power setting of up to 24 dBm to the system. This is a global attribute, assigned per small cell solution. Since the system supports a mixture of lower-power and enhanced coverage small cells, individual small cells can be assigned lower maximum transmit power settings as needed. This setting is the maximum power allocated. The actual power in use will still be set through the RF management code or configuration.

Upon initial system turn-up, lower-power small cells will receive a maximum transmit power setting of 20 dBm even if the system is configured for enhanced coverage. Any new lower-power small cells added to a system provisioned for extended coverage will receive a maximum transmit power setting of 20 dBm.



The system configures and reports power levels in units of 0.1 dBm.

### Note

To enable enhanced coverage small cells

**Step 1** From the Configuration Mode, issue the following command to enable enhanced maximum transmit power to all cells in the small cell solution. This example sets the maximum power assignment to the maximum rate of 24 dBm.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower -50..240
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF
MaxFAPTxPower -50..240;
```

## 5.6.3 Configuring Downlink Higher Order Modulation

3GPP Release 7 introduces the capability of higher order modulation scheme (Quadrature Amplitude Modulation (64-QAM)) on the shared HS-PDSCH, the downlink physical channel that carries data traffic for all HSDPA users. The 64-QAM scheme provides more information in each bit to increase the efficiency of the signal. With the introduction of 64-QAM on the HS-PDSCH, the base stations can support up to 21 Mbps on the downlink.

In order to realize 21 Mbps on the downlink, the system implements the mac-ehs subsystem within the high speed-schedulers on the small cell. This improves the airlink efficiency by reducing the amount of padding contained in the transport blocks. It also moves the Radio Link Control (RLC) packet segmentation function from the controller to the

small cell, reducing the controller load of segmentation and packet processing. This 3GPP feature is called the flexible RLC solution, where the downlink RLC block size is flexible, and can be as large as the IP packet, typically 1500 bytes.

The small cells support 64-QAM and up to 21 Mbps on the downlink for devices that support 64-QAM and have a Release 7 HSDPA category 13, 14, 17, or 18. For other devices, the R6 HSDPA data rates are applied.

This feature is a software upgrade. There are no hardware changes required to support this feature.

### To configure downlink higher order modulation

**Step 1** From the Configuration Mode, issue the following command to enable 64-QAM.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP MACehsEnable true SixtyFourQAMEnable true
FlexRLCEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP
MACehsEnable          true;
SixtyFourQAMEnable    true;
FlexRLCEnable         true;
```





# 6 LTE Radio Access Network

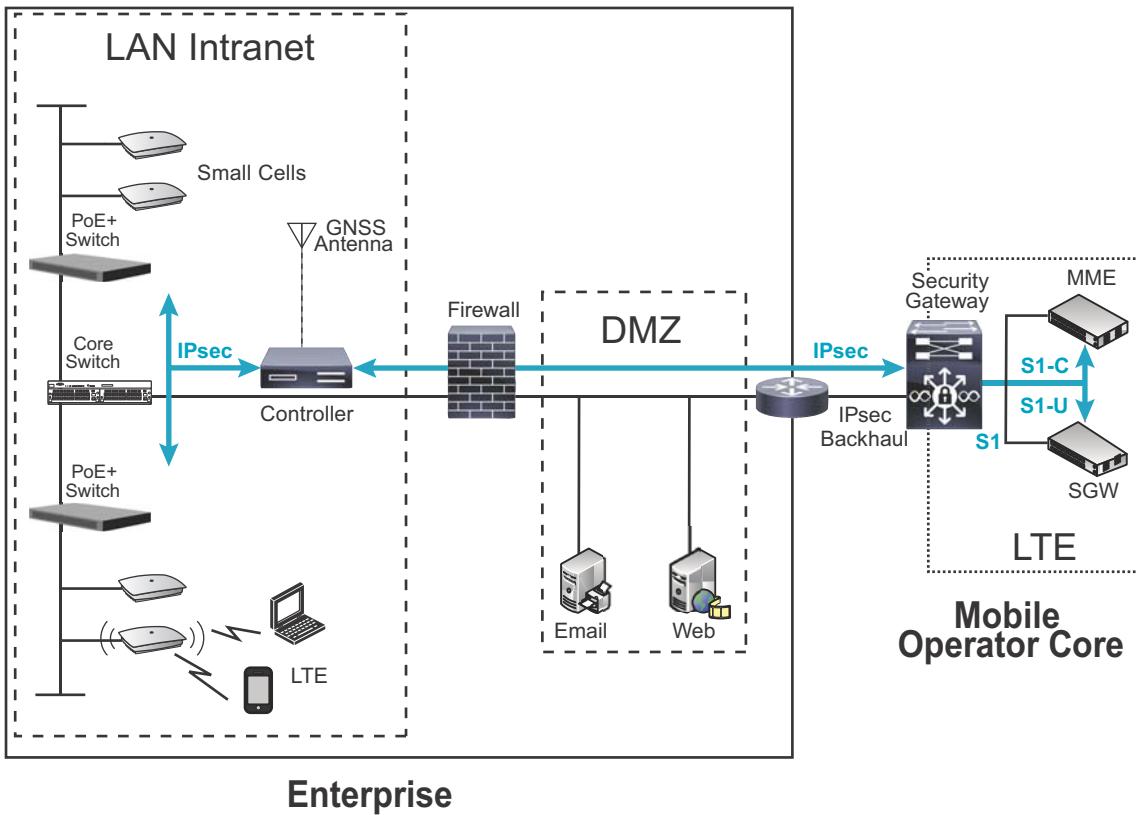
This chapter contains the following sections:

- [Section 6.1, Configuring the Core Network LTE Services](#) on page 97
- [Section 6.2, Configuring LTE Femto Access Point Service](#) on page 103
- [Section 6.3, Configuring Small Cells and Cells](#) on page 104
- [Section 6.4, Disabling and Enabling Cell Transmission](#) on page 106

## 6.1 Configuring the Core Network LTE Services

On the data plane, the controller uses the Real-time Transport Protocol (RTP) for Circuit-Switched (CS) communication (voice traffic) and the GPRS Tunnelling Protocol (GTP) for Packet-Switched (PS) communication (data traffic). On the control plane, the controller uses standard Iu/IP, Iuh, or S1 protocols to communicate between the controller and the provider core network.

Figure 27 on page 98 provides a logical view of the Cisco small cell architecture. Refer to [Section 6.1.2.1, Configuring Core Network LTE Settings](#) on page 100 and [Section 6.2, Configuring LTE Femto Access Point Service](#) on page 103 for information about configuring network settings.

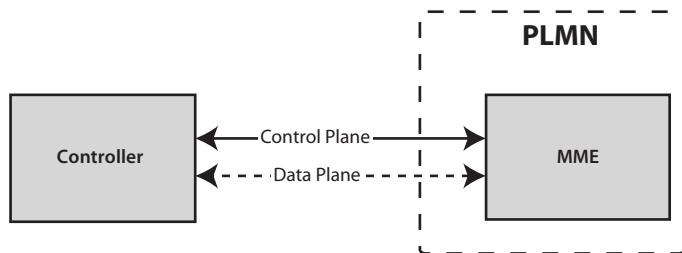


**Figure 27** Small Cell Solution Logical Architecture

A Public Land Mobile Network (PLMN) is uniquely identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each operator providing mobile services is assigned its own PLMN. The system supports up to six PLMNs for each UMTS and LTE service.

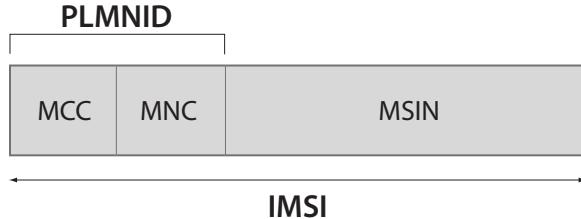
Each user device has a unique International Mobile Subscriber Identity (IMSI) that identifies the administrator's core network. It consists of a three digit Mobile Country Code (MCC), a two or three digit Mobile Network Code (MNC), and a ten digit Mobile Subscription Identification Number (MSIN).

Figure 28 illustrates communications between the controller and the provider core network.



**Figure 28** Communications Between the USC 8088 Controller and the Provider Core Network

The MCC and MNC are predefined within a UTRAN. [Figure 29](#) shows the relationship of the PLMNID components.



**Figure 29** IMSI Components

### 6.1.1 Deleting the Existing Configuration

The Radio Access Network (RAN) is the equipment and related services that manage voice and data traffic between the provider core network and the mobile user. The network implements a RAN in an enterprise environment. Before configuring the core network and RAN, delete any existing RAN configuration to avoid configuration errors and start with a fresh RAN configuration.

To delete the RAN configuration:

**Step 1** From the Configuration Mode, issue the following commands to delete the RAN configuration:

```
delete FAPService
delete RadioNode
delete Cell
```

**Step 2** Issue the **show FAPService** command to verify the configuration:

```
show FAPService
No entries found.
```

### 6.1.2 Configuring Core Network Settings

The S1 interface connects the controller to the serving gateway and Mobility Management Entity (MME) to provide voice and data traffic to the provider Evolved Packet Core (EPC) network. The S1 interface uses the S1 Application Protocol (S1AP) signaling protocol. You must define the following S1 parameters to configure the connection from the controller and the LTE core network:

**Table 16: S1 Serving Parameters**

Parameter	Description
S1ConnectionEnable	Enables or disables the S1 connection to the EPC gateway.
S1ConnectionHoldDownTime	The time, in seconds, that the cell provisioning is delayed from the instance that the first EPC S1-AP connection is established.
S1ConnectionMode	The number of connections between the controller and the EPC gateway. Selecting all enables S1 flex for network redundancy.
S1SigLinkLocalPort	The port number of the local endpoint for establishing SCTP connection with EPC gateway.
S1SigLinkServer	S1-AP remote signaling server endpoints. Supports up to eight S1SigLinkServers.



**Note** Cells do not radiate without a connection to the core network. If an existing connection to the core network goes down, all cells are deprovisioned and stop radiating. Cells begin radiating again when the connection to the core network is reestablished.

### 6.1.2.1 Configuring Core Network LTE Settings

In this configuration, the controller connects directly to the mobile core network through an IPsec tunneled S1 interface. It establishes an S1 connection to the MME that transports all LTE traffic.

All control and user traffic between the controller and the core network is then encapsulated into a single IPsec tunnel. The controller can authenticate with, and connect directly to, existing mobile core security gateways using factory provisioned digital certificates.

#### To configure the core network LTE settings

**Step 1** From the Configuration Mode, configure the parameters for the controller S1 connection to the core network for LTE services. This example:

- sets the S1 connection mode to *all* for server redundancy
- enables the connection
- sets the controller port of the STCP connection with the EPS server to 1025
- provisions and enables the connection of the S1 signal from the controller to a core network *MME* and assigns it IP address 192.168.1.2 port 36412.

```
set FAPService 1 FAPControl LTE Gateway S1ConnectionMode All S1ConnectionEnable true
S1SigLinkLocalPort 1025 S1SigLinkServer 1 Enable true Address 192.168.1.2 Port 36412 Type
MME
```

**Step 2** Issue the following commands to configure the security gateway servers. This example configures two servers with the IP addresses 172.15.1.1 and 172.15.1.2.

```
set FAPService 1 FAPControl LTE Gateway SecGWServer1 172.15.1.1
set FAPService 1 FAPControl LTE Gateway SecGWServer2 172.15.1.2
```

**Step 3** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE Gateway
SecGWServer1          172.15.1.1;
SecGWServer2          172.15.1.2;
S1ConnectionMode      All;
S1ConnectionEnable    true;
S1SigLinkLocalPort    1025;
S1SigLinkServer 1 {
    Enable   true;
    Address  192.168.1.2;
    Port     36412;
    Type     MME;
}
```

**Step 4** Issue the following command to set the Tracking Area Code (TAC) for LTE FAP of the Evolved Packet Core (EPC), to set the PLMN ID, and enable it. This example sets:

- the TAC to 1
- the PLMN EPC identity number to 1
- sets this as the primary PLMN ID
- sets the PLMN ID to 00102

```
set FAPService 1 CellConfig LTE EPC TAC 1 PLMNList 1 IsPrimary true PLMNID 00102 Enable
true
```

**Step 5** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE EPC
TAC          1;
PLMNList 1 {
    Enable           true;
    IsPrimary        true;
    PLMNID          00102;
}
```

**Step 6** Commit the configuration:

```
commit
```

**Step 7** After a successful commit, issue the **run show Core Control** command to verify the state information for the circuit-switched and packet-switched domains:

```
run show Core Control
Protocol: Iu/IP
CSDomain (Connected):
    SCTP Peering: Local 192.168.30.128:1024 <-> Remote 10.20.10.5:1075 (Connected)
    M3UA Peering: RC 47, NA 2 (Connected:Ready)
    SCCP Peering: ITU, OPC 100 <-> DPC 200 (Connected)
PSDomain (Connected):
    SCTP Peering: Local 192.168.30.128:1024 <-> Remote 10.20.10.8:1702 (Connected)
    M3UA Peering: RC 48, NA 4 (Connected:Ready)
    SCCP Peering: ITU, OPC 100 <-> DPC 250 (Connected)
```

### 6.1.2.2 LTE Cell Provisioning Timer

To prevent LTE cell provisioning and de-provisioning during a core connection flapping due to network issues, configure a cell provisioning timer to delay the time from the instance core network connection is established to when the system provisions the cells. The timer sets the provisioning delay in seconds from 0 through 300, with the default of 0.

To create a cell provisioning timer

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl LTE Gateway S1ConnectionHoldDownTime** command to create a cell provisioning timer. This example sets the timer for 20 seconds.

```
set FAPService 1 FAPControl LTE Gateway S1ConnectionHoldDownTime 20
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE Gateway S1ConnectionHoldDownTime
S1ConnectionHoldDownTime 20;
```

### 6.1.3 Configuring LTE S1 Load Redundancy and Load Balancing

The controller LTE system supports an S1 connection to up to eight S1AP endpoints for redundancy and load balancing in the EPC.

To configure LTE S1 load balancing and redundancy

**Step 1** From the Configuration Mode, issue the following commands to configure and enable the S1 signaling link servers. This example configures MME three servers:

- with IP addresses 192.167.1.1, 192.167.1.2, and 192.167.1.3
- on port 36412

```
set FAPService 1 FAPControl LTE Gateway S1SigLinkServer 1 Enable true Address 192.167.1.1
Port 36412 Type MME
```

```
set FAPService 1 FAPControl LTE Gateway S1SigLinkServer 2 Enable true Address 192.167.1.2
Port 36412 Type MME
```

```
set FAPService 1 FAPControl LTE Gateway S1SigLinkServer 3 Enable true Address 192.167.1.3
Port 36412 Type MME
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE Gateway S1SigLinkServer
S1SigLinkServer 1 {
    Enable true;
    Address 192.167.1.1;
    Port 36412;
    Type MME;
}
S1SigLinkServer 2 {
    Enable true;
    Address 192.167.1.2;
    Port 36412;
    Type MME;
}
S1SigLinkServer 3 {
    Enable true;
    Address 192.167.1.3;
    Port 36412;
    Type MME;
```

## 6.1.4 Enabling Dual-Band LTE Idle-Mode UE Load Balancing

Operators deploying dual-band LTE small cell have the option of distributing users between the two LTE bands. Distributing users across two channels doubles the small cell capacity and reduces the probability of congestion per channel, thereby enabling higher average user throughput and better call setup performance. In this software release, there are two options to distribute users across bands in idle mode:

- SIB-5 based band-class prioritization
- RRCCconnectionRelease user redirection

### SIB-5 based band class prioritization

In scenarios with a disproportionately large number of UEs that support only a single band (such as Band A), and a smaller proportion that supports dual band (such as Band A and Band B), a disproportional number of UEs will reside on Band A because such UEs are not capable of being served by an alternative band.

All dual band capable UEs can be forced to reselect the alternate Band B by setting higher reselection priority for Band B in System Information Block (SIB)-5. SIB-5 provides cell reselection information for inter-frequency EUTRAN cells and enables a band to have a higher priority for reselection than an alternative band. This will ensure that all UEs that are capable of being served by the alternative Band B, will idle and subsequently originate on that band.

### RRCCconnectionRelease user redirection

In scenarios where the operator has even distribution of dual band capable UEs (such as Band A and Band B), this feature aims to evenly distribute idle mode UEs across the two operating bands, which on average ensures even access originations and call setups across the operating bands.

Distribution of dual mode UEs across the two operating bands can be achieved by using the *idleModeMobilityControlInfo* attribute of the RRCCconnectionRelease message. This attribute provides each UE a dedicated cell reselection priority at the end of each RRC connection, including the connection for TAC update upon entering the small cell solution. By setting priority of one band to be higher than the alternative band for 50% of the UEs and the other band for the remaining 50% will on average allow an even distribution of idle mode UEs across the two operating bands.

The least significant digit of a statistically random IMSI is used as a key to distribute UEs across the two bands. All even numbered IMSIs will idle on one band, while all odd numbered IMSI will reside on the other band.

To enable dual-band LTE idle-mode UE load balancing

**Step 1** From the Configuration Mode, issue the following command to enable dual-band LTE idle-mode UE load balancing:

```
set FAPService 1 CellConfig LTE RAN Mobility IdleMode InterFreq ColocatedForceRedirect true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN Mobility IdleMode InterFreqColocatedForceRedirect ColocatedForceRedirect true;
```

## 6.2 Configuring LTE Femto Access Point Service

Femto Access Point (FAP) Service is an instance of a Broadband Forum TR-196 object, and associated Cisco extensions. It contains configuration, operational state, and performance counters pertaining to the system. The FAPService object includes information about the following:

- core network connection configuration and operational state
- access policies
- system configuration, operational state, and performance monitoring statistics
- channel bandwidth

You must specify the following mandatory parameters to create a FAPService:

- type of controller
- E-UTRA absolute radio frequency channel number in both the downlink and uplink directions

You can optionally set the downlink and uplink channel bandwidth by specifying the bandwidth in Resource Blocks (RBs). Uplink and downlink bandwidths must be identical. [Table 17](#) shows the mapping between resource blocks and frequency.

**Table 17: Resource Block to Frequency Mapping**

Resource Block #	MHz
6	1.4
15	3
25	5
50	10
75	15
100	20

To configure LTE FAP service

**Step 1** Issue the following command set the type of the controller. In this example, the controller is an eNodeB.

```
set FAPService 1 CellConfig LTE RAN Common eNodeBID
```

**Step 2** From the Configuration Mode, configure the channel number and channel bandwidth. In this example:

- the E-UTRA absolute radio frequency channel number is 3100 in the downlink direction
- the E-UTRA absolute radio frequency channel number is 21100 in the uplink direction

- the downlink bandwidth is 100 resource blocks (20 MHz)
- the uplink bandwidth is 100 resource blocks (20 MHz)

```
set FAPService 1 CellConfig LTE RAN RF EARFCNDL 3100 EARFCNUL 21100 DLBandwidth 100
ULBandwidth 100
```

**Step 3** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN
Common {
    eNodeBID 0;
}
RF {
    EARFCNDL      3100;
    EARFCNUL      21100;
    DLBandwidth    100;
    ULBandwidth    100;
```

**Step 4** Enable the network to serve LTE traffic:

```
set FAPService 1 FAPControl AdminState true LTE AdminState true
```

**Step 5** Issue the `show FAPService <ServiceNumber> FAPControl AdminState` command to verify the configuration:

```
show FAPService 1 FAPControl AdminState
AdminState true;
LTE {
    AdminState true;
}
```

## 6.3 Configuring Small Cells and Cells

Configuring small cells requires setting parameters such as the Media Access Control (MAC) address and the LTE transmission band. Configuring cells requires setting parameters such as the band number, the cell operational mode, PLMN parameters and TAC. Small cells and cells can be configured manually.

Active LTE cells can be in one of two operational modes:

- LTENetmon:** UMTS scan mode
- LTENodeB:** operational mode

Cells in *LTENetmon* mode do not transmit power.

### 6.3.1 Adding a Small Cell and a Cell Manually

Manually add an LTE cell to the network by creating a small cell then creating a cell within it. To manually create the small cell you must know the Media Access Control (MAC) address and the UMTS transmission band.

To manually create a cell, you must know the channel number, maximum transmit power, the cell operational mode, and primary scrambling code. Auto provisioning must be disabled to manually add small cells and cells.

To add a cell to the network manually

**Step 1** Enter the `set RadioNode <Number>` command to create the small cell in the system. This example creates small cell 55 with a MAC address of 00:24:48:00:00:3e transmitting on LTE band /IV.

```
set RadioNode 55 Enable true EthernetID 00:27:48:00:00:3e Radio 1 Band lte-band-IV Enable
true
```

**Step 2** Issue the `show RadioNode` command to verify the configuration:

```
show RadioNode
```

```
RadioNode 55 {
    Enable           true;
    EthernetID      00:27:48:00:00:3e;
    Radio 1 {
        Enable true;
        Band   lte-band-IV;
    }
}
```

**Step 3** Enter the `set LTECell <Number>` command to create and enable the cell in the small cell. This example creates and enables:

- cell 55 on radio 1 of small cell 55
- names it *Kitchen*
- gives it the description *Cell55*
- gives it the cell ID of 55

```
set LTECell 55 Enable true Description Kitchen Name Cell155 Radio 1 RadioNode 55 CellConfig
LTE RAN Common CellID 55
```

**Step 4** Issue the following command to configure the physical cell ID. This examples configures cell ID 411.

```
set LTECell 55 CellConfig LTE RAN RF PhyCellIDConfigured 411
```

**Step 5** Issue the following command to verify the configuration:

```
show LTECell 55
Enable       true;
Name         Cell155;
Description  Kitchen;
RadioNode    55;
Radio        1;
CellConfig {
    LTE {
        RAN {
            Common {
                CellID 55;
            }
            RF {
                PhyCellIDConfigured 411;
            }
        }
    }
}
```

**Step 6** Issue the following command to set the TAC for LTE FAP of the Evolved Packet Core (EPC), to set the PLMN ID, and enable it. This example sets:

- the TAC to 1
- the PLMN EPC identity number to 1
- sets this as the primary PLMN ID
- sets the PLMN ID to 00102

```
set FAPService 1 CellConfig LTE EPC TAC 1 PLMNLList 1 IsPrimary true PLMNID 00102 Enable
true
```

**Step 7** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE EPC
TAC          1;
EAID         22;
eNodeBName   Siva;
PLMNLList 1 {
    Enable           true;
    IsPrimary        true;
```

```
PLMNID          00102;
```

### 6.3.2 Deleting a Small Cell and a Cell

To delete a small cell, delete the cell and small cell from the configuration.

**To delete a cell and small cell**

**Step 1** From the Configuration Mode, issue the **delete Cell <Number>** command to delete the cell from the network. This example deletes cell 66.

```
delete Cell 66
```

**Step 2** Issue the **show Cell <Number>** command to verify the configuration:

```
show cell 66
-----^
syntax error: unknown element
```

**Step 3** Issue the **delete RadioNode <Number>** command to delete the small cell. This example deletes small cell 66.

```
delete RadioNode 66
```

**Step 4** Issue the **show RadioNode <Number>** command to verify the configuration

```
show RadioNode 66
-----^
syntax error: unknown element
[error] [2011-08-30 17:59:36]
```

## 6.4 Disabling and Enabling Cell Transmission

It is often useful to temporarily disable all LTE cell transmission in the system for administrative or diagnostic purposes. Issue the **request lte cell disable all** command to remove all cells from service. Issue the **request lte cell enable all** command to restart transmission on all cells in the system.

**To disable all cell transmission**

**Step 1** From the Operational Mode, issue the **request lte cell disable all** command to disable all LTE cell transmission:

```
request lte cell disable all
status OK
```

**To enable cell transmission on all cells**

**Step 1** From the Operational Mode, issue the **request lte cell enable all** command to re-enable transmission on all LTE cells in the system:

```
request lte cell enable all
status OK
```



## 7 UMTS RF Management

RF management includes discovering the macro cells in the area, discovering the internal topology, assigning primary scrambling codes, setting maximum transmit power levels, and configuring cell neighbor lists to make the system operational. The goal of RF management is to configure and administer a collection of installed small cells after basic objects have been entered into the system. It intelligently configures the system from an RF perspective by determining the external and internal topologies by establishing:

- which other small cells can each small cell hear in the network.
- which macro cells can each small cell hear, and on which GSM and UMTS channels.

The system gathers this information from a Radio Environment Measurement (REM) scan process where it scans the radio environment to discover its topology. After the network is operational, the system can periodically re-scan to detect topology changes and use historical data to optimize the system and improve performance.

When a small cell is powered on, it attempts to locate the controller it is physically cabled to. If successful, both nodes exchange information. When you enable auto provisioning, the controller additionally creates small cell, radio, and cell objects representing the small cell and its components in the network. The controller auto provisioning feature:

- provisions the cell with the UTRA Absolute Radio Frequency Channel Number (*UARFCNDL*) configured for the deployment.
- assigns parameters, such as the primary scrambling code (*PrimaryScramblingCode*) and a power level (*MaxFAPTxPower*), to the internal cells. These parameters are not assigned based on knowledge of the RF environment.

After a REM scan, RF management assumes administration of the controller to maximize efficiency among the cells. Once the network is ready for operation and all cells have been provisioned, the administrator initiates a scan to discover the latest internal and external topology configurations. Thereafter, a new scan may be initiated manually or automatically at scheduled periodic intervals.

This chapter contains the following sections:

- [Section 7.1, RF Management Configuration Overview](#) on page 108
- [Section 7.2, Initial System Provisioning with the LCI](#) on page 108
- [Section 7.3, Before You Begin](#) on page 108
- [Section 7.4, Initial UMTS RF Management Provisioning](#) on page 108
- [Section 7.5, Basic UMTS REM Scanning](#) on page 109
- [Section 7.6, The Maximum UMTS Cell Transmit Power](#) on page 114
- [Section 7.7, Viewing UMTS RF Management Configurations](#) on page 116
- [Section 7.8, Advanced RF Management](#) on page 118
- [Section 7.9, Self-Configuration Zones](#) on page 128

## 7.1 RF Management Configuration Overview

Provisioning the system with the CLI involves configuring the initial RF management, then providing ongoing maintenance to fine-tune the system. The initial stage consists of running the first REM scan and reviewing the results. You may then re-provisioning neighbors and adjust the maximum transmit power levels.

Once the system is functioning, ongoing RF maintenance starts with additional REM scans to detect topology changes. These operational REM scans can be configured to automatically make changes to the system, or you can lock one or more attributes in the system or individual cells and view the results to identify the changes to the system topology. You can later unlock locked attributes and make changes to adjust transmit power, change to primary scrambling codes, and configure ongoing periodic REM scans.

## 7.2 Initial System Provisioning with the LCI

If the controller received initial system provisioning with the Local Configuration Interface (LCI) it may have already had an initial REM scan and has system-wide topological knowledge and assigned primary scrambling codes. The cells still must be assigned maximum power transmission values. If your system has already had an initial REM scan through the LCI, many of the next sections are not applicable. Proceed to [Section 7.5.3, Configuring the Power Transmission Range](#) on page 112. Refer to the *Cisco USC 8000 Series System Commissioning Guide* for more information about configuring the system with the LCI.

## 7.3 Before You Begin

The operating channel (*UARFCN*) must be configured before RF management can be enabled. Refer to [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85.

To verify the channel number

**Step 1** From the Configuration Mode, verify that the channel number has been configured:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF UARFCNDL
UARFCNDL
      "[ 1937 ]";
```

## 7.4 Initial UMTS RF Management Provisioning

Initial RF management procedures involve enabling RF management and placing controllers in service.

### 7.4.1 Enabling UMTS RF Management

RF management must be enabled before self-configuration services can operate.

**Step 1** From the Configuration Mode, enable RF management:

```
set FAPService 1 FAPControl UMTS SelfConfig NeighborListSelfConfigEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS SelfConfig NeighborListSelfConfigEnable
NeighborListSelfConfigEnable true;
```

## 7.4.2 Placing the USC 8088 Controller In Service

Operators performing initial system provisioning with the LCI can activate the controller to the point where it is ready to operate but is in maintenance mode and the small cells will not transmit. The controller must be placed in-service from within the provider core network.

To place a controller in service

**Step 1** From the Configuration Mode, issue the **set System OperatingMode InService** command to change the controller primary state from maintenance to in-service:

```
set System OperatingMode InService
```

## 7.5 Basic UMTS REM Scanning

REM scans survey the small cell solution and adjacent provider macro network to provide a detailed topological map of configured inter-frequency channels and the deployment channel to optimize the wireless environment. The Cisco small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

A REM scan detects the topology. It then takes the information from the latest scan and combines it with the historical measurements from user equipment to update the topology, power levels, and neighbor lists. Depending upon the size of the deployment, this process can take tens of minutes.

### 7.5.1 Configuring Basic and Periodic Scanning Parameters

When performing a REM scan, the system always scans the deployment UARFCN defined in [Section 5.2, Configuring UMTS Femto Access Point Service](#) on page 85. The following example configures:

- The REM scan of the environment and updates the cell neighbor lists and the primary scrambling code assignments.
- Additional channels used by the controller to scan for external neighbors. These channels typically correspond to channels used by the macro network. Note that the system scans:
  - the deployment channel that is configured at the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP RF** hierarchy level.
  - the UMTS channels specified with the **set FAPService <ServiceNumber> REM WCDMAFDD UARFCNDLLIST** command.
  - the GSM channels specified with the **set FAPService <ServiceNumber> REM GSM** command.
- A time and an interval (in seconds) for the periodic scanning operation. In the following example:
  - The time is 2011-08-01 (a Thursday) at 02:00:00 a.m. UTC.
  - The interval is 604800 seconds (1 week). The interval for GSM scanning must the same as the interval for UMTS scanning. In this example, GSM scanning is performed every time UMTS scanning is performed.

Combined, these values trigger the periodic scanning operation to occur every Thursday at 2:00 a.m. UTC.

GSM and UMTS bands and channels that should be used by the controller to scan for external neighbors. Valid bands and channels depend on the UMTS band deployment. [Table 18](#) shows the GSM and UMTS bands that each radio can scan:

**Table 18: UMTS Band Properties**

	Band 1	Band 2	Band 4
Uplink	1920–1980 MHz	1850–1910 MHz	1710–1755 MHz
Downlink	2110–2170 MHz	1930–1990 MHz	2110–2155 MHz
UMTS Monitor	925–960 MHz (Band 8) 2110–2170 MHz (Band 1)	1930–1990 MHz (Band 2) 2110–2155 MHz (Band 4) 869–894 MHz (Band 5)	1930–1990 MHz (Band 2) 2110–2155 MHz (Band 4)
GSM Monitor	925–960 MHz (E-GSM 950) 1805–1880 MHz (DCS 1800)	869–894 MHz (GSM 850) 1930–1990 MHz (PCS 1900)	869–894 MHz (GSM 850) 1930–1990 MHz (PCS 1900)

To configure basic and periodic scanning parameters

**Step 1** From the Configuration Mode, configure the channels to scan for UMTS neighbors. This example initiates a periodic scan of channel 1937 once a week at 2 a.m.

```
set FAPService 1 REM WCDMAFDD UARFCNDLList [ 1937 ] ScanPeriodically true PeriodicTime
2011-08-01T02:00:00Z PeriodicInterval 604800
```

**Step 2** Configure the channels to scan for GSM neighbors. This example initiates a scan of channels 200 and 201 on GSM band 850 once a week.

```
set FAPService 1 REM GSM REMBandList [ GSM850 ] ARFCNList [ 200 201 ] PeriodicInterval
604800
```

**Step 3** Issue the `show FAPService <ServiceNumber> REM` command to verify the configuration:

```
show FAPService 1 REM
WCDMAFDD {
    ScanPeriodically           true;
    PeriodicInterval          604800;
    PeriodicTime               2011-08-01T02:00:00Z;
    UARFCNDLList              "[ 1937 ]";
}
GSM {
    PeriodicInterval 604800;
    REMBandList      "[ GSM850 ]";
    ARFCNList        "[ 200 201 ]";
}
```

## 7.5.2 Configuring Primary Scrambling Codes

Through REM scan operations, the controller discovers, maintains, and updates a topological state of the external and internal networks that includes a list of all detected primary scrambling codes and corresponding measured signal strengths. After internal topology discovery, the system assigns each cell a primary scrambling code. The system intelligently assigns primary scrambling codes to cells, reusing the same primary scrambling codes as rarely and spread apart as possible.

### 7.5.2.1 Designating Primary Scrambling Codes for the small cell solution

The administrator must designate the set of allowable primary scrambling codes that the system can assign to cells in the network. Designate a range by defining the lower and upper integers (in that order) separated by two periods (...). Designate two non-contiguous ranges by separating the ranges with a space.

To configure the set of primary scrambling codes for the small cell solution

**Step 1** From the Configuration Mode, configure the set of primary scrambling codes for use in the system. This example uses primary scrambling codes 100 through 120 and 200 through 220.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCode [ 100..120 200..220 ]
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCode
PrimaryScramblingCode "[ 100..120 200..220 ]";
```

### 7.5.2.2 Configuring Alternate Primary Scrambling Codes

The small cell solution requires a sufficiently large set of primary scrambling codes to ensure adequate signal separation between two cells with the same primary scrambling code. However, some primary scrambling codes are special in that a fixed set are typically hard-coded in macro cells as neighbors for idle-mode cell re-selection to femto cells.

To ensure idle mode re-selection from the macro network to the small cell solution, the controller can assign these alternate primary scrambling codes to specific cells in the small cell solution. It is essential that these alternate primary scrambling codes be assigned to specific cells in the small cell solution to expedite their discovery by the UE, typically to cells near entrances and exits of the facility coverage area.

Ensure that the set of hard-coded primary scrambling codes used by macro network is known to the small cell solution. This will be the set designated as the alternate set of primary scrambling codes. The total number of alternate primary scrambling codes is determined by the operator network. Cisco Systems has observed that typically this number is six.

Cisco Systems recommends the following guidelines for assigning alternate primary scrambling codes:

1. Determine the physical locations of all the cells in the deployment area prior to the assigning alternate primary scrambling codes.
2. Alternate primary scrambling codes can be used more than once in a deployment, but do not reuse the same alternate primary scrambling codes with two cells within 150 meters (500 feet) horizontally or vertically. With this restriction in mind:
  - Cells near entrances to the deployment coverage area should be assigned alternate primary scrambling codes.
  - Cells in common areas or with high user mobility should be assigned alternate primary scrambling codes. Examples of such locations are cells covering stairwells, elevators, lobbies, cafeterias.

Individually configure each cell to either use the alternate primary scrambling codes or not by setting the value of **Cell <Number> CellConfig UMTS RAN FDDFAP RF UseSelfConfigAlternatePSC**. The default is false.

- When set to false, the cell is a part of set 1 and will be assigned a primary scrambling code from the primary scrambling codes configured with the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCode** command.
- When set to true, the cell is a part of set 2 and will be assigned a primary scrambling code from the set of alternate primary scrambling codes configured with the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP RF SelfConfigAlternatePSC** command.

For example, to use primary scrambling codes 506 through 511 as the alternate primary scrambling codes, issue the following command from the Configuration Mode:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF SelfConfigAlternatePSC [ 506..511 ]
```

Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF SelfConfigAlternatePSC  
SelfConfigAlternatePSC "[ 506..511 ]";
```

The main set and alternate set of primary scrambling codes can have no elements in common.



Note

When auto provisioning is enabled, new cells are automatically provisioned with **UseSelfConfigAlternatePSC** = FALSE, and are assigned a primary scrambling code from **PrimaryScramblingCode**.

### 7.5.3 Configuring the Power Transmission Range

When RF management is enabled, the system assigns the maximum transmit power to individual cells in the small cell solution. Enter the range limits as integers separated by two periods (..) from lower to higher. The transmit power level can be defined for the small cell solution as a whole, or for individual cells in environments containing a mix of small cell types. Assigning a cell a higher than its supported powering range triggers a PROV\_FAULT alarm and enters the cell into OOS-FAULT state.



Note

The system configures and reports power levels in units of 0.1 dBm.

To configure the maximum power transmission level for the small cell solution

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower** command to configure the maximum power transmission level for the small cell solution by defining the range of allowable transmission powers. The default range is -100 through 200 enterprise small cells and -100 through 240 for the optional extended coverage small cells. This example sets the range to -50 through 200.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower -50..200
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower  
MaxFAPTxPower -50..200;
```

To configure the maximum power transmission level for a cell

**Step 1** From the Configuration Mode, issue the **set Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower** command to configure the maximum power transmission level for a single cell. The default range is -100 through 200 enterprise small cells and -100 through 240 for the optional extended coverage small cells. This example sets the range of cell 1 to -50 through 240.

```
set Cell 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower -50..240
```

**Step 2** Issue the following command to verify the configuration:

```
show Cell 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower  
MaxFAPTxPower -50..240;
```

### 7.5.3.1 Configuring Periodic Power Reassignment

The network allows administrators to enable periodic power reassignment, during which the controller analyzes historical power measurements collected from user equipment to compute optimal power transmission values for each cell, and then assigns them.

To configure periodic power reassignment

- Step 1** From the Configuration Mode, configure the periodic power reassignment. This example enables periodic power reassignment once per day at 2:00 a.m.

```
set FAPService 1 REM WCDMAFDD PeriodicTxPwrRefresh true PeriodicTxPwrRefreshTime 2011-08-01T02:00:00Z PeriodicTxPwrRefreshInterval 86400
```

- Step 2** Issue the `show FAPService <ServiceNumber> REM WCDMAFDD` command to verify the configuration:

```
show FAPService 1 REM WCDMAFDD
ScanPeriodically          true;
PeriodicInterval           604800;
PeriodicTime               2011-08-01T02:00:00Z;
PeriodicTxPwrRefresh      true;
PeriodicTxPwrRefreshTime   2011-08-01T02:00:00Z;
PeriodicTxPwrRefreshInterval 86400;
```

### 7.5.4 Initial UMTS Self-Configuration

Once the RF management parameters have been configured and all cells are in service, issue the `request umts rem start` command from the Operational Mode to discover the topology, assign the primary scrambling codes, and to construct the neighbor lists for all individual cells. After initially running this command, you can issue it again manually or schedule it to run periodically as configured in [Section 7.5.1, Configuring Basic and Periodic Scanning Parameters](#) on page 109.

Note that accurate topology discovery requires that the small cells have settled local oscillators. Issue the `show RadioNode` command to ensure that all small cells are in the IS-NORMAL state. The system will reject the `request umts rem start` command unless all small cells are in the IS-NORMAL state.



The Cisco small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

**Note**

### 7.5.5 Aborting a UMTS REM Scan

You can manually stop a running LTE REM scan that you do not want to complete. For example, if you notice that the configuration is incorrect while the scan is in progress, rather than waiting for the scan to complete, you can abort the scan, change the configuration, and start a new scan. Aborting a REM scan will revert the system to the last known state.

To abort a UMTS REM scan

- Step 1** From the Operational Mode, issue the `request umts rem stop` command to manually abort a running UMTS REM scan:

```
request umts rem stop
```

## 7.6 The Maximum UMTS Cell Transmit Power

RF management allows you to configure the maximum UMTS cell transmit power or assign a cell its maximum transmit power based upon its physical location. Once the maximum transmit power has been configured, Cisco recommends limiting the difference in transmit power of adjacent cells.

### 7.6.1 Configuring the Maximum UMTS Cell Transmit Power

The maximum transmit power level for each UMTS cell is defined by the lowest configured value of the maximum transmit power of the cell, FAPservice (radio services), and small cell. The value is computed by the formula  $\text{Minimum}(\text{maxTx1}, \text{maxTx2}, \text{maxTx3})$ , where:

- **maxTx1** is the value defined in `Cell <Number> CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower <minTx1>..<maxTx1>`
- **maxTx2** is the value defined in `FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPower <minTx2>..<maxTx2>`
- **maxTx3** is the value defined in `RadioNode <Number> Radio 1 MaxTxPower <maxTx3>`



RF management transmit power allocation commands cannot be run during a REM scan.

#### Note

To configure the maximum UMTS cell transmit power

**Step 1** From the Operational Mode, issue the `request umts self-config tx-power-assignment max-power` command to update the cell power assignments to the maximum allowable power:

```
request umts self-config tx-power-assignment max-power
```

### 7.6.2 Configuring Location-Based Power Allocation

Administrators can assign location types to a cell that best describes the cell's placement. The system supports the following location types.

The system contains the following location types:

- **Atrium:** The cell is located in or near an atrium of the building.
- **Basement:** The cell is located in the basement of the building.
- **Cafeteria:** The cell is located in or near a cafeteria.
- **Egress:** The cell is located near an entrance.
- **Elevator:** The cell is close to an elevator.
- **Exterior:** The cell is externally facing. Non small cell solution users are expected to see this cell.
- **HandIn:** The cell is located in hand-in zone.

- **Interior:** The cell is internal to the small cell solution. Non small cell solution deployment users are not expected to see this cell.
- **MeetingRoom:** The cell is located in a meeting room.

You can assign a cell multiple location types. For example, if a cell is located near an entryway and also close to an elevator, you can assign it the location type parameter value: **LocationType [ Elevator Egress ]**.



RF management transmit power allocation commands cannot be run during a REM scan.

#### Note

To configure location-based power allocation

- Step 1** From the Configuration Mode, issue the **set cell <Number> LocationType** command to set the location type of the new cell. This example modifies cell 1 in small cell 1 and locates the cell in a meeting room named *Meeting\_Room1*.

```
set Cell 1 Enable true LocationType [ MeetingRoom ] Description Meeting_Room1 RadioNode 1
```

- Step 2** Issue the **commit** command to commit the changes:

```
commit
```

- Step 3** From the Operational Mode, issue the following command to apply location-based maximum power assignments:

```
request umts self-config tx-power-assignment location-type-based
```

- Step 4** Issue the following command to verify the configuration.

```
show Cell UMTS
```

CellHandle	Name	RN	CID	UCID	PSC	MaxTxPwr	ModeInUse	RLs
1	Meeting_Room1	1	1	66191771	114	20.0dBm	UMTSNodeB	

### 7.6.3 Configuring the Maximum Cell Power Level Delta

In typical scenarios, nearby cells should not have very disparate power levels. The system can be configured with a maximum transmission power delta such that neighboring cells cannot differ by more than the value of the delta. A cell covering areas with large path losses in one direction, such as near an entrance, simultaneously covers points with large path losses in all directions, which can easily cause nearby cells to shrink. When a system is assigned the maximum cell power level delta, the delta constraint is applied when any transmit power assignment commands are run and powers are reset.

To set the maximum power level delta for adjoining cells

- Step 1** From the Configuration Mode, issue the following command to run the RF management powering algorithm to limit the power differential of adjacent cells. This example sets the power delta to 20 dBm (200 units of 0.1 dBm).

```
set FAPService 1 FAPControl UMTS SelfConfig MaxPowerDelta 200
```

- Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS SelfConfig MaxPowerDelta  
MaxPowerDelta 20;
```

## 7.7 Viewing UMTS RF Management Configurations

This section discusses how to view the RF management configuration and REM scan results.

### 7.7.1 Viewing the UMTS RF Management Configuration

Before fine-tuning the system after the initial REM scan, view the current RF management configuration.

To view the current UMTS RF management configuration

**Step 1** From the Operational Mode, issue the **show RFMgmt UMTS Configuration** command to view the current configuration space before running the REM scan:

```
show RFMgmt UMTS Configuration
Global:
=====
FAPService FAPControl UMTS Self-Config. Param's:
-----
Neighbor List Self-Config. Enable           false
Meas. IMSI List                           0000000000000000
Meas. Loading Factor                     70
FAP Coverage Target Value 2             -30
FAP Coverage Target Addition Delta     30
Num. Meas. UE                            2
Num. PTS Thresh.                         1000
Num. IMSI Thresh.                        2
Num. Valid RS Thresh.                   2
R Meas. Discard                          0
Require Freq. Stability For Topo. Disc. true

FAPService Provisioned External InterRAT (GSM) Neighbors:
-----
Index  Enable  Inclusion Mode  PLMNID  LAC    BSIC  CI   Band Indicator  ARFCN  Q Offset 1  RSSI
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
FAPService Provisioned External UMTS IntraFreq Neighbors:
-----
Index  Enable  Inclusion Mode  PLMNID  RNCID  CID   LAC    RAC  URA    PSC  PCPICHTxPower  Q Offset 1  Q Offset 2  CPICH RSCP
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
FAPService Provisioned External UMTS InterFreq Neighbors:
-----
Index  Enable  Inclusion Mode  PLMNID  RNCID  CID   LAC    RAC  URA    PSC  PCPICHTxPower  Q Offset 1  Q Offset 2  CPICH
RSCP  DL  UARFCN
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
[output truncated]
```

### 7.7.2 Viewing UMTS REM Scan Results

You can view the results of a UMTS REM scan for all detected cells, detected internal GSM cells, detected internal UMTS cells, and cell neighbors.



Issuing the **show RFMgmt UMTS DetectedCells** command while a REM scan is active can return inaccurate results. The screen displays the following message:

Note: RF Management is active.

To view UMTS REM scan results

**Step 1** From the Operational Mode, issue the **show RFMgmt UMTS DetectedCells** command to view all detected cells:

```
show RFMgmt UMTS DetectedCells
Note: RF Management is active.
```

List Of Cells Detected By Internal Cell With Cell Handle 73, CID 73, And Cell ID 73:

Detected Internal UMTS Cells:

Cell Handle	CID	Cell ID	PSC	DL UARFCN	CPICH RSCP*
-------------	-----	---------	-----	-----------	-------------

\* Measured When Detected Internal UMTS Cell Was Transmitting At FAPService Maximum MaxFAPTxPower  
[output truncated]

**Step 2** Issue the **show RFMgmt UMTS MeasurementOfGSMCell** command to view detected internal GSM cells:

**show RFMgmt UMTS MeasurementOfGSMCell**

Note: RF Management is active.

Detecting CellID	Detecting CID	BSIC	CI	ARFCN	BandID	RSSI
------------------	---------------	------	----	-------	--------	------

**Step 3** Issue the **show RFMgmt UMTS MeasurementOfUMTSCell** command to view detected internal UMTS cells:

**show RFMgmt UMTS MeasurementOfUMTSCell**

Note: RF Management is active.

Detecting CellID	Detecting CID	CellID	RNCID	CID	UARFCNDL	PSC	CPICHRSCP
1382	1382	196611307	3000	3307	10800	222	-41
3307	3307	196609382	3000	1382	10800	220	-41

**Step 4** Issue the **show RFMgmt UMTS NeighborCells** command to view detected neighbor cells. Note that the CPICH RSCP value of -3276 is invalid and only used when the cell is included as a neighbor of itself.

**show RFMgmt UMTS NeighborCells**

Note: RF Management is active.

List Of Neighbors Of Internal Cell with Cell Handle 73 And CID 73:

Internal And External IntraFreq UMTS Neighbors:

CID	RNCID	PSC	CPICH RSCP	Tier
3307	4037	221	-3276	0
28276	4037	5	-85	1
27467	4037	3	-85	1
27459	4037	506	-85	1
33092	706	20	-85	1

External InterFreq UMTS Neighbors:

CID	RNCID	PSC	DL UARFCN	CPICH RSCP	Tier
52098	706	50	10736	-85	1
44593	706	53	10736	-85	1
53059	706	52	10712	-85	1

GSM Neighbors:

ARFCN	Frequency	Band	BSIC	CI	RSSI	Tier
77	GSM	900	48	18647	-85	1
555	DCS	1800	32	10005	-85	1
87	GSM	900	53	18321	-85	1
549	DCS	1800	43	10068	-85	1

```

85      GSM 900    17  29292   -85     1
77      GSM 900    17  3774    -85     1

```

[output truncated]

## 7.8 Advanced RF Management

Advanced RF management consists of the following tasks:

- [Section 7.8.1, Training the System to Set Cell Power Levels](#) on page 118
- [Section 7.8.2, Provisioning UMTS Neighbor Lists](#) on page 119
- [Section 7.8.3, Adding or Deleting a UMTS Cell from an Operational Network](#) on page 120
- [Section 7.8.4, Excluding a Cell from all small cell solution Neighbor Lists](#) on page 121
- [Section 7.8.5, Including and Excluding a Neighbor for a UMTS Single Cell](#) on page 121
- [Section 7.8.6, Creating the Final UMTS Neighbor List](#) on page 122
- [Section 7.8.7, Bypassing UMTS REM Scan Topology Components](#) on page 123
- [Section 7.8.8, Manually Assigning Primary Scrambling Codes](#) on page 124
- [Section 7.8.9, Manually Assigning Maximum Power Transmission Levels](#) on page 124
- [Section 7.8.10, UMTS REM Scan Locking](#) on page 124
- [Section 7.8.11, Reinitializing the UMTS RF Management Suite](#) on page 127

### 7.8.1 Training the System to Set Cell Power Levels

After initial self-configuration the system will gather measurements and tune power levels over time if periodic transmit power refresh is enabled. The administrator can optionally tune the power levels quickly by performing a UE walkthrough of the deployment area.

This method requires that you take the measurements in every part of the deployment area that you expect cell service to reach using a device with a known International Mobile Subscriber Identity (IMSI). The device is configured by the system to feed measurements back to the controller.



The UE walkthrough procedure requires no special equipment or software. Any network-compatible off-the-shelf device may be used.

#### Note

After a complete walkthrough of the deployment area, the gathered measurements are processed to determine the *MaxFAPTxPower* assignments for the cells in the system.

To manually train the system

**Step 1** Identify the IMSI of an off-the-shelf UMTS device.

**Step 2** From the Configuration Mode, enter the IMSI in the system database. In this example, the IMSI is 123456789101001.

```
set FAPService 1 FAPControl UMTS SelfConfig MeasIMSLList 123456789101001
```

**Step 3** Issue the following command to verify the IMSI number:

```
show FAPService 1 FAPControl UMTS SelfConfig MeasIMSLList
MeasIMSLList 123456789101001;
```

**Step 4** Connect the UE with a voice or data session, and walk throughout the entire deployment area, staying within the required coverage area. During this time, the network automatically gathers standardized UE measurements reported to the network for handoff purposes. If the UE call drops, reconnect and continue.

**Step 5** Once the walk-through is complete, terminate all UE CS and PS connections. Either turn the UE completely off or enter it into Airplane Mode.

**Step 6** Issue the following command from the Operational Mode to instruct the controller to process the UE measurements:

```
run request umts self-config tx-power-assignment ue-measurement-based
```

The controller computes a maximum power assignment for each cell and configures the cells accordingly.

**Step 7** Issue the `run show Cell UMTS` command to verify the configuration:

```
run show Cell UMTS
```

CellHandle	Name	RN	CID	UCID	PSC	MaxTxPwr	ModeInUse	RLs
1	-		1	1		1 400	11.0dBm UMTSNetmon	0
2	-		2	2		2 400	11.0dBm UMTSNetmon	0

## 7.8.2 Provisioning UMTS Neighbor Lists

The Cisco small cell network automatically detects UMTS and GSM macro network neighbors for each cell on the channels configured for scanning in the `FAPService <ServiceNumber> REM` object. You can optionally manually add up to 32 macro neighbors for a cell for each neighbor type:

- intra-frequency (UMTS, co-channel)
- inter-frequency (UMTS, not co-channel)
- inter-RAT (GSM)

For inter-frequency provisioned UMTS neighbors, the provisioned information is handled differently depending upon whether the specific `UARFCNDL` is one of those scanned by the system (as specified in the `UARFCNDLList` of the REM object, described in [Section 7.5.1, Configuring Basic and Periodic Scanning Parameters](#) on page 109).

Inter-RAT GSM neighbors are managed in a similar fashion as inter-frequency UMTS neighbors, but use the `BCCHARFCN` parameter rather than `UARFCNDL`.

To manually provision cell neighbors

**Step 1** From the Configuration Mode, provision an intra-frequency UMTS neighbor. In this example, provisioned intra-frequency neighbor index 1 is a cell with the primary scrambling code 125.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList IntraFreqCell 1 Enable true
PCPICHScramblingCode 125 CID 51 RNCID 102 LAC 10 RAC 10 URA 10 PLMNID 00102 MustInclude
true
```

**Step 2** Add an inter-frequency UMTS neighbor. In this example, provisioned inter-frequency neighbor index 1 is a cell with operating channel 2087 and primary scrambling code 203.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList InterFreqCell 1 Enable true
UARFCNDL 2087 PCPICHScramblingCode 203 CID 410 RNCID 102 LAC 10 RAC 10 URA 10 PLMNID 00102
MustInclude true
```

**Step 3** Add a GSM neighbor. In this example, the provisioned inter-RAT neighbor index 1 is a cell with operating channel 1000 in band `GSM850`.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList InterRATCell GSM 1 Enable true
BCCHARFCN 1000 BSIC 58 CID 103 BandIndicator GSM\ 850 LAC 14 PLMNID 00102 MustInclude true
```

**Step 4** Issue the following command to verify the neighbor list configuration. Note that this command returns only manually provisioned cell neighbors. Refer to [Section 7.7.1, Viewing the UMTS RF Management Configuration](#) on page 116 for more information about viewing cell neighbors.

```
show FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList
IntraFreqCell 1 {
    Enable          true;
    PLMNID         00102;
    RNCID          102;
    CID            51;
    LAC             10;
    RAC             10;
    URA             10;
    PCPICHScramblingCode 125;
    InclusionMode  MustInclude;
}
InterFreqCell 1 {
    Enable          true;
    PLMNID         00102;
    RNCID          102;
    CID            410;
    LAC             10;
    RAC             10;
    URA             10;
    UARFCNDL       2087;
    PCPICHScramblingCode 203;
    InclusionMode  MustInclude;
}
InterRATCell {
    GSM 1 {
        Enable          true;
        PLMNID         00102;
        LAC            14;
        BSIC           58;
        CI              103;
        BandIndicator "GSM 850";
        BCCHARFCN     1000;
        InclusionMode MustInclude;
    }
}
```

### 7.8.3 Adding or Deleting a UMTS Cell from an Operational Network

To add a UMTS cell to the network, add the small cell and the cell to an operational network either manually or by using the auto provisioning feature. Once the small cell and corresponding cell is ready, the small cell solution will automatically self-configure it. All other cells in the small cell solution remain operational throughout this process.



When a cell is added to an operational network, the topology discovery of the newly added cell is determined by the external network. Additionally, the new cell maximum transmit power will typically be relatively low. The administrator can optionally let the system tune itself in periodic operations or reinitialize it as shown in [Section 7.8.11, Reinitializing the UMTS RF Management Suite](#) on page 127.

If a cell is removed from the network, first delete the cell and then the small cell from the configuration. Refer to [Section 5.3.3, Deleting a Small Cell and a Cell](#) on page 90 for more information.

## 7.8.4 Excluding a Cell from all small cell solution Neighbor Lists

If there are particular external cells that appear in a UMTS REM scan that you want to ignore, you can define cells that will be excluded from the neighbor list of all cells in the system.

To exclude a cell from all neighbor lists in the small cell solution

**Step 1** From the Configuration Mode, issue the following command to exclude a cell as an intra-frequency neighbor for all neighbor lists in the system. This list excludes cell 111.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList IntraFreqCell 111 InclusionMode MustExclude Enable true
```

**Step 2** Issue the following command to exclude a cell as an inter-frequency neighbor for all neighbor lists in the system. This list excludes cell 222.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList InterFreqCell 222 InclusionMode MustExclude Enable true
```

**Step 3** Issue the following command to exclude a cell as an intra-RAT GSM neighbor for all neighbor lists in the system. This list excludes cell 333.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList InterRATCell GSM 333 InclusionMode MustExclude Enable true
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList
NeighborListLockEnable false;
InterFreqCell 222 {
    Enable                  true;
    InclusionMode          MustExclude;
}
InterRATCell {
    GSM 303 {
        Enable                  true;
        InclusionMode          MustExclude;
    }
    GSM 333 {
        Enable                  true;
        InclusionMode          MustExclude;
    }
}
```

## 7.8.5 Including and Excluding a Neighbor for a UMTS Single Cell

You can define a neighbor that must be included to the neighbor list of a specific cell. For example, a cell by an entrance could be assigned the neighbor of the closest mobile provider macro cell to hand users off to when they leave the building. You can also exclude a neighbor from a single cell neighbor list.

Including and excluding cells for a single cell neighbor list is similar for inter-frequency, intra-frequency, and inter-RAT cells. For brevity, the example below shows one command each for adding and excluding a cell to a single cell neighbor list.

Before including or including a specific neighbor cell from a cell in the small cell solution, ensure that this neighbor cell is already defined in under FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList. Then use the cell identifier as a reference to include/ exclude such neighbor cells from the individual cell neighbor list using one of the following commands:

```
set Cell <CellNumber> CellConfig UMTS RAN FDDFAP NeighborList InterFreqCell <CellNumber> InclusionMode MustInclude
```

or

```
set Cell <CellNumber> CellConfig UMTS RAN FDDFAP NeighborList InterFreqCell <CellNumber>
InclusionMode MustExclude
```

The examples below use existing neighbor cells verified with the following command:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList
IntraFreqCell 1001 {
InterRATCell {
    GSM 2001 {

[output truncated]
```

To include a neighbor to a UMTS single cell

**Step 1** From the Configuration Mode, issue the following command to add a neighbor to the neighbor list of a single cell. This example includes cell 1001 to the neighbor list of cell 9999.

```
set Cell 9999 CellConfig UMTS RAN FDDFAP NeighborList InterFreqCell 1001 InclusionMode
MustInclude
```

**Step 2** Issue the following command to exclude a neighbor from the neighbor list of a single cell. This example excludes cell 2001 from the neighbor list of cell 9999.

```
set Cell 9999 CellConfig UMTS RAN FDDFAP NeighborList InterRATCell GSM 2001 InclusionMode
MustExclude
```

**Step 3** Issue the following command to verify the configuration:

```
show Cell 9999 CellConfig UMTS RAN FDDFAP NeighborList
NeighborList {
    InterFreqCell 1001 {
        InclusionMode MustInclude;
    }
    InterRATCell {
        GSM 2001 {
            InclusionMode MustExclude;
        }
    }
}
```

## 7.8.6 Creating the Final UMTS Neighbor List

After tuning UMTS neighbor lists by manually adding or excluding cells, create the final neighbor list by issuing the **request umts self-config neighborlist-create** command. This command combines the neighbor information detected during REM scans with the manually provisioned cell neighbors for the final neighbor lists.

To create a final LTE neighbor list

**Step 1** From the Operational Mode, issue the following command to create the final neighbor list. This combines the topological information from the REM scan with the manually provisioned neighbor lists.

```
request umts self-config neighborlist-create
```

**Step 2** Issue the **show RFMgmt UMTS NeighborCells** command to view the final neighbor list. Note that the CPICH RSCP value of -3276 is invalid and only used when the cell is included as a neighbor of itself.

```
show RFMgmt UMTS NeighborCells
List Of Neighbors Of Internal Cell with Cell Handle 1 And CID 1:
-----
Internal And External IntraFreq UMTS Neighbors:
=====
```

```

CID  RNCID  PSC  CPICH RSCP  Tier
----  -----  ---  -----  -----
 1    1000   15      -3276    0
 2    1000    0       -32      1

External InterFreq UMTS Neighbors:
=====
CID  RNCID  PSC  DL UARFCN  CPICH RSCP  Tier
----  -----  ---  -----  -----  -----
[output truncated]

```

## 7.8.7 Bypassing UMTS REM Scan Topology Components

To granularly fine-tune a REM scan, you can configure which parts of the topology are scanned. For example, if the internal topology functions properly and UMTS neighbors are stable, you can save time and network resources by scanning only for GSM neighbors. A topological REM scan can be subdivided by enabling or disabling the following components:

- **UMTSExtIntraFreqREMScanEnable**: external UMTS intra-frequency neighbor cells
- **UMTSExtInterFreqREMScanEnable**: external UMTS inter-frequency neighbor cells
- **GSMREMScanEnable**: external inter-RAT GSM neighbor cells
- **InternalTopologyDiscoveryEnable**: Cisco internal cells

To configure REM scan topological parameters

**Step 1** From the Configuration Mode, issue the following command to configure the external UMTS intra-frequency neighbor component of the REM scan. This example enables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig UMTSExtIntraFreqREMScanEnable true
```

**Step 2** Issue the following command to configure the external UMTS inter-frequency neighbor component of the REM scan. This example disables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig UMTSExtInterFreqREMScanEnable false
```

**Step 3** Issue the following command to configure the external inter-RAT GSM neighbor component of the REM scan. This example enables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig GSMREMScanEnable true
```

**Step 4** Issue the following command to configure the Cisco internal neighbor component of the REM scan. This example disables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig InternalTopologyDiscoveryEnable false
```

**Step 5** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS SelfConfig
UMTSExtIntraFreqREMScanEnable          true;
UMTSExtInterFreqREMScanEnable          false;
GSMREMScanEnable                      true;
InternalTopologyDiscoveryEnable        false;
```

## 7.8.8 Manually Assigning Primary Scrambling Codes



Note

---

Neighbor cells are a combination of detected and provisioned cells.

---

You can manually assign a cell a specific primary scrambling code. Valid options are 0 through 511.

To assign a cell a primary scrambling code

**Step 1** From the Configuration Mode, issue the following command to assign a cell a primary scrambling code. This example assigns cell 22 the primary scrambling code 101,

```
set cell 22 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCode 101
```

**Step 2** Issue the following command to verify the configuration:

```
show Cell 22 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeConfigured
PrimaryScramblingCodeConfigured 101;
```

## 7.8.9 Manually Assigning Maximum Power Transmission Levels

You can manually assign a cell a specific maximum power transmission level. Valid options are -100 through 240 (in units of 0.1 dBm).



Note

---

If periodic REM scanning is enabled, the system will continue to change maximum transmit power over time.

---

To assign a cell a maximum power transmission level

**Step 1** From the Configuration Mode, issue the following command to assign a cell a maximum power transmission level. This example assigns cell 33 the maximum power transmission level of 10 dBm (100 units of 0.1 dBm).

```
set Cell 33 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerConfigured 100
```

**Step 2** Issue the following command to verify the configuration:

```
show cell 33 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerConfigured
MaxFAPTxPowerConfigured 100;
```

## 7.8.10 UMTS REM Scan Locking

You can lock the attributes, including primary scrambling code, maximum transmit power level, and neighbor lists, for all cells in the small cell solution, cells in the default SONConfig zone, or individual cells such that a REM scan detects the topology but takes no action to reconfigure the specific attributes of the system or cells. These RF attributes can be manually configured at a later date if needed.

Alternatively, you can lock the individual attributes for all cells or individual cells during a REM scan such that the locked attributes retain their values but the unlocked attributes will be reconfigured after the scan using the new topological information. Locked cells and attributes cannot be modified. Unlock the cell or attribute to make changes to it.

Locking is hierarchical, when an attribute is locked from the system (FAPService) level, all cells in the system have that attribute locked during REM scans until it is unlocked. Similarly, when one or more attributes are locked for a specified cell, they remain locked for that cell until they are unlocked.

For an individual cell:

- the primary scrambling code is locked when:
  - `FAPService 1 CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable true`
- the maximum transmit power is locked when:
  - `FAPService 1 CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable true`
- the neighbor list is locked when:
  - `FAPService 1 CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP RF RFLockEnable true`
  - `Cell <CellNumber> CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable true`

#### 7.8.10.1 Locking System-Wide UMTS Cell RF Attributes During REM Scan

Locking system-wide cell attributes (FAPService) prevents changes to the primary scrambling code, maximum power level, and neighbor list of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

To lock all RF attributes during UMTS REM scanning for all cells

- Step 1** From the Configuration Mode, issue the following command to lock the cell RF attributes during REM scanning for all cells in the small cell solution.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF RFLockEnable true
```

- Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF RFLockEnable  
RFLockEnable true;
```

#### 7.8.10.2 Locking Attributes of a Single Cell During a UMTS REM Scan

Locking single cell attributes prevents changes to the primary scrambling code, maximum power level, and neighbor list on the specified cell. These attributes remain locked during REM scans until unlocked. To change any of these parameters, unlock the cell and make the changes. You can then re-lock the cell as needed.

To lock the RF attributes of a single cell during REM scan

- Step 1** From the Configuration Mode, issue the following command to lock the RF attributes of a single cell during REM scan. This example uses cell 100.

```
set Cell 100 CellConfig UMTS RAN FDDFAP RF RFLockEnable true
```

- Step 2** Issue the following command to verify the configuration:

```
show cell 100 CellConfig UMTS RAN FDDFAP RF RFLockEnable  
RFLockEnable true;
```

### 7.8.10.3 Locking System-Wide Primary Scrambling Codes

You can prevent a REM scan from changing the primary scrambling codes of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these primary scrambling codes, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

#### To lock primary scrambling codes for all cells

**Step 1** From the Configuration Mode, issue the following command to lock all primary scrambling codes in the system:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable  
PrimaryScramblingCodeLockEnable true;
```

### 7.8.10.4 Locking Single Cell Primary Scrambling Codes

Locking a single cell primary scrambling code prevents changes to the primary scrambling code on the specified cell. These attributes remain locked during REM scans until unlocked. To change this parameter, unlock the cell and make the changes. You can then re-lock the cell as needed.

#### To lock the primary scrambling code for a cell

**Step 1** From the Configuration Mode, issue the following command to lock the primary scrambling code for a single cell. This example locks cell 101.

```
set cell 101 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show Cell 101 CellConfig UMTS RAN FDDFAP RF PrimaryScramblingCodeLockEnable  
PrimaryScramblingCodeLockEnable true;  
MaxFAPTxPower -100..100;
```

### 7.8.10.5 Locking System-Wide Maximum Power Transmission Levels

You can prevent a REM scan from changing the maximum power transmission level of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

#### To lock maximum power transmission levels for all cells

**Step 1** From the Configuration Mode, issue the following command to lock all maximum power transmission level in the system:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable  
MaxFAPTxPowerLockEnable true;
```

### 7.8.10.6 Locking Single Cell Maximum Power Transmission Levels

Locking a single cell maximum power transmission level prevents changes to the maximum power transmission level on the specified cell. This attribute remains locked during REM scans until unlocked. To change this parameter, unlock the cell and make the changes. You can then re-lock the cell as needed.

To lock the maximum power transmission level for a cell

**Step 1** From the Configuration Mode, issue the following command to lock the maximum power transmission level for a single cell. This example locks cell 102.

```
set cell 102 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show cell 102 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable
MaxFAPTxPowerLockEnable true;
```

#### 7.8.10.7 Locking System-Wide UMTS Neighbor Lists

You can prevent a REM scan from changing the neighbor list of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

To lock neighbor lists of all cells

**Step 1** From the Configuration Mode, issue the following command to lock all neighbor lists in the system:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable
NeighborListLockEnable true;
```

#### 7.8.10.8 Locking Single Cell Neighbor Lists

Locking a single cell neighbor list prevents changes to the primary scrambling code on the specified cell. This attribute remains locked during REM scans until unlocked. To change this parameter, unlock the cell and make the changes. You can then re-lock the cell as needed.

To lock the neighbor list for a cell

**Step 1** From the Configuration Mode, issue the following command to lock the neighbor list level for a single cell. This example locks cell 103.

```
set Cell 103 CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show Cell 103 CellConfig UMTS RAN FDDFAP NeighborList NeighborListLockEnable
NeighborListLockEnable true;
```

### 7.8.11 Reinitializing the UMTS RF Management Suite

The administrator can reinitialize the entire self-configuring subsystem at any time. The following examples are typical reasons to reinitialize the RF management suite:

- If new cells have been added to the system, have been physically moved, or construction has altered the deployment area and the administrator wants an optimal topology discovery, run a new REM scan. Refer to [Section 7.5.4, Initial UMTS Self-Configuration](#) on page 113.
- You can retrain power levels in the following ways:
  - ♦ To reset all cell powers to the maximum level, issue the following command from the Operational Mode:

```
request umts self-config tx-power-assignment max-power
```

- ♦ To discard all UE measurement reports, issue the following command from the Operational Mode:

```
request umts self-config clear-ue-measurements
```

- ♦ Refer to [Section 7.6.1, Configuring the Maximum UMTS Cell Transmit Power](#) on page 114.

When the procedure has completed, walk through the deployment area to gather new measurements as described in [Section 7.8.1, Training the System to Set Cell Power Levels](#) on page 118.

## 7.9 Self-Configuration Zones

For incremental provisioning, and fast scanning of a subset of cells, cells in the Cisco small cell network can be segregated into zones for RF management purposes. Self-configuration zones offer flexibility in system configuration and management. Self-configuration zones can be defined for the following use cases:

- To configure one building at a time in multi-building deployment. The buildings must be separated by at least 100 meters (325 feet).
- To create a subset of internal cells for periodic scans.
- To create multiple zones to execute passive REM scans in parallel.
- To split a long GSM ARFCN list across multiple zones to reduce scan time.
- To assign different operating parameters to certain cells in a deployment.
- To use zones to reduce the time required for internal topology discovery.
- To execute the transmit power assignment on a subset of cells.
- To leave certain zones operational while others are engaged in RF management activities.

Two types of zones have been introduced to support these use cases:

- **SONConfigAndScanZone:** Every cell belongs to one and only one SONConfigAndScanZone. When a REM scan is executed on a SONConfigAndScanZone, the primary scrambling code, transmit power and neighbor list of the cells in the zone is set to be consistent with these configuration parameters.

You can create multiple SONConfigAndScan zones. Cells of one SONConfigAndScanZone can be operational while other zones are engaged in RF management activities.

When a cell is created it belongs to the default SONConfigAndScan zone unless specified otherwise. The default zone is the FAPService. One cannot explicitly add or remove cells from the default zone. A cell is automatically removed from the default zone when it is placed into another SONConfigAndScan zone. It is added to the default zone when it is deleted from another SONConfigAndScan zone.

Placing a cell in one SONConfigAndScan zone removes it from its former zone. If the deployment topology requires that one or more cells be assigned a unique set of attributes, such as primary scrambling codes or power assignments, then create a SONConfigAndScan zone and place the cells in it so that those cells can be configured independently of other cells. Refer to [Section 7.9.3.1, Turning up a Multi-Building Campus](#) on page 138 for an example of using multiple SONConfigAndScan zones.

- **SONScanZone:** Used to execute a REM scan on a subset of cells, a SONScanZone REM scan does not change the operational parameters of the cells. It is used to execute passive REM scans on the sets of cells in the zone. A cell may belong to multiple SONScanZones.

Only one SONScan or SONConfigAndScan zone can be executing REM operations on any one cell at any given time.

## 7.9.1 Managing Zones

The following sections have information about managing zones:

- [Section 7.9.1.1, Creating a Zone](#) on page 129
- [Section 7.9.1.2, Adding a Cell to a Zone](#) on page 130
- [Section 7.9.1.3, Enabling all Cells in a Zone](#) on page 130
- [Section 7.9.1.4, Disabling all Cells in a Zone](#) on page 130
- [Section 7.9.1.5, Deleting a Cell from a Zone](#) on page 130
- [Section 7.9.1.6, Moving a Cell to a Different SONConfig Zone](#) on page 131
- [Section 7.9.1.7, Creating a UMTS Zone Reference Neighborhood List](#) on page 131
- [Section 7.9.1.8, Deleting a UMTS Zone Reference Neighborhood List](#) on page 131
- [Section 7.9.1.9, Deleting a UMTS Zone Detected Neighborhood List](#) on page 132
- [Section 7.9.1.10, Deleting a Zone](#) on page 132
- [Section 7.9.1.11, Viewing the Zone Configuration](#) on page 132
- [Section 7.9.1.12, Viewing the Default SONConfigAndScan Zone](#) on page 133
- [Section 7.9.1.13, Executing a REM Scan on a Zone](#) on page 134
- [Section 7.9.1.14, Assigning Cell Transmit Power Levels to a Zone](#) on page 135
- [Section 7.9.1.15, Configuring Maximum Cell Transmit Power in a Zone](#) on page 135

### 7.9.1.1 Creating a Zone

You can create up to 32 total zones of all types. Once a zone is created, its zone type cannot be modified.

To create an RF management zone

- Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> UMTS Zone** command to create a zone. This example creates a SONScanZone number 1, names it *Entrances*, and enables periodic scanning every 86400 seconds (1 day).

```
set FAPService 1 UMTS Zone 1 Description Entrances Type SONScanZone SONscan
ScanPeriodically true PeriodicInterval 86400
```

- Step 2** Issue the **show FAPService <ServiceNumber> UMTS Zone** command to verify the configuration:

```
show FAPService 1 UMTS Zone
Zone 1 {
    Description Entrances;
    Type        SONScanZone;
    CellList    "[ ]";
    SONScan {
        ScanPeriodically      true;
        PeriodicInterval     86400;
    }
}
```

### 7.9.1.2 Adding a Cell to a Zone

Adding a cell to a zone does not change any cell configuration parameters. If RF management operations are running, cells can be added to unconfigured zones.

To add a cell to a zone

**Step 1** From the Configuration Mode, issue the following command to add a cell to a zone. This example adds cells 44, 45, and 46 to SONConfig zone 2.

```
set FAPService 1 UMTS Zone 2 Type SONConfig CellList [ 44 45 46 ]
```

**Step 2** Issue the show **FAPService <ServiceNumber> UMTS Zone** command to verify the configuration:

```
show FAPService 1 UMTS Zone
Zone 2 {
    Type          SONConfig;
    CellList     "[ 44 45 46 ]";
}
}
```

### 7.9.1.3 Enabling all Cells in a Zone

You can enable all cells in a zone at one time

To enable all cells in a zone

**Step 1** From the Operational Mode, issue the **request umts cell enable zone-id** command to enable all cells in a zone. This example enables all cells in zone 3.

```
request umts cell enable zone-id 3
```

**Step 2** Issue the command to verify the configuration:

show cell						
CellHandle	Name	RN	Radio	ModeInUse	ConfState	OperState
1	-	8	1	UMTSNodeB	PROVISIONED	OS-DISABLE
2	-	5	1	UMTSNodeB	PROVISIONED	IS-IDLE
3	-	9	1	UMTSNodeB	PROVISIONED	OS-DISABLE
4	-	2	1	UMTSNodeB	PROVISIONED	IS-IDLE

### 7.9.1.4 Disabling all Cells in a Zone

You can disable all cells in a zone at one time.

To disable all cells in a zone

**Step 1** From the Operational Mode, issue the **request umts cell disable zone-id** command to disable all cells in a zone. This example disables all cells in zone 3.

```
request umts cell disable zone-id 3
```

**Step 2** Issue the command to verify the configuration:

```
show
```

### 7.9.1.5 Deleting a Cell from a Zone

Delete a cell from a zone by redefining the cells in the zone. Deleting a cell from a SONConfig zone moves it back to the default zone.

## To delete a cell from a zone

**Step 1** From the Configuration Mode, issue the **show FAPService <ServiceNumber> UMTS zone** command to view the existing configuration. This example shows SONScanZone zone 3 contains cells 9, 10, 11, 12, and 13.

```
show FAPService 1 UMTS zone 3
Description Interior;
Type SONScanZone;
CellList "[ 9 10 11 12 13 ]";
```

**Step 2** Issue the **set FAPService <ServiceNUMBER> UMTS Zone** command to re-define the cells in the zone. This example removes cell 13 from the configuration.

```
set FAPService 1 UMTS Zone 3 CellList [ 9 10 11 12 ]
```

**Step 3** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS zone 3
CellList "[ 9 10 11 12 ]";
```

### 7.9.1.6 Moving a Cell to a Different SONConfig Zone

When moving a cell from one SONConfig zone to another, Follow these procedures:

- Disable the cell as shown in [Section 5.4, Disabling and Enabling Cell Transmission](#) on page 91.
- Delete it from its current zone as shown in [Section 7.9.1.5, Deleting a Cell from a Zone](#) on page 130.
- Add the cell to a new zone as shown in [Section 7.9.1.2, Adding a Cell to a Zone](#) on page 130.
- Enable the cell as shown in [Section 5.4, Disabling and Enabling Cell Transmission](#) on page 91.

Disabling and re-enabling the cell is not required if the cell is moved within a single commit cycle. Cells cannot be moved between zones if either zone is in REM scan mode.

### 7.9.1.7 Creating a UMTS Zone Reference Neighborhood List

You can create a list of all external macro cells detected by one or more small cell solution cells in a given zone during a REM scan or manually added to the list. The system compares this list with the detected external macro neighbors detected in subsequent REM scans.

If an external macro cell is not in the zone reference neighborhood list but is detected in the REM scan, the system sends a *NEIGHBORHOOD\_CELL\_UNEXPECTED* event. Similarly, if an external macro cell is in the zone reference neighborhood list but is not detected in the REM scan, the system sends a *NEIGHBORHOOD\_CELL\_MISSING* event. In both cases, the system raises a *NEIGHBORHOOD\_REFERENCE\_DELTA* alarm. The alarm clears if all the unexpected external macro cells disappear and all the missing external macro cells re-appear in a subsequent REM scan which raises a *NEIGHBORHOOD\_REFERENCE\_MISMATCH\_REMOVED* event. If you believe that the external macro cell has been added or permanently removed as a neighbor, you can delete the reference neighborhood list and create a new one.

## To create a UMTS zone reference neighborhood list

**Step 1** From the Operational Mode, issue the following command to create a reference neighborhood list for all zones. This example creates the list for zone 2.

```
request umts zone referenceneighborhood set zoneid 2
```

### 7.9.1.8 Deleting a UMTS Zone Reference Neighborhood List

You can delete the reference neighborhood for a specific zone. If no zone is specified it deletes the reference neighborhood list for the default zone.

To delete a UMTS zone reference neighborhood list

**Step 1** From the Operational Mode, issue the following command to delete a reference neighborhood list for a zone. This example uses zone 1.

```
request umts zone referenceneighborhood delete zoneid 1
```

#### 7.9.1.9 Deleting a UMTS Zone Detected Neighborhood List

You can delete the detected neighborhood list of a specified zone.

To delete a UMTS zone detected neighborhood list

**Step 1** From the Operational Mode, issue the following command to delete a detected neighborhood list for a zone. This example uses zone 2.

```
request umts zone detectedlist delete-all zoneid
```

#### 7.9.1.10 Deleting a Zone

The default SONConfig zone cannot be deleted. All other zones can be deleted when not in REM scan mode. When a SONConfig zone other than the default zone is deleted, all of its cells are moved to the default zone and all detected cells in that exist only in that zone are deleted from the neighbor lists. Its reference list is also deleted.

To delete a zone

**Step 1** From the Configuration Mode, issue the **show FAPService <ServiceNumber> UMTS Zone** command to view the existing configuration:

```
show FAPService 1 UMTS Zone
Zone 1 {
    Description Entrances;
    Type SONConfigAndScanZone;
    CellList "[ ]";
    SONScan {
        ScanPeriodically true;
        PeriodicInterval 86400;
    }
}
```

**Step 2** Issue the **delete FAPService 1 UMTS Zone** command to delete the zone. This example deletes zone 1.

```
delete FAPService 1 UMTS Zone 1
```

**Step 3** Issue the **show FAPService <ServiceNumber> UMTS Zone** command to verify the configuration:

```
show FAPService 1 UMTS Zone
No entries found.
```

#### 7.9.1.11 Viewing the Zone Configuration

You can view the configuration of all zones in the system.

To view zone configurations

**Step 1** From the Configuration Mode, issue the **show FAPService <ServiceNumber> UMTS Zone** command to view the configuration of all zones in the system:

```
show FAPService 1 UMTS Zone
Zone 1 {
    Type SONScan;
    CellList "[ 323 28 ]";
    SONConfig {
        NeighborList {
```

```

        NeighborListLockEnable false;
    }
    SelfConfig {
        PrimaryScramblingCodeLockEnable false;
        MaxFAPTxPower           -101;
        MaxFAPTxPowerLockEnable false;
        RFLockEnable             false;
    }
    Coverage {
        FAPCoverageTargetMinBase      -900;
        FAPCoverageTargetValue1       50;
        PeriodicTxPwrRefresh        false;
        PeriodicTxPwrRefreshInterval 86400;
        PeriodicTxPwrRefreshTime     1970-01-04T00:00:00Z;
    }
}
SONScan {
    UMTSExtIntraFreqREMScanEnable true;
    UMTSExtInterFreqREMScanEnable true;
    GSMREMScanEnable             true;
    InternalTopologyDiscoveryEnable true;
    ScanPeriodically             false;
    PeriodicInterval              86400;
    PeriodicTime                  1970-01-04T00:00:00Z;
    WCDMAFDD {
        UARFCNDLLList "[ 10600 10800 ]";
    }
    GSM {
        REMBandList "[ E-GSM900 ]";
        ARFCNList   "[ 26 28 ]";
    }
}
[output truncated]

```

### 7.9.1.12 Viewing the Default SONConfigAndScan Zone

You can view the default SONConfigAndScan zone.

**Step 2** From the Operational Mode, issue the following command to view the default SONConfigAndScan zone configuration:

```
show RFMgmt UMTS Configuration DefaultZone
```

```
Default-Zone of Type SONConfigAndScanZone:
=====
Default-Zone Config. Param's:
.....
RF Lock                      false
Neighbor List Lock            false
PSC Lock                     false
Max FAP Tx Power Lock        false
```

Primary Scrambling Code	[ "33..35" ]
Alternate Primary Scrambling Code	[ ]
Max FAP Tx Power	-100..240
FAP Coverage Target Min Base	-900
FAP Coverage Target Value 1	50
Periodic Tx Power Refresh	true
Periodic Tx Power Refresh Interval	480
Periodic Tx Power Refresh Time	-
 Default-Zone REM Scan Param's:	
UMTS Ext InterRAT REM Scan	false
UMTS Ext IntraFreq REM Scan	true
UMTS Ext InterFreq REM Scan	true
UMTS Int IntraFreq REM Scan	true
 Scan Periodically	false
Periodic Interval	300
Periodic Time	1970-01-04T00:00:00Z
 WCDMAFDD:	
DL UARFCN List	[ 10600 10800 ]
 GSM:	
REM Band List	[ "E-GSM900" ]
ARFCN List	[ "26" ]
REM Scan Status	REMStatusIdle

### 7.9.1.13 Executing a REM Scan on a Zone

A REM scan must be executed on a per-zone basis. You can run a REM scan on multiple zones concurrently as long as none of the affected cells are in more than one zone.



**Note** Running REM scans on multiple SONScan zones simultaneously potentially decreases the accuracy of the resulting neighbor lists. Obtain best results by running simultaneous REM scans on zones where none of the cells can execute a soft handover to any cells in the other zone.

A cell begins its REM scan activities when any of its zones begin a REM scan. All zone parameters are locked during a REM scan and cannot be changed until the scan has completed.



**Note** The Cisco small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

A REM scan updates the UMTS and GSM detected neighbor list for each zone. Since a cell may be in more than one zone and each zone may scan the same UMTS and GSM channels, the same internal or external cell might be detected by the same cell in multiple zones and appear on multiple neighbor lists.

The **request umts rem start** command runs a REM scan on the default zone. To run a REM scan on one or more specific zones, issue the **request umts rem start zone <ZoneID>** command. For example, **request umts rem start zone 2,4,5** initiates a REM scan on zones 2, 4, and 5. Set the parameters for a zone REM scan with the **set FAPService 1 UMTS Zone** command to **true** before issuing the **request umts rem start** command:

- **GsmREMScanEnable:** enables a GSM scan.

- **UMTSExtInterFreqREMScanEnable**: enables a UMTS inter-frequency scan.
- **UMTSExtIntraFreqREMScanEnable**: enables a UMTS intra-frequency scan.
- **InternalTopologyDiscoveryEnable**: enables an internal topology scan.

To execute a REM scan on the default zone

- Step 1** From the Operational Mode, issue the following command to start a REM scan on the default zone. Note that no zone number is provided, the REM scan initiates on the default zone 0, which can be specified but is not required. Therefore the two following commands are identical in behavior.

```
request umts rem start zones
request umts rem start zones 0
```

To execute a REM scan on defined zones

- Step 1** From the Operational Mode, issue the **request umts rem start zone <ZoneID>** command to start a REM scan on one or more zones. This example initiates a REM scan on zones 2, 4, and 5.

```
request umts rem start zones 2,4,5
```

#### 7.9.1.14 Assigning Cell Transmit Power Levels to a Zone

You can assign transmit power levels to a subset of cells by assigning them to a separate SONConfig zone. For example, you might assign exterior-facing cells a lower transmit power levels than interior cells for more consistent powering to provide more evenly distributed coverage.

To assign transmit power levels to cells in a zone

- Step 1** From the Configuration Mode, issue the command to assign transmit power levels to a cell zone. In this example, cells 1 2 3 4 are in zone 2 and are assigned to transmit power level 150.

```
request umts self-config tx-power-assignment ue-measurement-based zoneid 2
```

#### 7.9.1.15 Configuring Maximum Cell Transmit Power in a Zone

You can configure the maximum cell transmit power of all cells in a zone either through the methods shown in [Section 7.6.1, Configuring the Maximum UMTS Cell Transmit Power](#) on page 114 or [Section 7.6.2, Configuring Location-Based Power Allocation](#) on page 114.

To configure maximum cell transmit power in a zone

- Step 1** From the Operational Mode, issue the **request umts self-config tx-power-assignment max-power** command to update the cell power assignments to the maximum allowable power. This example configures zone 1.

```
request umts self-config tx-power-assignment max-power zoneid 1
```

To configure location-based initial power allocation in a zone

- Step 1** From the Configuration Mode, issue the following command to add a cell to a zone. This example adds cell 1 to SONConfig zone 2.

```
set FAPService 1 UMTS Zone 2 Type SONConfigAndScanZone CellList [ 1 ]
```

- Step 2** Issue the show **FAPService <ServiceNumber> UMTS Zone** command to verify the configuration:

```
show FAPService 1 UMTS Zone
Zone 2 {
    Type          SONConfigAndScanZone;
    CellList     "[ 1 ]";
}
```

}

- Step 3** Issue the `set cell <Number> LocationType` command to set the location type of the new cell. This example modifies cell 1 in small cell 2 and locates the cell in a meeting room named *Meeting\_Room2*.

```
set Cell 1 Enable true LocationType [ MeetingRoom ] Description Meeting_Room2 RadioNode 2
```

- Step 4** Issue the `commit` command to commit the changes:

```
commit
```

- Step 5** From the Operational Mode, issue the following command to apply location-based maximum power assignments to zone 2:

```
request umts self-config tx-power-assignment location-type-based
```

- Step 6** Issue the following command to verify the configuration. Note the cell was assigned the maximum power of 20 dBm (200 units of 0.1 dBm)

show Cell UMTS							
CellHandle	Name	RN	CID	UCID	PSC	MaxTxPwr	ModeInUse
2	Meeting_Room2	2	1	66191771	114	20.0dBm	UMTSNodeB

## 7.9.2 Locking Cells in a Zone

This section discusses zone-wide attribute locking during REM scan for cells that are not in the default SONConfig zone. The behavior of cells in the default SONConfig zone during REM scanning is described in [Section 7.8.10, UMTS REM Scan Locking](#) on page 124.

You can lock the attributes, including primary scrambling code, maximum transmit power level, and neighbor lists, for all cells in a SONConfig zone such that a REM scan detects the topology but takes no action to reconfigure the specific attributes of the system. These RF attributes can be manually configured at a later date if needed.

Alternatively, you can lock the individual attributes for all cells in a SONConfig zone during a REM scan such that the locked attributes retain their values but the unlocked attributes will be reconfigured after the scan using the new topological information. Locked cells and attributes cannot be modified. Unlock the cell or attribute to make changes to it.

Locking is hierarchical, when an attribute is locked from the zone level, all cells in the zone have that attribute locked during REM scans until it is unlocked. Similarly, when one or more attributes are locked for a specified zone, they remain locked for that zone until they are unlocked.

For an individual cell:

- the primary scrambling code is locked in a zone when:
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig RFLockEnable true`
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig PrimaryScramblingCodeLockEnable true`
- the maximum transmit power is locked in a zone when:
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig RFLockEnable true`
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig MaxFAPTxPowerLockEnable true`
- the neighbor list is locked in a zone when:
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig RFLockEnable true`
  - `FAPService 1 UMTS Zone <ZoneID> SONConfig SelfConfig NeighborList NeighborListLockEnable true`

### 7.9.2.1 Locking Zone-Wide Cell RF Attributes During REM Scan

Locking all cell attributes in a SONConfig zone prevents changes to the primary scrambling code, maximum power level, and neighbor list of all cells in a SONConfig zone. These attributes remain locked during REM scans until unlocked on a zone or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system, zone, or cell as needed.

To lock all RF attributes during REM scanning for all cells in a zone

**Step 1** From the Configuration Mode, issue the following command to lock the cell RF attributes during REM scanning for all cells in a zone. This example locks cells in zone 1.

```
set FAPService 1 UMTS Zone 1 SONConfig SelfConfig RFLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone 1 SONConfig SelfConfig RFLockEnable  
RFLockEnable true;
```

### 7.9.2.2 Locking Zone-Wide Primary Scrambling Codes

You can prevent a REM scan from changing the primary scrambling codes of all cells in a SONConfig zone. These attributes remain locked during REM scans until unlocked on a zone-wide or individual cell basis. To change any of these primary scrambling codes, unlock the system or individual cell and make the changes. You can then re-lock the zone or cell as needed.

To lock primary scrambling codes for all cells

**Step 1** From the Configuration Mode, issue the following command to lock all primary scrambling codes in a zone. This example locks cells in zone 2.

```
set FAPService 1 UMTS Zone 2 SONConfig SelfConfig PrimaryScramblingCodeLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone 2 SONConfig SelfConfig PrimaryScramblingCodeLockEnable  
PrimaryScramblingCodeLockEnable true;
```

### 7.9.2.3 Locking Zone-Wide Maximum Power Transmission Levels

You can prevent a REM scan from changing the maximum power transmission level of all cells in a SONConfig zone. These attributes remain locked during REM scans until unlocked on a zone-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the zone or cell as needed.

To lock maximum power transmission levels for all cells

**Step 1** From the Configuration Mode, issue the following command to lock all maximum power transmission level in a zone. This example locks cells in zone 3.

```
set FAPService 1 UMTS Zone 3 SONConfig SelfConfig MaxFAPTxPowerLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone 3 SONConfig SelfConfig MaxFAPTxPowerLockEnable  
MaxFAPTxPowerLockEnable true;
```

### 7.9.2.4 Locking Zone-Wide Neighbor Lists

You can prevent a REM scan from changing the neighbor list of all cells in the in a SONConfig zone. These attributes remain locked during REM scans until unlocked on a zone-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the zone or cell as needed.

To lock neighbor lists of all cells

**Step 1** From the Configuration Mode, issue the following command to lock all neighbor lists a zone. This example locks cells in zone 4.

```
set FAPService 1 UMTS Zone 4 SONConfig NeighborList NeighborListLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone 4 SONConfig NeighborList NeighborListLockEnable
NeighborListLockEnable true;
```

### 7.9.3 Alternative RF Management Scenarios

In almost all cases, RF management will be deployed as previously described. However, there are scenarios where alternative deployments are more effective. For example:

- turning up a multi-building campus
- providing services while performing RF management

These types of deployments can be managed more efficiently by segregating cells into zones for the purposes of RF management.

#### 7.9.3.1 Turning up a Multi-Building Campus

In a campus setting it can be logically easier to turn up services one building at a time. For this procedure, each building must be separated by at least 100 meters (325 feet) so that no cells from any building can discover any cells another building. Otherwise the general radio environment is similar across the campus. For this purpose we create a SONConfig zone for each building.

Follow these high-level steps to turn up a multi-building campus. This example uses two buildings: A and B.

To turn up a multi-building campus

**Step 1** From the Configuration Mode, issue the `set FAPService <ServiceNumber> UMTS Zone` command to create a zone. This example creates SONConfig zone 1, containing cells 11, 12, 13, and 14, named *Building\_A*, with a pool of primary scrambling codes 300 through 310.

```
set FAPService 1 UMTS Zone 1 Type SONConfigAndScanZone CellList [ 11 12 13 14 15 ]
Description Building_A SONConfig SelfConfig PrimaryScramblingCode [300..310 ]
```

**Step 2** The following command enables intra-frequency, inter-frequency, and GSM scanning and internal topology discovery and disables periodic scanning:

```
set FAPService 1 UMTS Zone 11 Type SONConfigAndScanZone SONScan
UMTSExtIntraFreqREMScanEnable true UMTSExtInterFreqREMScanEnable true GSMREMScanEnable
true InternalTopologyDiscoveryEnable true ScanPeriodically false
```

**Step 3** Issue the `show FAPService <ServiceNumber> UMTS Zone` command to verify the configuration:

```
show FAPService 1 UMTS Zone Type SONConfigAndScanZone
Zone 1 {
    Description Building_A;
    Type SONConfigAndScanZone;
    CellList "[ 11 12 13 14 15 ]";
    SONConfig {
        SelfConfig {
            PrimaryScramblingCode
                "[ 300..310 ]";
        }
    }
}
```

**Step 4** From the Operational Mode, issue the `request umts rem start zones` command to run a REM scan on building A.

```
request umts rem start zones 1
```

**Step 5** Configure building B in a similar manner using zone 2 and a different set of cells. Then run a REM scan on building B after the REM scan on zone 1 has completed.

**Step 6** Commit the configuration:

**Commit**

**Step 7** From the Operational Mode, run the following command to verify the configuration:

```
show RFMgmt UMTS Configuration Zone ID 1
```

Zone 2 of Type SONConfigZone:

```
=====
```

Zone Description

Zone Cell List [ 11 12 13 14 15 ]

Zone 2 Config. Param's:

```
.....
```

RF Lock	false
Neighbor List Lock	false
PSC Lock	false
Max FAP Tx Power Lock	false

Primary Scrambling Code	[ "300..310" ]
Alternate Primary Scrambling Code	[ ]
Max FAP Tx Power	200

FAP Coverage Target Min Base	-900
FAP Coverage Target Value 1	50

Periodic Tx Power Refresh	false
Periodic Tx Power Refresh Interval	86400
Periodic Tx Power Refresh Time	1970-01-04T00:00:00Z

Zone 2 Scan Param's:

```
.....
```

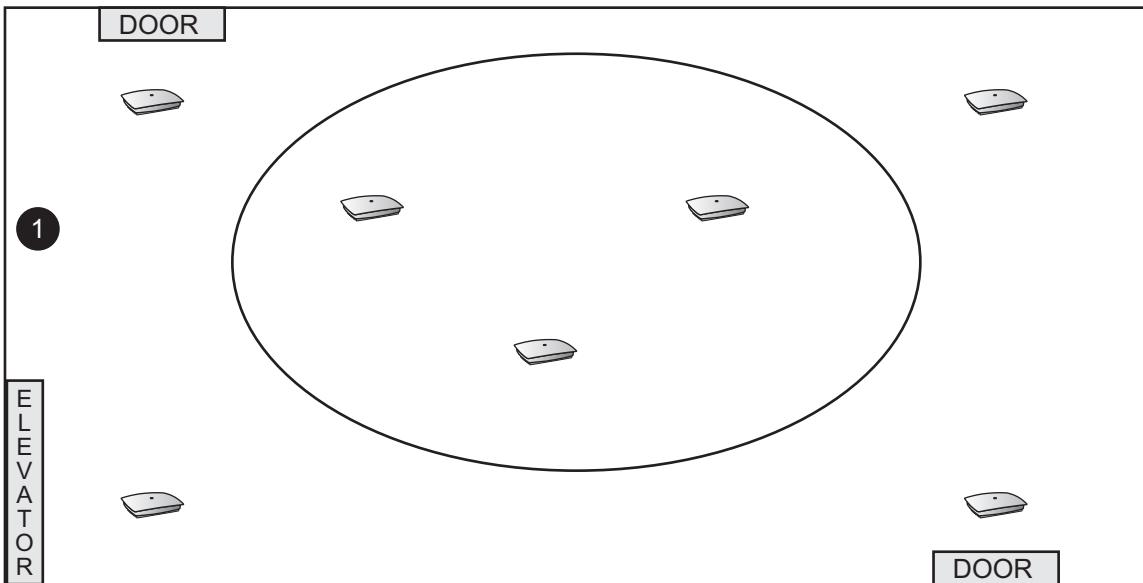
UMTS Ext InterRAT REM Scan	true
UMTS Ext IntraFreq REM Scan	true
UMTS Ext InterFreq REM Scan	true
UMTS Int IntraFreq REM Scan	true

Scan Periodically	false
Periodic Interval	240

REM Scan Status	REMStatusIdle
-----------------	---------------

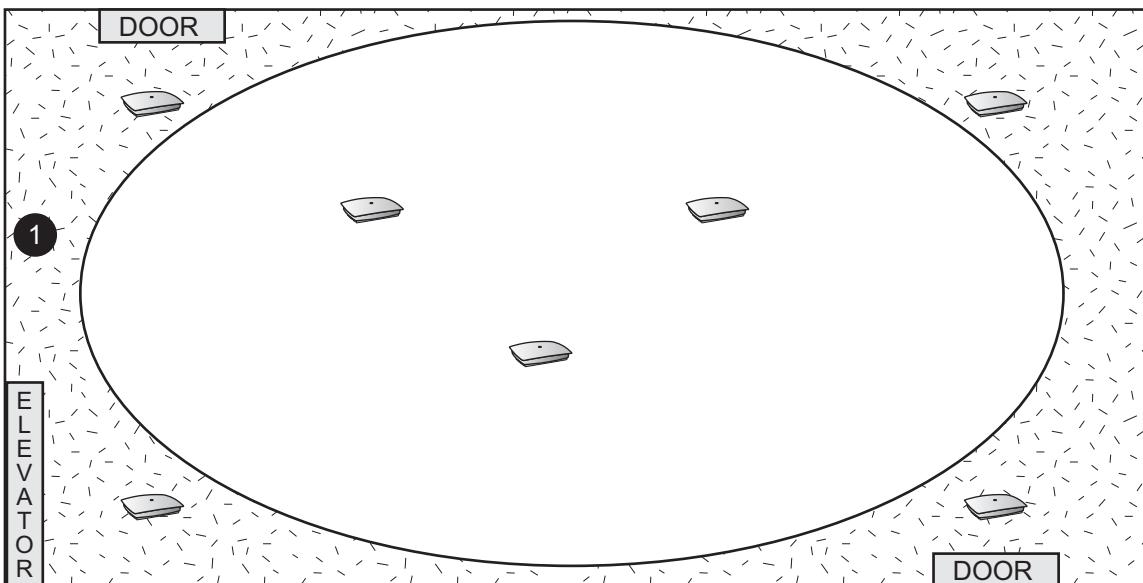
### 7.9.3.2 Initiating Fast Scanning for Changes in the External RF Environment

Figure 30 shows a work area with all cells in the default SONConfig zone 0. The four small cells in the corners are perimeter small cells that interact and/or external GSM neighbors. They are in SONScan zone 1. The three interior small cells that have little contact with external neighbors are not in a SONScan zone. During normal operation the system offers complete coverage of the work area:



**Figure 30** Small Cell Solution Coverage During Normal Operation

**Figure 31** shows the same work area during a REM scan for external GSM neighbors on SONScan zone 1. The interior small cells are not in REM scan mode and provide cell coverage while the exterior small cells are not scanning for changes in the external network for a short duration.



**Figure 31** Small Cell Solution Coverage During REM Scan



Note

The small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

## To run a GSM/UMTS REM scan on a subset of cells

**Step 1** From the Configuration Mode, issue the following command to enable REM scanning on a subset of zones. This example enables zone 1 REM scanning for GSM neighbors. It disables scanning intra-frequency and inter-frequency neighbors.

```
set FAPService 1 UMTS Zone 1 Type SONScanZone CellList [ 1 2 3 4 ] SONScan GSMREMScanEnable
true UMTSExtInterFreqREMScanEnable false UMTSExtIntraFreqREMScanEnable false
InternalTopologyDiscoveryEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone
Zone 1 {
    Type          SONScanZone;
    CellList     "[ 1 2 3 4 ]";
    SONScan {
        UMTSExtIntraFreqREMScanEnable   false;
        UMTSExtInterFreqREMScanEnable  false;
        GSMREMScanEnable              true;
        InternalTopologyDiscoveryEnable true;
    }
}
```

**Step 3** Issue the following command to start a REM scan:

```
request umts rem start
```

**Step 4** (Optional) Configure periodic REM scanning. Refer to [Section 7.5.1, Configuring Basic and Periodic Scanning Parameters](#) on page 109.

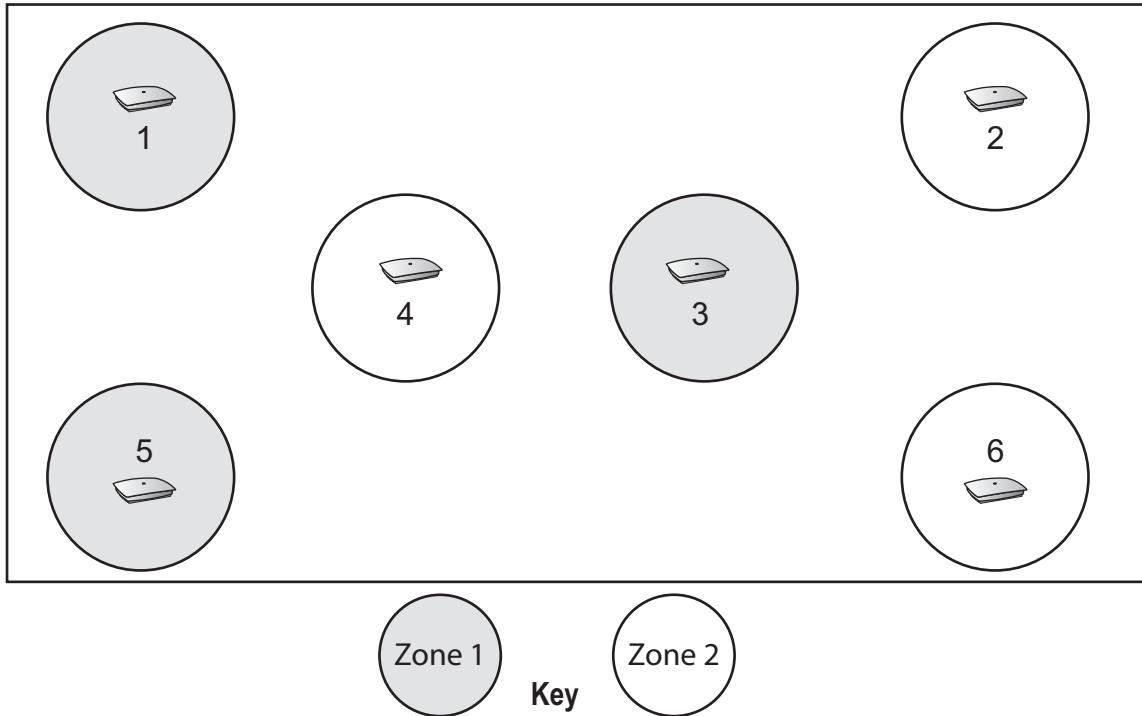
### 7.9.3.3 Detecting Changes in the GSM Environment

To detect changes in the GSM environment during a short REM scanning maintenance window, you can split the list of bands to scan into multiple SONScan zones and run multiple scans at the same time. Parallel scanning is much faster than a complete REM scan. In this scenario you create zones with interspersed cells for a representative topological sampling and enable only GSM scanning during the REM scan.



The small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

In the configuration example below, odd numbered cells are placed in SONScan zone 1, represented by grey circles in [Figure 32](#). Even numbered cells are placed in zone 2, represented by clear circles.



**Figure 32** SONScan Zones 1 and 2

To detect changes in the GSM environment

**Step 1** From the Configuration Mode, issue the following command to place selected cells in a SONScan zone. This example places cells, 1, 3, and 5 in SONScan zone 1.

```
set FAPService 1 UMTS Zone 1 Type SONScanZone CellList [ 1 3 5 ]
```

**Step 2** Issue the following command to define the zone 1 GSM band and frequency to scan. This example sets the GSM band to *GSM850* and the frequency between 128 and 256 inclusive.

```
set FAPService 1 UMTS Zone 1 SONScan GSM REMBandList [ GSM850 ] ARFCNList  
[ 128..256 ]
```

**Step 3** Issue the following command to disable all other REM scan activities other than GSM scanning in zone 1:

```
set FAPService 1 UMTS Zone 1 SONScan UMTSExtIntraFreqREMScanEnable false  
UMTSExtInterFreqREMScanEnable false InternalTopologyDiscoveryEnable false
```

**Step 4** Issue the following command to create a second SONScan zone. This example places cells 2, 4, and 6 in SONScan zone 2.

```
set FAPService 1 UMTS Zone 2 Type SONScanZone CellList [ 2 4 6 ]
```

**Step 5** Issue the following command to define the zone 2 GSM band and frequency to scan. This example sets the GSM band to *PCS1900* and the frequency between 512 and 600 inclusive.

```
set FAPService 1 UMTS Zone 2 SONScan GSM REMBandList [ PCS1900 ] ARFCNList [512..600]
```

**Step 6** Issue the following command to disable all other REM scan activities other than GSM scanning in zone 2:

```
set FAPService 1 UMTS Zone 2 SONScan UMTSExtIntraFreqREMScanEnable false
UMTSExtInterFreqREMScanEnable false InternalTopologyDiscoveryEnable false
```

**Step 7** Issue the following command to verify the configuration:

```
show FAPService 1 UMTS Zone
Zone 1 {
    Type          SONScanZone;
    CellList     "[ 1 3 5 ]";
    SONScan {
        UMTSExtIntraFreqREMScanEnable  false;
        UMTSExtInterFreqREMScanEnable  false;
        GSMREMScanEnable             true;
        InternalTopologyDiscoveryEnable false;
        GSM {
            REMBandList "[ GSM850 ]";
            ARFCNList   "[ 128..256 ]";
        }
    }
}
Zone 2 {
    Type          SONScanZone;
    CellList     "[ 2 4 6 ]";
    SONScan {
        UMTSExtIntraFreqREMScanEnable  false;
        UMTSExtInterFreqREMScanEnable  false;
        GSMREMScanEnable             true;
        InternalTopologyDiscoveryEnable false;
        GSM {
            REMBandList "[ PCS1900 ]";
            ARFCNList   "[ 512..600 ]";
        }
    }
}
```

**Step 8** Commit the configuration

```
commit
```

**Step 9** From the Operational Mode, issue the following command to trigger a REM scan simultaneously on zones 1 and 2:

```
request umts rem start zones 1,2
```

**Step 10** Issue the following commands to save reference neighborhoods of zones 1 and 2:

```
run request umts zone referenceneighborhood set zoneid 1
```

```
run request umts zone referenceneighborhood set zoneid 2
```

**Step 11** From the Configuration Mode, issue the following commands to configure periodic REM scans at midnight GMT every day on zones 1 and 2:

```
set FAPService 1 UMTS Zone 1 SONScan ScanPeriodically true PeriodicInterval 86400
PeriodicTime 1970-01-04T00:00:00Z
```

```
set FAPService 1 UMTS Zone 2 SONScan ScanPeriodically true PeriodicInterval 86400
PeriodicTime 1970-01-04T00:00:00Z
```

**Step 12** Commit the configuration

```
commit
```

**Step 13** View the alarm and event lists to determine whether any new cells have been added or are missing from the reference neighbor list. Search for the *NEIGHBORHOOD\_REFERENCE\_DELTA* alarm that indicates the neighborhood has changed. The *NEIGHBORHOOD\_CELL\_UNEXPECTED* event indicates a newly detected cell. The *NEIGHBORHOOD\_CELL\_MISSING* event indicates a missing cell. From the Operational Mode, issue the following commands:

```
show System Alarm  
show System Event
```

**Step 14** Issue the following commands to update the reference neighborhoods of zones 1 and 2:

```
run request umts zone referenceneighborhood set zoneid 1  
run request umts zone referenceneighborhood set zoneid 2
```

**Step 15** Issue the following command to trigger a REM scan on the default zone to enable all cells to find their new neighbors:

```
request umts rem start
```



## 8 LTE RF Management

LTE RF management includes discovering the macro cells in the area, discovering the internal topology, assigning Physical Cell IDs (PCIs), and configuring cell neighbor lists to make the system operational. The goal of RF management is to configure and administer a collection of installed small cells after basic objects have been entered into the system. It intelligently configures the system from an RF perspective by determining the external and internal topologies by establishing:

- which other small cells can each small cell hear in the network.
- which macro cells can each small cell hear, and on which LTE channels.

The system gathers this information from a Radio Environment Measurement (REM) scan process where it scans the radio environment to discover its topology. After the network is operational, the system can periodically re-scan to detect topology changes and use historical data to optimize the system and improve performance.

When a small cell is powered on, it attempts to locate the controller it is physically cabled to. If successful, both nodes exchange information. When you enable auto provisioning, the controller additionally creates small cell, radio, and cell objects representing the small cell and its components in the Cisco small cell network.

After a REM scan, RF management assumes administration of the controller to maximize efficiency among the cells. Once the network is ready for operation and all cells have been provisioned, the administrator initiates a scan to discover the latest internal and external topology configurations. Thereafter, a new scan may be initiated manually.

This chapter contains the following sections:

- [Section 8.1, LTE RF Management Configuration Overview](#) on page 145
- [Section 8.2, Initial System Provisioning with the LCI](#) on page 146
- [Section 8.3, Before You Begin](#) on page 146
- [Section 8.4, Initial LTE RF Management Provisioning](#) on page 146
- [Section 8.5, Basic LTE REM Scanning](#) on page 147
- [Section 8.6, LTE Cell Transmit Power](#) on page 149
- [Section 8.7, Viewing LTE RF Management Configurations](#) on page 150
- [Section 8.8, Advanced RF Management](#) on page 152
- [Section 8.9, Centrally-Coordinated Dynamic Fractional Frequency Reuse](#) on page 157

### 8.1 LTE RF Management Configuration Overview

Provisioning the system with the CLI involves configuring the initial RF management, then providing ongoing maintenance to fine-tune the system. The initial stage consists of running the first REM scan and reviewing the results. You may then re-provisioning neighbors.

Once the system is functioning, ongoing RF maintenance starts with additional REM scans to detect topology changes. These operational REM scans can be configured to automatically make changes to the system, or you can lock one or more attributes in the system or individual cells and view the results to identify the changes to the system topology. You can later unlock locked attributes and make changes to the configuration.

## 8.2 Initial System Provisioning with the LCI

If the controller received initial system provisioning with the Local Configuration Interface (LCI) it may have already had an initial REM scan and has system-wide topological knowledge and assigned primary scrambling codes and physical cell IDs. If your system has already had an initial REM scan through the LCI, many of the next sections are not applicable. Proceed to [Section 8.5.3, Initial LTE Self-Configuration](#) on page 148. Refer to the *Cisco USC 8000 Series System Commissioning Guide* for more information about configuring the system with the LCI.

## 8.3 Before You Begin

The E-UTRA absolute radio frequency channel number in both the downlink and uplink directions must be configured before RF management can be enabled. Refer to [Section 6.2, Configuring LTE Femto Access Point Service](#) on page 103.

To verify the channel number

**Step 1** From the Configuration Mode, verify that the channel number has been configured:

```
show FAPService 1 CellConfig LTE RAN
RF {
    EARFCNDL          3100;
    EARFCNUL          21100;
```

## 8.4 Initial LTE RF Management Provisioning

Initial LTE RF management procedures involve enabling RF management and placing controllers in service.

### 8.4.1 Enabling LTE RF Management

RF management must be enabled before self-configuration services can operate.

**Step 1** From the Configuration Mode, enable RF management:

```
set FAPService 1 FAPControl LTE SelfConfig NeighborListSelfConfigEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE SelfConfig NeighborListSelfConfigEnable
NeighborListSelfConfigEnable true;
```

### 8.4.2 Placing the USC 8088 Controller In Service

Operators performing initial system provisioning with the LCI can activate the controller to the point where it is ready to operate but is in maintenance mode and the small cells will not transmit. The controller must be placed in-service from within the provider core network.

To place a controller in service

**Step 1** From the Configuration Mode, issue the `set System OperatingMode InService` command to change the controller primary state from maintenance to in-service:

```
set System OperatingMode InService
```

## 8.5 Basic LTE REM Scanning

REM scans survey the small cell solution and adjacent provider macro network to provide a detailed topological map of configured inter-frequency channels and the deployment channel to optimize the wireless environment. The Cisco small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

A REM scan detects the topology. It then takes the information from the latest scan and combines it with the historical measurements from user equipment to update the topology and neighbor lists. Depending upon the size of the deployment, this process can take tens of minutes.

### 8.5.1 Configuring Basic Scanning Parameters

When performing a REM scan, the system always scans the deployment E-UTRA absolute radio frequency channels in both the downlink and uplink directions defined in [Section 6.2, Configuring LTE Femto Access Point Service](#) on page 103. The following example configures:

- The REM scan of the environment and updates the cell neighbor lists and the Physical Cell ID (PCI) assignments.
- Additional channels used by the controller to scan for external neighbors. These channels typically correspond to channels used by the macro network. Note that the system scans:
  - the deployment channel that is configured at the **set FAPService <ServiceNumber> CellConfig LTE RAN FDDFAP RF** hierarchy level.
  - the LTE channels specified with the **set FAPService <ServiceNumber> REM LTE EUTRACarrierARFCNDLList** command.
  - the UMTS channels specified with the **set FAPService 1 REM WCDMAFDD UARFCNDLList command**.
  - the GSM channels specified with the **set FAPService <ServiceNumber> REM GSM** command.

LTE bands and channels that should be used by the controller to scan for external neighbors. Valid bands and channels depend on the LTE band deployment. [Table 19](#) shows the LTE bands that each LTE radio can scan:

**Table 19: Radio Bands Scanned**

Small Cell Model	LTE	UMTS Monitor	GSM Monitor
SCRN310-0701	2600/1800/800 MHz	2100/900 MHz	900/1800 MHz
SCRN310-0402	2100/700 MHz	2100/1900/850 MHz	850/1900 MHz

To configure basic scanning parameters

- Step 1** From the Configuration Mode, configure the channels to scan for neighbors. This example initiates scan of channel.

```
set FAPService 1 REM WCDMAFDD UARFCNDLList [ 2350 2062 1962 ]
```

- Step 2** Configure the channels to scan for neighbors. This example initiates a scan of channels 2350, 2062, and 1962.

```
set FAPService 1 REM LTE EUTRACarrierARFCNDLList [ 2350 2062 1962 ]
```

- Step 3** Issue the **show FAPService <ServiceNumber> REM LTE** command to verify the configuration:

```
show FAPService 1 REM LTE
EUTRACarrierARFCNDLList "[ 2350 2062 1962 ]";
```

## 8.5.2 Configuring Physical Cell IDs

Through REM scan operations, the controller discovers, maintains, and updates a topological state of the external and internal networks that includes a list of all detected physical cell IDs and corresponding measured signal strengths. After internal topology discovery, the system assigns each cell a physical cell IDs. The system intelligently assigns physical cell IDs to cells, reusing the same physical cell IDs as rarely and spread apart as possible.

### 8.5.2.1 Designating Physical Cell IDs for the small cell solution

The administrator must designate the set of allowable physical cell IDs that the system can assign to cells in the network. Designate a range by defining the lower and upper integers (in that order) separated by two periods (...). Designate two non-contiguous ranges by separating the ranges with a space. Valid options are integers from 0 through 503.

To configure the set of physical cell IDs for the small cell solution

**Step 1** From the Configuration Mode, configure the set of physical cell IDs for use in the system. This example uses physical cell IDs 100 through 120 and 200 through 220.

```
set FAPService 1 CellConfig LTE RAN FDDFAP RF PhyCellID [ 100..120 200..220 ]
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN FDDFAP RF PhyCellID  
PhyCellID "[ 100..120 200..220 ]";
```

## 8.5.3 Initial LTE Self-Configuration

Once the LTE RF management parameters have been configured and all cells are in service, issue the **request lte rem start** command from the Operational Mode to discover the topology, assign the physical cell IDs, and to construct the neighbor lists for all individual cells. After initially running this command, you can issue it again as needed.



The small cell network carries no user voice or data traffic during a REM scan. Therefore, Cisco Systems recommends performing REM scans only during a regular maintenance window.

Note that accurate topology discovery requires that the small cells have settled local oscillators. Issue the **show RadioNode** command to ensure that all small cells are in the IS-NORMAL state. The system will reject the **request lte rem start** command unless all small cells are in the IS-NORMAL state.

## 8.5.4 Aborting an LTE REM Scan

You can manually stop a running LTE REM scan that you do not want to complete. For example, if you notice that the configuration is incorrect while the scan is in progress, rather than waiting for the scan to complete, you can abort the scan, change the configuration, and start a new scan. Aborting a REM scan will revert the system to the last known state.

To abort an LTE REM scan

**Step 1** From the Operational Mode, issue the **request lte rem stop** command to manually abort a running LTE REM scan:

```
request lte rem stop
```

## 8.6 LTE Cell Transmit Power

RF management allows you to configure the maximum LTE cell transmit power for all LTE cells in the system or an individual cell. Cell transmit powers are defined in terms of reference signal power. The ratio between the reference signal power and the maximum cell transmit power is fixed, for a given LTE bandwidth. [Table 20](#) shows the mapping between the reference signal power and total transmit power for supported LTE bandwidths:

**Table 20: Reference Signal and Total Transmit Power Mapping**

Bandwidth	Total Transmit Power/ Reference Signal Power
3 MHz	22.6 dB
5 MHz	24.8 dB
10 MHz	27.8 dB
15 MHz	29.5 dB
20 MHz	30.8 dB

The total transmit power = the reference signal power plus the value from [Table 20](#). For example, for a 10MHz bandwidth cell with reference signal power of -10dBm: Total transmit power = -10 + 27.8 = 17.8dBm.

Once the maximum transmit power has been configured, Cisco recommends limiting the difference in transmit power of adjacent cells.



RF management transmit power allocation commands cannot be run during a REM scan.

### Note

### 8.6.1 Configuring the Maximum LTE Cell Transmit Power for all Cells

To configure the maximum LTE cell transmit power for all cells

**Step 1** From the Operational Mode, issue the `request lte self-config tx-power-assignment max-power` command to update the cell power assignments to the maximum allowable power:

```
request lte self-config tx-power-assignment max-power
```

### 8.6.2 Configuring the Transmit Power for an Individual Cell

You can override the system-wide LTE transmit power for an individual cell by configuring the reference signal power manually.

To configure the maximum LTE cell transmit power for an individual cell

**Step 1** From the Configuration Mode, issue the following command to set the transmit power for an individual cell. The example sets the transmit power for cell to 11 and the reference signal power to -7.0 dBm (7 units of 0.1 dBm) for a 20 MHz LTE band.

```
set LTECell 11 CellConfig LTE RAN rf ReferenceSignalPowerConfigured -7
```

**Step 2** Issue the following command to verify the configuration:

```
show LTECell 11 CellConfig LTE RAN rf ReferenceSignalPowerConfigured
ReferenceSignalPowerConfigured -7;
```

### 8.6.3 Configuring REM Scan-Based LTE Power Assignments

You can configure LTE cell power assignments based upon the results of a REM scan. Refer to [Section 8.5.3, Initial LTE Self-Configuration](#) on page 148 for information about initiating a REM scan.

To configure LTE cell power assignments based upon REM scan results

**Step 1** From the Operational mode, issue the following command to set LTE cell power assignments based upon a REM scan:

```
request lte self-config tx-power-assignment rem-based
```

## 8.7 Viewing LTE RF Management Configurations

This section discusses how to view the RF management configuration and REM scan results.

### 8.7.1 Viewing the LTE RF Management Configuration

Before fine-tuning the system after the initial REM scan, view the current RF management configuration.

To view the current LTE RF management configuration

**Step 1** From the Operational Mode, issue the **show RFMgmt LTE Configuration** command to view the current configuration space before running the REM scan:

```
show RFMgmt LTE Configuration
Scan Config Params:
-----
Neighbor List Self-Config. Enable          true
LTE IntraFreq Scan Enable                 true
LTE InterFreq Scan Enable                true
UMTS Scan Enable                         true
Internal Topology Scan Enable            true
Require Freq. Stability For Topo. Disc. false

LTE:
  EARFCNDL List                          [ 2350 2062 1962 ]
  REM Scan Status                         REMStatusIdle

Config. Param's:
-----
RF Lock                                false
Neighbor List Lock                      false
PCI Lock                               false
Root Sequence Lock                     false

Physical Cell ID                        [ "0..503" ]

FAPService Provisioned External LTE Neighbors:
-----
Index  Enable  Inclusion Mode  EARFCN  PCI  PLMNID  CID  Blacklisted  CIO  Qoffset  RSTxPower  RSRP
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
1      true    MustInclude   0       0     001012  1     false        0     0        -128      -95
2      true    MustInclude   0       0     -       1     false        0     0        -128      -95

FAPService Provisioned External UMTS Neighbors:
-----
Index  Enable  Inclusion Mode  DL UARFCN  PLMNID  RNCID  CID  LAC  RAC  URA  PSC  PCPICHTxPower  CPICH RSCP
-----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
1      true    MustInclude   437     00104    0       1     22103  0     0        0     0        -85
2      true    MustInclude   437     00104    0       2     100     123    0        10    0        -99
```

[output truncated]

## 8.7.2 Viewing LTE REM Scan Results

You can view the results of a REM scan for all detected cells, detected internal LTE cells and cell neighbors.



Issuing the **show RFMgmt LTE NeighborCells** command while a REM scan is active can return inaccurate results. The screen displays the following message:

Note: RF Management is active.

### To view LTE REM scan results

**Step 1** From the Operational Mode, issue the **show RFMgmt LTE MeasurementOfLTECell** command to view internal cells that detected UMTS cells:

**show RFMgmt LTE MeasurementOfLTECell**

Detecting CID	Detected CID	EARFCNDL	PCI	PLMNID	TAC	RSRP
534784	2	2200	10	102	1	-9
534784	3	2200	12	102	1	-9
534784	6	2200	0	102	1	-9
534784	7	2200	4	102	1	-7
534784	335365	2350	0	150	1	-67
534786	0	2200	8	102	1	-7
534786	3	2200	12	102	1	-9
534786	6	2200	0	102	1	-8
534786	7	2200	4	102	1	-10
534786	335365	2350	0	150	1	-6
534787	0	2200	8	102	1	-10

[output truncated]

**Step 2** Issue the **show RFMgmt LTE Configuration** command to view the LTE RF management configuration:

**show RFMgmt LTE Configuration**

Scan Config Params:

```
Neighbor List Self-Config. Enable      true
LTE IntraFreq Scan Enable            true
LTE InterFreq Scan Enable           true
UMTS Scan Enable                   true
Internal Topology Scan Enable       true
Require Freq. Stability For Topo. Disc.  false
```

LTE:

  EARFCNDL List [ 2350 2062 1962 ]

REM Scan Status

  REMStatusIdle

Config. Param's:

```
RF Lock                           false
Neighbor List Lock                false
PCI Lock                          false
Root Sequence Lock               false
```

Physical Cell ID [ "0..503" ]

FAPService Provisioned External LTE Neighbors:

Index	Enable	Inclusion Mode	EARFCN	PCI	PLMNID	CID	Blacklisted	CIO	QOffset	RSTxPower	RSRP
1	true	MustInclude	0	0	001012	1	false	0	0	-128	-95
2	true	MustInclude	0	0	-	1	false	0	0	-128	-95

```
FAPService Provisioned External UMTS Neighbors:
.....
Index  Enable  Inclusion Mode  DL UARFCN  PLMNID  RNCID  CID    LAC    RAC    URA    PSC    PCPICHTxPower  CPICH RSCP
----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
1     true    MustInclude    437      00104    0        1       22103   0        0       0        0        -85
2     true    MustInclude    437      00104    0        2       100      123     0       10       0        -99
[output truncated]
```

## 8.8 Advanced RF Management

Advanced RF management consists of the following tasks:

- [Section 8.8.1, Provisioning LTE Neighbor Lists](#) on page 152
- [Section 8.8.2, Adding or Deleting an LTE Cell from an Operational Network](#) on page 154
- [Section 8.8.3, Excluding a Cell from all small cell solution Neighbor Lists](#) on page 154
- [Section 8.8.4, Creating the Final Neighbor List](#) on page 154
- [Section 8.8.5, Bypassing LTE REM Scan Topology Components](#) on page 155
- [Section 8.8.6, Manually Assigning Physical Cell IDs](#) on page 156
- [Section 8.8.7, LTE REM Scan Locking](#) on page 156

### 8.8.1 Provisioning LTE Neighbor Lists

The small cell network automatically detects LTE, UMTS, and GSM macro network neighbors for each cell on the channels configured for scanning in the **FAPService <ServiceNumber> REM** object. You can optionally manually add up to 32 macro neighbors for a cell for each neighbor type:

- intra-frequency (LTE, co-channel)
- inter-frequency (LTE, not co-channel)
- inter-RAT (GSM and UMTS)

To provision the LTE neighbors in the small cell solution, you must specify:

- the E-UTRA Absolute Radio Frequency Channel Number (EARFCN) for downlink and uplink directions for LTE neighbors
- the UTRA Absolute Radio Frequency Channel Number (UARFCN) for downlink and uplink directions for UMTS neighbors
- the UTRA Radio Frequency Channel Number (UARFCN) for downlink and uplink directions for GSM neighbors

To manually provision cell neighbors

**Step 1** Issue the following command to provision and enable LTE neighbors. This example provisioned:

- LTE cell 2
- physical cell ID 126
- cell ID 52
- PLMN ID 00103

It must include all such neighbors.

```
set FAPService 1 CellConfig LTE RAN NeighborList LTECell 2 Enable true PhyCellID 126 CID
52 PLMNID 00103 InclusionMode MustInclude
```

**Step 2** From the Configuration Mode, provision and enable an intra-RAT UMTS neighbor. This example provisioned:

- the inter-RAT UMTS neighbor index 1
- a cell with the primary scrambling code 125 and cell ID 51
- a PLMN ID 00102,

It must include all such neighbors.

```
set FAPService 1 CellConfig LTE RAN NeighborList InterRATCell UMTS 1 Enable true
PCPICHScramblingCode 125 CID 51 PLMNID 00102 InclusionMode MustInclude
```

**Step 3** Issue the following command to provision and enable GSM neighbors. This example provisions:

- the Base Station Identity Code (BSIC) 5
- the BCCHARFCN 26
- cell ID 10
- band indicator GSM 900

It must include all such neighbors.

```
set FAPService 1 CellConfig LTE RAN NeighborList InterRATCell GSM 1 BSIC 5 BCCHARFCN 26
CI 10 BandIndicator GSM\ 900 Enable true
```

**Step 4** Issue the following command to verify the neighbor list configuration. Note that this command returns only manually provisioned cell neighbors. Refer to [Section 8.7.1, Viewing the LTE RF Management Configuration](#) on page 150 for more information about viewing cell neighbors.

```
show FAPService 1 CellConfig LTE RAN NeighborList
LTECell 2 {
    Enable          true;
    PLMNID         00103;
    CID            52;
    PhyCellID      126;
    InclusionMode  MustInclude;
}
InterRATCell {
    GSM 1 {
        Enable          true;
        BSIC           5;
        CI             10;
        BandIndicator "GSM 900";
        BCCHARFCN     26;
    }
    UMTS 1 {
        Enable          true;
        PLMNID         00102;
        PCPICHScramblingCode 125;
        InclusionMode  MustInclude;
    }
}
```

## 8.8.2 Adding or Deleting an LTE Cell from an Operational Network

To add an LTE cell to the network, add the small cell and the cell to an operational network manually. Once the small cell and corresponding cell is ready, the small cell solution will automatically self-configure it. All other cells in the small cell solution remain operational throughout this process.



When a cell is added to an operational network, the topology discovery of the newly added cell is determined by the external network.

### Note

If a cell is removed from the network, first delete the cell and then the small cell from the configuration. Refer to [Section 6.3.2, Deleting a Small Cell and a Cell](#) on page 106 for more information.

## 8.8.3 Excluding a Cell from all small cell solution Neighbor Lists

If there are particular external cells that appear in an LTE REM scan that you want to ignore, you can define cells that will be excluded from the neighbor list of all cells in the system.

### To exclude a cell from all neighbor lists in the small cell solution

From the Configuration Mode, issue the following command to exclude an LTE cell as a neighbor for all neighbor lists in the system. This list excludes cell **111.set FAPService 1 CellConfig LTE RAN NeighborList LTECell 111 InclusionMode MustExclude Enable true**

**Step 5** Issue the following command to exclude a cell as an intra-RAT UMTS neighbor for all neighbor lists in the system. This list excludes cell 333.

```
set FAPService 1 CellConfig LTE RAN NeighborList InterRATCell UMTS 333 InclusionMode
MustExclude Enable true
```

**Step 6** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN NeighborList
```

## 8.8.4 Creating the Final Neighbor List

After tuning LTE neighbor lists by manually adding or excluding cells, create the final neighbor list by issuing the **request lte self-config neighborlist-create** command. This command combines the neighbor information detected during REM scans with the manually provisioned cell neighbors for the final neighbor lists.

### To create a final LTE neighbor list

**Step 1** From the Operational Mode, issue the following command to create the final neighbor list. This combines the topological information from the REM scan with the manually provisioned neighbor lists.

```
request lte self-config neighborlist-create
```

**Step 2** Issue the **show RFMgmt LTE NeighborCells** command to view the final neighbor list. Note that the CPICH RSCP value of -3276 is invalid and only used when the cell is included as a neighbor of itself.

```
show RFMgmt LTE NeighborCells
```

List Of Neighbors Of Internal Cell with Cell Handle 1 And CellID 1:  
-----

LTE Neighbors:

PLMNID	CID	PCI	EUARFCN	DL Bandwidth	UL Bandwidth	RSRP	Tier
00102	2	10	2200	50	50	-102	1

```

00102      3    12     2200          50          50   -107   1
00102      4    19     2200          50          50   -126   1
00102      5    17     2200          50          50   -116   1
00150  25600    5    2350  4294967295  4294967295   -81   1
00102      1    4     2350  4294967295  4294967295   -95   1

```

**UMTS Neighbors:**

```

=====
PSC  CID     RNCID   DL UARFCN   CPICH  RSCP   Tier
---  ---     -----  ---  -----  -----  ---  ---
100      1      0       437      -85      1
      0      1      0      1891      -85      1
101      2      0       437      -99      1

```

**GSM Neighbors:**

```

=====
BSIC  CI     Frequency Band  ARFCN  RSSI   Tier
---  ---     -----  ---  -----  ---  ---
27   25451      PCS 1900    678    -87      1

```

[output truncated]

## 8.8.5 Bypassing LTE REM Scan Topology Components

You can configure which parts of the topology are scanned. For example, if the internal topology functions properly, you can save time by scanning only for intra-frequency and inter-frequency neighbors. A topological REM scan can be subdivided by enabling or disabling the following components:

- **LTEExtIntraFreqREMScanEnable:** external LTE intra-frequency neighbor cells
- **LTEExtInterFreqREMScanEnable:** external LTE inter-frequency neighbor cells
- **UMTSREMScanEnable:** external UMTS neighbor cells
- **InternalTopologyDiscoveryEnable:** Cisco internal cells

To configure REM scan topological parameters

- Step 1** From the Configuration Mode, issue the following commands to configure the external LTE intra-frequency neighbor component of the REM scan. This example enables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig UMTSExtIntraFreqREMScanEnable true
set FAPService 1 FAPControl LTE SelfConfig LTEExtIntraFreqREMScanEnable true
```

- Step 2** Issue the following command to configure the external LTE inter-frequency neighbor component of the REM scan. This example disables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig UMTSExtInterFreqREMScanEnable false
set FAPService 1 FAPControl LTE SelfConfig LTEExtInterFreqREMScanEnable false
```

- Step 3** Issue the following commands to configure the external UMTS neighbor component of the REM scan. This example enables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig GSMREMScanEnable true
set FAPService 1 FAPControl LTE SelfConfig UMTSREMScanEnable true
```

- Step 4** Issue the following commands to configure the Cisco internal neighbor component of the REM scan. This example disables scanning of these cells.

```
set FAPService 1 FAPControl UMTS SelfConfig InternalTopologyDiscoveryEnable false
set FAPService 1 FAPControl LTE SelfConfig InternalTopologyDiscoveryEnable false
```

- Step 5** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE SelfConfig
LTEExtIntraFreqREMScanEnable      true;
LTEExtInterFreqREMScanEnable      false;
UMTSREMScanEnable                true;
InternalTopologyDiscoveryEnable  false;
```

## 8.8.6 Manually Assigning Physical Cell IDs



Neighbor cells are a combination of detected and provisioned cells.

### Note

You can manually assign a cell a specific physical cell IDs. Valid options are *0* through *503*.

To assign a cell a physical cell ID

**Step 1** From the Configuration Mode, issue the following command to assign a cell a physical cell ID. This example assigns cell 22 the physical cell ID 101,

```
set cell 22 CellConfig LTE RAN RF PhyCellIDConfigured 101
```

**Step 2** Issue the following command to verify the configuration:

```
show LTECell 22 CellConfig LTE RAN RF PhyCellIDConfigured
PhyCellIDConfigured 101;
```

## 8.8.7 LTE REM Scan Locking

You can lock the attributes, including physical cell ID and neighbor lists, for all cells in the small cell solution such that a REM scan detects the topology but takes no action to reconfigure the specific attributes of the system or cells. These RF attributes can be manually configured at a later date if needed.

Alternatively, you can lock the individual attributes for all cells during a REM scan such that the locked attributes retain their values but the unlocked attributes will be reconfigured after the scan using the new topological information. Locked cells and attributes cannot be modified. Unlock the cell or attribute to make changes to it.

Locking is hierarchical, when an attribute is locked from the system (FAPService) level, all cells in the system have that attribute locked during REM scans until it is unlocked.

For an individual cell:

- the physical cell ID is locked when:
  - **FAPService 1 FAPControl LTE SelfConfig PhyCellIDLockEnable true**
- the neighbor list is locked when:
  - **FAPService 1 FAPControl LTE SelfConfig NeighborListLockEnable true**

### 8.8.7.1 Locking System-Wide LTE Cell RF Attributes During REM Scan

Locking system-wide cell attributes (FAPService) prevents changes to the physical cell IDs and neighbor list of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

To lock all RF attributes during LTE REM scanning for all cells

**Step 1** From the Configuration Mode, issue the following command to lock the cell RF attributes during REM scanning for all cells in the small cell solution.

```
set FAPService 1 FAPControl LTE SelfConfig RFLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE SelfConfig RFLockEnable
RFLockEnable true;
```

#### 8.8.7.2 Locking System-Wide Physical Cell IDs

You can prevent a REM scan from changing the physical cell IDs of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide. To change any of these physical cell IDs, unlock the system and make the changes. You can then re-lock the system as needed.

To lock physical cell IDs for all cells

**Step 1** From the Configuration Mode, issue the following command to lock all physical cell IDs in the system:

```
set FAPService 1 FAPControl LTE SelfConfig PhyCellIDLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE SelfConfig PhyCellIDLockEnable
PhyCellIDLockEnable true;
```

#### 8.8.7.3 Locking System-Wide LTE Neighbor Lists

You can prevent a REM scan from changing the neighbor list of all cells in the system. These attributes remain locked during REM scans until unlocked on a system-wide or individual cell basis. To change any of these parameters, unlock the system or individual cell and make the changes. You can then re-lock the system or cell as needed.

To lock neighbor lists of all cells

**Step 1** From the Configuration Mode, issue the following command to lock all neighbor lists in the system:

```
set FAPService 1 FAPControl LTE SelfConfig NeighborListLockEnable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE SelfConfig NeighborListLockEnable
NeighborListLockEnable true;
```

## 8.9 Centrally-Coordinated Dynamic Fractional Frequency Reuse

Fractional Frequency Reuse (FFR) is an Inter-Cell Interference Coordination (ICIC) technique well-suited for Orthogonal Frequency-Division Multiple Access (OFDMA) based wireless networks wherein cells can be partitioned into segments with different frequency reuse factors. FFR can help mitigate inter-cell interference by allocating dedicated frequency sub-bands to cell edge users, while assigning the entire available bandwidth to cell center users.

The controller continuously monitors network-wide interference and varying traffic loads and centrally coordinates FFR across all small cells in the building, to optimize cell-edge performance and improve overall spectral efficiency. This ensures reliable mobility within the small cell solution coverage area and minimizes interference at the cell-edge, improving cell-edge throughput and overall system spectral efficiency. Cisco's controller-based architecture enables

operators to deploy scalable, dense LTE small cell networks and realize the benefits of ICIC.

FFR is enabled separately for downlink and uplink connections. It is disabled in both directions by default. FFR offers the following functionalities:

- The controller centrally coordinates Radio Environment Monitoring (REM) as part of the SON functionality and maintains up-to-date Radio Frequency (RF) topology information for the small cell solution.
- The controller combines RF topology with small cell resource availability and traffic load variation to allocate frequency resources to each small cell.
- Frequency resource allocation for downlink and uplink channels is adapted periodically and an updated FFR pattern for each cell is communicated from the controller to the small cells.
- The FFR pattern includes frequency allocations for cell-edge and cell-center regions for the cell.
- Each small cell independently schedules uplink and downlink transmissions in the allocated sub-bands for cell-center and cell-edge users.

There are three modes of FFR:

- **Disabled:** disables FFR, cells configured with entire system bandwidth as cell center region
- **Dynamic:** enables dynamic FFR, cells dynamically configured with cell center and cell edge regions
- **Static:** enables static FFR, cells statically configured with cell center and cell edge regions

Changes to the FFR mode are dynamic. They take effect immediately without impact to active sessions without requiring a reboot of the controller.

### To enable fractional frequency reuse scheduling

**Step 1** From the Configuration Mode, issue the following command to enable FFR scheduling in the downlink and uplink connections. This example enables *Dynamic* downlink and uplink FFR.

```
set FAPService 1 CellConfig LTE RAN MAC Scheduling DLFFRMode Dynamic ULFFRMode Dynamic
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN MAC Scheduling
DLFFRMode Dynamic;
ULFFRMode Dynamic;
```



## 9 LTE Zones

### 9.1 Creating an LTE Zone

LTE zones facilitate configuration of LTE cells. It allows simultaneous setting of common parameters, such as bandwidth, for all cells in a zone. New cells added to an existing zone are automatically assigned these common parameters.

Specify the downlink and uplink channel bandwidth by specifying the bandwidth in Resource Blocks (RBs). Uplink and downlink bandwidths must be identical. Table 5.6-1. [Table 21](#) shows the mapping between resource blocks and frequency.

**Table 21: Resource Block to Frequency Mapping**

Resource Block #	MHz
6	1.4
15	3
25	5
50	10
75	15
100	20

To create an LTE zone

**Step 1** From the Configuration Mode, issue the following command to create an LTE zone. This example:

- creates an LTE zone number 1 as a configuration zone
- includes cells 1, 2, 3, and 4
- sets the following parameters: downlink EARFCN 2200, uplink EARFCN 20200, downlink bandwidth 50 resource blocks, uplink bandwidth to 50 resource blocks, primary synchronization channel power offset 0 dB, secondary synchronization channel power offset to 0 dB, and the physical broadcast channel power offset to 0 dB

```
set FAPService 1 LTE Zone 1 Type ConfigZone CellList [ 1 2 3 4 ] Config RAN RF EARFCNDL
2200 EARFCNUL 20200 DLBandwidth 50 ULBandwidth 50 PSCHPowerOffset 0 SSCHPowerOffset 0
PBCHPowerOffset 0
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 LTE Zone 1
Type          ConfigZone;
CellList      "[ 1 2 3 4 ]";
Config {
    RAN {
        RF {
```

```
    EARFCNDL      2200;
    EARFCNUL     20200;
    DLBandwidth   50;
    ULBandwidth   50;
    PSCHPowerOffset 0;
    SSCHPowerOffset 0;
    PBCHPowerOffset 0;
}
}
}
```



# 10 Access Control Topics

Access control is an integral part of the Cisco small cell network. It provides administrators the ability to differentiate service offerings to system users based on their identities.

Access is configured based on the IMSI of the device. In a cellular system, the IMSI is uniquely tied to the user, is authenticated, and cannot be spoofed. Therefore the IMSI provides a secure means to configure access management without certificates, client-side software, or user intervention.

The IMSI can then be assigned to a Policy, which is a collection of rules that specify how data traffic should be handled by the controller. A policy can include rules such as:

- whether the traffic for a device should be sent directly to the provider core network or is locally switched
- which Class of Service (CoS) to use
- whether traffic shaping should be enforced

Policy settings are more fully explained in [Section 12.2, Configuring Policies](#) on page 178.

This chapter contains the following sections:

- [Section 10.1, Open Subscriber Groups](#) on page 161
- [Section 10.2, Closed Subscriber Groups](#) on page 161
- [Section 10.3, UMTS Admission Control](#) on page 166
- [Section 10.4, LTE Admission Control](#) on page 168

## 10.1 Open Subscriber Groups

In the open subscriber group configuration, access is permitted to all users. User authentication is deferred to the provider core network. This is equivalent to the operational mode of a macro cell deployed by the network operator, and is the default mode of operation for the Cisco network.

However, unlike the conventional macro network where all user treatment is effectively identical, the Cisco small cell network can be configured with multiple service classes. Even with open subscriber groups, each service class can be treated with different service differentiation and prioritization.

The Cisco small cell network is configured for open subscriber groups by default. Refer to [Section 12.5, User Configuration Examples](#) on page 186 for information about configuring service classes.

## 10.2 Closed Subscriber Groups

The closed subscriber group feature allows the small cell solution to service a limited number of authorized users without affecting the services of other users that are rejected and forced to use the provider macro network. The feature assumes that the small cell solution is deployed with a unique Location Area Code and Routing Area Code or physical cell ID that is different from the ones used in the provider macro network.

This difference in Location Area Code and Routing Area Code or physical cell ID between the small cell solution and the core network causes all UE to perform a location update and routing area update upon entering the network coverage area. All unauthorized users will be rejected by the small cell solution, at which point they will fall back to the provider macro network.



The closed subscriber group feature should not be used if the small cell solution is deployed in the same frequency or UMTS/LTE channel as the macro network, if the small cell solution does not have a unique Location Area Code or physical cell ID from the macro network, or if

macro network coverage is not available to perform the redirect.

At a high level, the system will reject a user whose IMSI has not been entered onto the whitelist of authorized IMSIs by trapping Non-Access Stratum (NAS) layer registration messages and sending the appropriate NAS-layer reject messages. The macro network is not involved in this process. As a consequence, the UE will add the Location Area Code or physical cell ID to its list of forbidden location areas and will not attempt to use any small cell solution cell until the mobile device is power-cycled.

Use the *Action* parameter of the Policy configuration object to enable a closed subscriber group. The system enables the Closed Subscriber Group by pointing the *UnknownUEPolicyIndex* to a Policy whose action is set to reject. Refer to [Section 12.2, Configuring Policies](#) on page 178 for more information about policies.

To create a closed subscriber group

**Step 1** From the Configuration Mode, create and enable Policy 1 that rejects users from the system:

```
set FAPService 1 AccessMgmt Policy 1 Enable true Action Reject
```

**Step 2** Create and enable Policy group 1 with Policy 1:

```
set FAPService 1 AccessMgmt PolicyGroup 1 Enable true PolicyIndexList [ 1 ]
```

**Step 3** Assign unknown users to Policy group 1:

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 1
```

**Step 4** Create and enable Policy 2 that allows users on the system:

```
set FAPService 1 AccessMgmt Policy 2 Enable true Action Accept
```

**Step 5** Create and enable Policy group 2 with Policy 2:

```
set FAPService 1 AccessMgmt PolicyGroup 2 Enable true PolicyIndexList [ 2 ]
```

**Step 6** Create member 1, define an IMSI, and assign it to a Policy. This example uses IMSI 001010123456873, user name *Kim\_Lee*, and assign it to Policy 2 to route traffic through the small cell solution.

```
set FAPService 1 AccessMgmt MemberDetail 1 Enable true IMSI 001010123456873 Username Kim_Lee PolicyGroupIndex 2
```

**Step 7** Create member 2, define an IMSI, and assign it to a Policy. This example uses IMSI 001010123456875, user name *Robin\_Lang*, and assign it to Policy 2 to route traffic through the small cell solution.

```
set FAPService 1 AccessMgmt MemberDetail 2 Enable true IMSI 001010123456875 Username Robin_Lang PolicyGroupIndex 2
```

**Step 8** Issue the following command to enable IMSI identity requests verification:

```
set FAPService 1 AccessMgmt IMSIIdentityRequestEnable true LTE IMSIIdentityRequestEnable true
```

**Step 9** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 1;
IMSIIdentityRequestEnable true;
MemberDetail 1 {
```

```

        Enable          true;
        IMSI           001010123456873;
        PolicyGroupIndex 2;
        Username        Kim_Lee;
    }
MemberDetail 2 {
    Enable          true;
    IMSI           001010123456875;
    PolicyGroupIndex 2;
    Username        Robin_Lang;
}
LTE {
    MaxUEsServed      60;
    IMSIIdentityRequestEnable true;
PolicyGroup 1 {
    Enable          true;
    PolicyIndexList "[ 1 ]";
}
PolicyGroup 2 {
    Enable          true;
    PolicyIndexList "[ 2 ]";
}
Policy 1 {
    Enable          true;
    Action          Reject;
}
Policy 2 {
    Enable          true;
    Action          Accept;
}

```

### 10.2.1 Adding Users through the Web Interface

The controller has a web interface for users to add themselves to the enterprise whitelist in a closed subscriber group configuration so they can access the enterprise network resources on their UE devices. The enterprise administrator provides each user the IP address of the controller web server. The user then opens that address with the Secure Socket Layer (SSL) protocol in a browser of their UE device, and enters their AAA user name and password.

All user maintenance, such as adding users, deleting users, and changing passwords, is the responsibility of the enterprise administrator and is handled through the enterprise AAA RADIUS (RFC 2865 and RFC 5176) system.

A Policy is a collection of settings that fully specify how data traffic is classified and managed. Before users can enroll in local switching in a closed user group configuration, the administrator must define separate Policies for unknown and authorized users:

- One Policy directs unknown users to the provider macro network for all sessions except browser sessions directed to the IP address of the controller web server. Those sessions are routed to the self-enrollment screen where users can authenticate by entering their AAA user name and password. Successful enrollment enables local switching and will route their traffic to the enterprise LAN.
- The second Policy configures local switching.

#### Before You Begin

Before you can add users through the web interface, be sure the following criteria are met:

- The enterprise server must support dynamic user revocation/update as defined in RFC 5176.

- Each user on the server must be configured with the appropriate PolicyGroup index, using the Vendor-Specific Attribute 1 (Vendor-specific Company Code 36707).
- The enterprise server must be configured with the service node web server IP address and port number.
- The user must know their AAA user name and password pair.
- The local switching policies must be configured for authorized and unknown users.

To configure enrollment policies

**Step 1** From the Configuration Mode, enter the **set System WebManagement** command to enable the web interface:

```
set System WebManagement Service 2 Enable true LocalPort 49152 Protocol
HTTPS ServiceType Enrollment LocalCertIndex 1
```

**Step 2** Enter the **show System WebManagement** command to verify the configuration:

```
show System WebManagement
Enable true;
Service 1 {
    Enable      true;
    LocalPort   443;
    Protocol    HTTPS;
    ServiceType LCI;
    LocalCertIndex 1;
}
Service 2 {
    Enable      true;
    LocalPort   49152;
    Protocol    HTTPS;
    ServiceType Enrollment;
    LocalCertIndex 1;
}
```

**Step 3** Create and enable a Policy that sets the switching mode to local switching for authorized users. In this example, Policy 3 sets local data switching in the *NAPT* mode to IP interface 1 on Ethernet port 1.

```
set FAPService 1 AccessMgmt Policy 3 Description Local_switching Enable true SwitchingMode
NAPT PrimaryLANDevice 1 PrimaryIPInterface 1
```

**Step 4** Create and enable Policy group 3 with Policy 3:

```
set FAPService 1 AccessMgmt PolicyGroup 3 Enable true PolicyIndexList [ 3 ]
```

**Step 5** Create and enable a Policy that sets the switching mode for local switching only for enrollment in the closed subscriber group. In this example, Policy 100 sets local data switching only for enrollment in the closed subscriber group in the *Enrollment-NAPT* mode to IP interface 1 on Ethernet port 1.

```
set FAPService 1 AccessMgmt Policy 100 Description Enrollment_only Enable true
SwitchingMode Enrollment-NAPT PrimaryLANDevice 1 PrimaryIPInterface 1
```

**Step 6** Create and enable a user Policy group that applies Policy 100 to users so that they can be routed on the LAN for enrollment:

```
set FAPService 1 AccessMgmt PolicyGroup 100 Enable true PolicyIndexList [ 100 ]
```

**Step 7** Assign PolicyGroup 100 to unknown users so that they can be routed on the LAN for enrollment:

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 100
```

**Step 8** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 100;
PolicyGroup 3 {
    Enable      true;
    PolicyIndexList "[ 3 ]";
```

```

}
PolicyGroup 100 {
    Enable          true;
    PolicyIndexList "[ 100 ]";
}
Policy 3 {
    Enable          true;
    Description    Local_switching;
    SwitchingMode NAPT;
}
Policy 100 {
    Enable          true;
    Description    Enrollment_only;
    SwitchingMode Enrollment-NAPT;
}

```

**Step 9** Set and enable the enrollment method for local switching by defining the type of authentication, defining the associated parameters. In this example, the authentication is *RADIUS*, using controller web server with the IP address 10.10.10.8 port 443, the RADIUS server with the IP address 10.50.10.5, RADIUS port 1812, a secret of *radius-secret*, with a timeout after 3, and 4 retry attempts.

```
set FAPService 1 AccessMgmt Enrollment Web AAAServerType RADIUS Server 10.10.10.8 Port 443 RADIUS Server 10.50.10.5 Port 1812 Secret radius-secret Retry 3 Timeout 4
```

**Step 10** Issue the **set FAPService 1 AccessMgmt Enrollment DynamicAuth RADIUS Secret <secret>** command to set the secret for the RADIUS server. This secret must match the secret set in the step above.

```
set FAPService 1 AccessMgmt Enrollment DynamicAuth RADIUS Secret radius-secret
```

**Step 11** Issue the **show FAPService <ServiceNumber> AccessMgmt Enrollment** command to verify the configuration. Note that after a configuration commit, the RADIUS secret output is obfuscated.

```
show FAPService 1 AccessMgmt Enrollment
Enable true;
Web {
    AAAServerType RADIUS;
    Server      10.10.10.8;
    Port        443;
    RADIUS {
        Server  10.50.10.5;
        Port    1812;
        Secret  $obf$/38L/zQuXVJcJV0JfAZKUEopWw==;
        Timeout 4;
        Retry   3;
    }
}
DynamicAuth {
    RADIUS {
        Secret $obf$NJpgR6KIPCsUDidFZjorKQICJg==;
    }
}
```

---

The closed subscriber group must be properly configured before users can be added through the GUI.


**Note**

To add a user through the web interface

**Step 1** Enter the controller IP address into your browser address bar and press **Enter**. Be sure to use the Secure Socket Layer (SSL) protocol by entering **https://** before the IP address. The user self-enrollment screen displays.

**Step 2** Enter the AAA user name and password.

**Step 3** Click **submit**. A confirmation message displays.

## 10.3 UMTS Admission Control

UMTS admission control prevents resource overload by provisioning rules that selectively restrict access to only a defined set of users to improve the service quality of those users of the system. Implemented by the controller and enforced by individual small cells, admission control policies give priority to the following traffic types in decreasing priority:

- Registration
- Emergency
- Voice
- Data

The priority is configurable through the CLI, and optionally can be applied to prioritize authorized users over guest users. Additionally you can configure policies to reduce the chance of existing sessions dropping when handed over to small cells under heavy traffic loads.

Each small cell supports up to 15 concurrent sessions. Registration sessions, such as location updates and GMM attach events are always allowed and can use the small cell's 16th channel. A small cell will always accept emergency calls unless it is already supporting 15 emergency calls.

The resource constraint is handled differently for mobility events and session establishment:

- A configurable number of UMTS channels on each small cell can be set aside for use for mobility events. This ensures that sessions that have already been admitted through other small cells are less likely to get dropped during a handover to a loaded small cell.
- If downlink resources are not available on the primary scrambling code, the dedicated downlink will be configured on the secondary scrambling codes.

If resources are not available on the small cell during mobility or call establishment, a prioritization table is referenced for identifying the user session to be dropped. [Table 22](#) shows the default prioritization table where a lower number assigns a higher priority:

**Table 22: UMTS Admission Control Priority Matrix**

Parameter	Range	Default
Emergency	0,0	0
Voice	1, 65535	65533
HSDPA	1, 65535	65534
HSUPA	1, 65535	65534
R99Data	1, 65535	65535

Sessions carrying multiple types of traffic (multi-RAB sessions) with different priorities are always assigned the highest of those priorities.

If a small cell is at capacity and a user cannot gain resources to initiate a new voice session, the user will be handed over to the provider macro network if available. Otherwise, the call will be dropped.

The *AdmissionPriorityGroup* entity specifies session priorities. You can configure multiple *AdmissionPriorityGroup* entities, each defining a particular admission priority class. One or more policies can then refer to each such *AdmissionPriorityGroup*.

### To configure UMTS admission control policies

**Step 1** From the Configuration Mode, enable admission control and configure the global mobility link reservation default (3 in this example). This serves as the default for the cell-specific value when a new cell is created. If the configuration changes, all cells will be reprovisioned. As a result all sessions will be cleared.

```
set FAPService 1 AccessMgmt AdmissionControl Enable true MobilityLinkReservation 3
```

**Step 2** Configure the mobility link reservation for a single cell (in this example, cell 259). This represents the number of radio links that are reserved for mobility events (in this example 4) and determines the threshold beyond which sessions initiated at the small cell will either not be allowed or result in congestion mitigation. Changing this value does not affect existing sessions. The updated mobility link reservation will be used for the next session initiation or mobility event.

```
set Cell 259 AccessMgmt AdmissionControl MobilityLinkReservation 4
```

**Step 3** Configure an admission priority group (in this example, *Engineering\_users*). A separate unknown user admission priority group can be configured which is referenced by the Policy that maps to unknown users.

```
set FAPService 1 AccessMgmt AdmissionPriorityGroup 1 Enable true Description
Engineering_users Emergency 0 Voice 1 HSDPA 2 HSUPA 2 R99Data 3
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt AdmissionPriorityGroup
AdmissionPriorityGroup 1 {
    Enable      true;
    Description Engineering_users;
    Emergency   0;
    Voice       1;
    HSDPA      2;
    HSUPA      2;
    R99Data    3;
}
```

**Step 5** Create and enable Policy 6 and assign it to admission priority group 1. This example names the Policy *Engineering* and accepts the UE.

```
set FAPService 1 AccessMgmt Policy 6 AdmissionPriorityGroupIndex 1 Enable true Description
Engineering Action Accept
```

**Step 6** Create and enable a Policy group with Policy 6. This example names it *Engineering\_group*.

```
set FAPService 1 AccessMgmt PolicyGroup 6 Enable true Description Engineering_group
PolicyIndexList [ 6 ]
```

**Step 7** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt
PolicyGroup 6 {
    Enable          true;
    Description    Engineering_group;
    PolicyIndexList "[ 6 ]";
}
Policy 6 {
    Enable          true;
    Description    Engineering;
    Action          Accept;
    AdmissionPriorityGroupIndex 1;
```

**Step 8** Apply the Policy group to a specific UE by specifying the IMSI (in this example 123456789101001).

To apply the Policy to all unknown users, go to [Step 10](#).

```
set FAPService 1 AccessMgmt MemberDetail 1 IMSI 123456789101001 PolicyGroupIndex 6 Enable
true
```

**Step 9** Issue the `show FAPService <ServiceNumber> AccessMgmt MemberDetail` command to verify the configuration:

```
show FAPService 1 AccessMgmt MemberDetail
MemberDetail 1 {
    Enable          true;
    IMSI           123456789101001;
    PolicyGroupIndex 6;
}
```

**Step 10** Apply the Policy group to unknown users:

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 6
```

**Step 11** Issue the `show FAPService <ServiceNumber> AccessMgmt UnknownUEPolicyGroupIndex` command to verify the configuration:

```
show FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex
UnknownUEPolicyGroupIndex 6;
```

## 10.4 LTE Admission Control

LTE admission control defines the number of UE on a cell and configures emergency call priorities.

### 10.4.1 Configuring the Maximum Number of UEs LTE Per-Cell

You can configure the maximum number of UEs allowed on LTE cells in the system. The setting is global and not configurable on a per-cell basis. The default value is 64.

To configure the maximum number of UEs per LTE cell

**Step 1** From the Configuration Mode, issue the following command to limit the number of UEs permitted on each LTE cell in the system. This example sets the limit to 60.

```
set FAPService 1 AccessMgmt LTE MaxUEsServed 60
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt LTE MaxUEsServed
MaxUEsServed 60;
```

## 10.4.2 Configuring the LTE Emergency Priority Level

You can assign a priority level from 1 through 14 for determining emergency call status based on the priority level specified in RAB assignment request. Emergency calls typically have the value 1, but this number is configurable by the mobile provider. The value 0 indicates that the reported priority level is not used to determine emergency call status.

If the priority level is set to 0, the system will not be able to assign emergency call status to calls which are reported by the mobile core network to be emergency calls based on the priority level. The system will continue to assign emergency call status based on the establishment cause regardless of the configured priority level.

To configure the system emergency priority level

- Step 1** From the Configuration Mode, issue the following command to set the system emergency priority level.  
This example sets the level to 1.

```
set FAPService 1 AccessMgmt LTE EmergencyPriorityLevel 1
```

- Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt LTE EmergencyPriorityLevel  
EmergencyPriorityLevel 1;
```





# 11 Regulatory Features

- [Section 11.1, Configuring Emergency Calls on page 171](#)
- [Section 11.2, Configuring ACCOLC on page 172](#)
- [Section 11.3, LTE Public Warning Systems on page 173](#)
- [Section 11.4, Restricting LTE Cell Access on page 174](#)
- [Section 11.5, Configuring UMTS Cell Broadcast Services on page 175](#)

## 11.1 Configuring Emergency Calls

The small cell system supports defining the location of each small cell in the RAN. This location is relayed to responders in an emergency situation. Refer to [Section 3.5.2, Small Cell Location on page 36](#) for information about the small cell location. The system also supports emergency call redirect to the mobile provider core network.

### 11.1.1 Emergency Call Redirect

#### 11.1.1.1 Redirecting Emergency Call Traffic

You can redirect all emergency calls to the mobile provider UTMS or GSM macro network. The emergency call is transferred to the macro network through RRC redirection (with a RRC Connection Reject message) or a hard handover attempt (if the RRC redirection fails). The system will suspend reporting location information to the mobile provider during the emergency call unless the handover fails.

If the device reattempts an emergency call on the small cell network within 30 seconds after an RRC redirection attempt, the RRC redirection is considered to have failed and the small cell system will set up the radio bearer and then attempt a measurement based hard handover. If both RRC redirection and hard handover attempt fail, the emergency call will be handled by the small cell network and location information will be reported.

To redirect emergency calls to the provider UTMS network

**Step 1** From the Configuration Mode, issue the following command to redirect emergency calls with an RRC connection reject from the Cisco small cell network to the mobile provider UMTS network. To later disable the redirection of emergency call from the small cell network, issue the command with the *OffloadEnabled false* attribute. By default the RRC redirection will be to the provider UMTS network if the UMTS neighbor information is present. Otherwise redirection will be to the GSM network.

```
set FAPService 1 AccessMgmt EmergencyCall OffloadEnabled true
```

To redirect emergency calls to the provider GSM network

**Step 1** From the Configuration Mode, issue the following command to redirect emergency calls from the small cell network to the mobile provider GSM network through an RRC connection reject message. To change the RRC redirect default target back to the UMTS network, issue the command with the *GSMRedirectPreferred false* attribute.

```
set FAPService 1 AccessMgmt EmergencyCall GSMRedirectPreferred true
```

### 11.1.1.2 Assigning Emergency Call Priority Levels

You can assign a priority level from 1 through 14 for determining emergency call status based on the priority level specified in RAB assignment request. Emergency calls typically have the value 1, but this number is configurable by the mobile provider. The value 0 indicates that the reported priority level is not used to determine emergency call status.

If the priority level is set to 0, the OS will not be able to assign emergency call status to calls which are reported by the mobile core network to be emergency calls based on the priority level. The OS will continue to assign emergency call status based on the establishment cause regardless of the configured priority level.

#### To assign emergency call priority levels

**Step 1** From the Configuration Mode, issue the following command to assign a priority level to emergency calls. This example uses priority 1.

```
set FAPService 1 AccessMgmt EmergencyCall CNPriorityLevel 1
```

## 11.2 Configuring ACCOLC

The OS supports Access Overload Control (ACCOLC) functionality. ACCOLC is a UMTS access control mechanism to ensure that public safety and emergency authorities have priority access to the cellular network in times of emergency. Typically police departments are the only authority permitted to invoke ACCOLC, which is implemented on a local level, usually in a small geographic area. In 2009 ACCOLC was replaced by MTPAS (Mobile Telecommunication Privileged Access Scheme).

All regular user devices are assigned to one of ten randomly allocated group classes. This designation is stored in the device SIM/USIM. A separate group of five classes is reserved for mobile operator staff, emergency services, public utilities, and security services. The following list defines the classes and their increasing priority:

- Class 0-9 - Ordinary users
- Class 10 - Emergency calls
- Class 11 - PLMN use
- Class 12 - Security services
- Class 13 - Public utilities (such as water/gas suppliers)
- Class 14 - Emergency services
- Class 15 - PLMN staff

In an emergency situation, the relevant authorities contact the mobile provider NOC and request MTPAS activation in a specific geographical area. Cells adjacent to the incident are identified and MTPAS is implemented on those cells while other cells operate normally. High priority UE are allowed access to the network.

#### To activate emergency call restriction

**Step 1** From the Configuration Mode, enter the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellRestriction** command to define the group classes to restrict access to the circuit- and packet-switched domains of cellular network. This example restricts access to group classes 1 through 5 on both the circuit and packet-switched domains.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellRestriction AccessClassBarredListCS [ 1 2 3 4 5 ] AccessClassBarredListPS [ 1 2 3 4 5 ]
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellRestriction
AccessClassBarredListCS "[ 1 2 3 4 5 ]";
AccessClassBarredListPS "[ 1 2 3 4 5 ]";
```

To deactivate emergency call restriction

**Step 1** From the Configuration Mode, enter the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellRestriction** command restore access to all users to the circuit- and packet-switched domains of the cellular network. This example restores access on both the circuit and packet-switched domains.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellRestriction AccessClassBarredListCS [ ]
AccessClassBarredListPS [ ]
```

**Step 2** Issue the following command to verify the configuration:

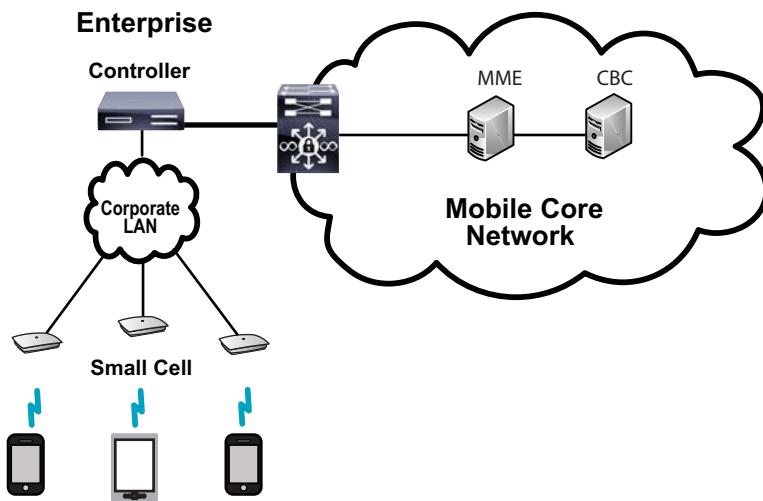
```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellRestriction
AccessClassBarredListCS "[ ]";
AccessClassBarredListPS "[ ]";
```

## 11.3 LTE Public Warning Systems

The small cell solution implements the Commercial Mobile Alert Service (CMAS) supporting multiple concurrent unacknowledged unidirectional messages to be sent out to all users in a defined area. CMAS supports three classes of warnings as per 3GPP technical specification 36.413:

- Presidential
- Imminent threat
- Child abduction emergency

The messages originate from Cell Broadcasting Entities (CBEs) which lie outside the mobile core network. The messages are received by Cell Broadcast Centers (CBCs) in the core network and sent through the MME over the S1AP interface to the controller which broadcasts the messages to all cells in its network. [Figure 33](#) shows the cell broadcast logical architecture.



**Figure 33** CMAS Architecture

Emergency Operations Centers (EOCs) generate the messages that include the geographic location defined in 3GPP-TS.36.413 Section 9.2.1.47 to broadcast in and the valid times to broadcast and forward them to the MME. The MME distributes the messages to the affected cells.

Alerts are aggregated in the core network which compiles a list of affected cells and passes the S1AP messages along to the appropriate controllers. The controllers then broadcasts the warning to all LTE cells in its small cell solution in less

than four seconds. CMAS messages can be canceled at any time. UEs will receive the messages regardless of their idle or connected states.

Messages are stored on the controller for the configured duration. If the controller reboots, the messages need to be resent by the MME. The controller reports delivery success or failure back to the MME. Broadcasting messages generate a syslog event.

Each CMAS message has a unique identifier. Duplicate messages from different MMEs, such as in the case of S1 flex configurations, are filtered by the controller and only one instance of the duplicate broadcast message are broadcast.

The controller can have up to two active messages at one time and filters duplicate messages send from multiple MMEs in the core network. With two active messages, a third message will be rejected. If one of the two active messages is terminated, an additional message will be accepted. The CBC can replace one of its active messages with another, which will then be broadcast as one of the two active messages.

### To configure an LTE public warning system

**Step 1** From the Configuration Mode, issue the following command to enable CMAS warnings. This example uses the Emergency Area ID (EAID) 100:

```
set FAPService 1 CellConfig LTE EPC EAID 100 PWS CMAS
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE EPC
EAID      100;
PWS       CMAS;
```

## 11.4 Restricting LTE Cell Access

The OS supports restricting access to LTE cells to ensure that public safety and emergency authorities have priority access to the cellular network in times of emergency. Typically police departments are the only authority permitted to invoke LTE cell access restriction, which is implemented on a local level, usually in a small geographic area.

All regular user devices are assigned to one of ten randomly allocated group classes. This designation is stored in the device SIM/USIM. A separate group of five classes is reserved for mobile operator staff, emergency services, public utilities, and security services. These class designations are valid only in the home country of the UE and do not provide elevated priority in other countries.

The following list defines the classes and their increasing priority:

- Class 0-9 - Ordinary users
- Class 10 - Emergency calls
- Class 11 - PLMN use
- Class 12 - Security services
- Class 13 - Public utilities (such as water/gas suppliers)
- Class 14 - Emergency services
- Class 15 - PLMN staff

In an emergency situation, the relevant authorities contact the mobile provider NOC and request LTE cell restriction activation in a specific geographical area. Cells adjacent to the incident are identified and LTE cell restriction is implemented on those cells while other cells operate normally. High priority UE are allowed access to the network.

### To activate LTE cell restriction to allow access only for emergency calls and high priority UE

**Step 1** From the Configuration Mode, issue the commands to enable barring ordinary user calls from UE belonging to Access Class 0-9:

```
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringForMOSignallingEnable true
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringFactorMOSignalling 0
```

**Step 2** Issue the following commands to enable barring ordinary user data calls from UE belonging to Access Class 0-9:

```
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringForMODataEnable true
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringFactorData 0
```

**Step 3** If needed, issue the following command to disable Emergency call barring:

```
set FAPService 1 CellConfig LTE RAN CellRestriction BarringForEmergency false
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN CellRestriction
BarringForEmergency          false;
ACBarringForMOSignallingEnable true;
ACBarringFactorMOSignalling   0;
ACBarringForMODataEnable     true;
```

To deactivate LTE cell restriction

**Step 1** From the Configuration Mode, issue the following commands to deactivate cell restriction:

```
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringForMOSignallingEnable false
set FAPService 1 CellConfig LTE RAN CellRestriction ACBarringForMODataEnable false
```

**Step 2** Issue the following command to verify the configuration:

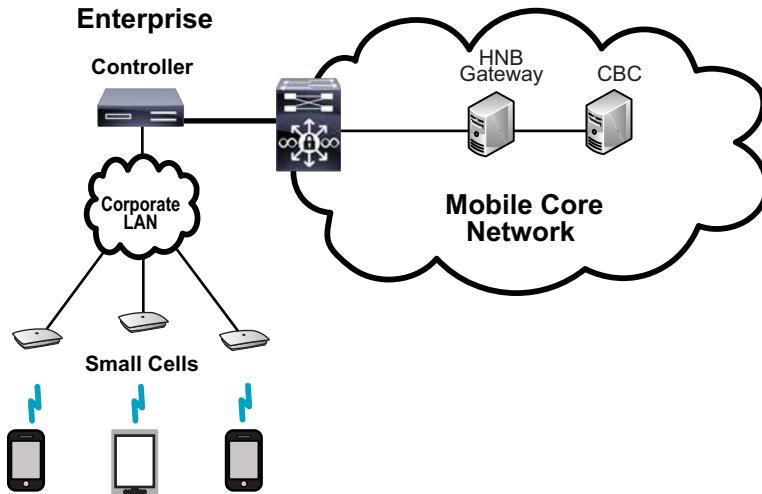
```
show FAPService 1 CellConfig LTE RAN CellRestriction
ACBarringForMOSignallingEnable false;
ACBarringForMODataEnable       false;
```

## 11.5 Configuring UMTS Cell Broadcast Services

Cell Broadcast Service (CBS) permits broadcasting a number of unacknowledged unidirectional messages to be sent out to all users in a defined area. The area maybe a number of cells or span the entire PLMN.

The messages originate from Cell Broadcasting Entities (CBEs) which lie outside the mobile core network. The messages are received by Cell Broadcast Centers (CBCs) in the core network and sent through the Iuh gateway to the controller which broadcasts the messages to all cells in its network. The controller accepts the IuBC messages only when relayed over the Iuh interface by an Iuh gateway. Direct connection to CBC is not supported. [Figure 34](#) shows the

cell broadcast logical architecture.



**Figure 34** Cell Broadcast Architecture

The controller can have up to the four active messages at one time. With four active messages, a fifth message will be rejected. If one of the four active messages is terminated, an additional message will be accepted. The CBC can replace one of its active messages with another, which will then be broadcast as one of the four active messages.

Messages are stored on the controller for the configured duration. If the controller reboots, the messages are re-sent. The controller reports delivery success or failure back to the CBC. Broadcasting messages generate a syslog event.

### To configure UMTS cell broadcasting

**Step 1** From the Configuration Mode, issue the following command to enable cell broadcasting:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellBroadcast Enable true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellBroadcast
Enable true;
```

**Step 3** Issue the following command to set the broadcast SAC. This example sets the SAC to 140.

```
set FAPService 1 CellConfig UMTS CN BroadcastSAC 140
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS CN BroadcastSAC
BroadcastSAC 140;
```

# 12 Session Management

One of the key benefits of the small cell solution architecture is the ability to provide local data switching and IP session continuity, fully integrated with user mobility. Local data switching allows authorized subscribers, such as enterprise staff, to directly access the corporate Intranet. It also offloads a mobile operator's backhaul requirements and reduces traffic load on mobile core elements, allowing for faster user experience, new services, and applications.

The controller serves as the central policy provisioning and enforcement point for the overall small cell solution. Data traffic can be configured on a per user (IMSI) or a per session (APN) basis, to be forwarded to the mobile operator's core network (passthrough mode), or to be switched locally through the enterprise network (also referred to as local switching or local breakout).

This chapter contains the following sections:

- [Section 12.1, Overview](#) on page 177
- [Section 12.2, Configuring Policies](#) on page 178
- [Section 12.3, Configuring Local Switching](#) on page 182
- [Section 12.4, Configuring UMTS Walled Garden Access](#) on page 183
- [Section 12.5, User Configuration Examples](#) on page 186

## 12.1 Overview

This chapter discusses in detail how to configure the system to enable session management functionalities and take advantage of the rich feature set and flexibility of wireless session management. Key elements in this chapter are the terms *Policy group* and *Policy*. A Policy group consists of a set of configurable Policies, which in turn are collections of customizable rules that determine how data sessions are handled.

These rules include everything from queuing and classification, to rate limiting and policing. [Figure 35](#) on page 178 shows the policy hierarchy and how different classes of subscribers (identified through *MemberDetails*) can be mapped to different policy groups, allowing for differentiated service offerings. [Section 12.5, User Configuration Examples](#) on page 186 shows examples of how these elements can be used to create different classifications of users with different access permissions and priorities.

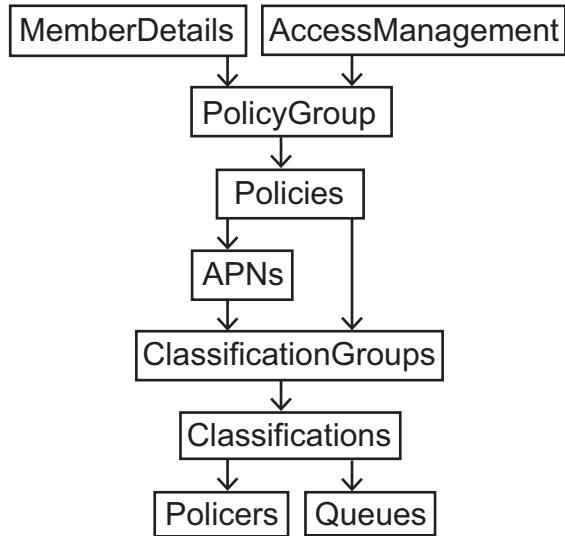


Figure 35 Policy Hierarchy

## 12.2 Configuring Policies

A Policy is a collection of settings that fully specify how data traffic is classified and managed. It includes firewalls, queuing, policing, walled gardens, access control, and user administration. Each user, identified by IMSI, is assigned a Policy that defines access permissions to network resources and quality of service.

UE data sessions are created in the context of an Access Point Name (APN). The choice of APN might be made by the provider, the UE, or UE manufacturer.

Policies are collected into Policy groups, which are then referenced when a user tries to join the system. A Policy group contains a list of Policies that are evaluated in the listed order. This might be useful, for example, to allow different policies to be applied for a user's access to different APNs.

The *APNMatchList* object setting defines a list of APN indexes. If it is present, the Policy will be executed only if the index of the session APN is in the *APNMatchList*. If the *APNMatchList* is not present, the Policy will always be executed for all APNs. Together with the ability to evaluate a list of policies one after the other in a sequence for a particular session, the *APNMatchList* allows the specification of settings for all APNs as well as specific settings for particular APNs for a class of users.

When there is no Policy configured for a user, the user session is assigned the following properties:

- **SwitchingMode:** PassThrough
- **PassThroughUplinkClassificationGroup:** no groups used
- **PassThroughDownlinkClassificationGroup:** no groups used
- **DefaultClassQueue:** no queue override

Policies for a given session can be automatically updated by setting the *AutoPolicyUpdate* parameter to *true*. This means that any changes to that policy will take effect immediately on all active sessions using that Policy after the configuration is committed. *AutoPolicyUpdate* does not affect admission control priority group objects discussed in [Section 10.3, UMTS Admission Control](#) on page 166.

The following procedure creates three Policies and three Policy groups with differing system Classes of Service (CoS). It then assigns two users to different Policies. Refer to [Section 12.5, User Configuration Examples](#) on page 186 for additional sample configurations.

### To create a Policy

**Step 1** From the Configuration Mode, create and enable a Policy and assign the CoS levels. In this example, Policy 1 named *Guest\_user* has passthrough switching and CoS 1.

```
set FAPService 1 AccessMgmt Policy 1 Enable true Description Guest_user SwitchingMode
PassThrough DefaultClassQueue 1
```

**Step 2** Create and enable Policy group 1 with Policy 1: In this example, guest users are assigned to Policy group 1. The highest level of authorized users are assigned to Policy group 20. Typical authorized users are assigned to Policy group 10.

```
set FAPService 1 AccessMgmt PolicyGroup 1 Enable true Description Guest_Users
PolicyIndexList [ 1 ]
```

**Step 3** Create and enable a Policy and assign the CoS levels. In this example:

- Policy 10 named *Employees*
- switches traffic through *NAPT* to IP interface 1
- on Ethernet port 3
- with CoS 5

```
set FAPService 1 AccessMgmt Policy 10 Enable true Description Employees APNMatchList [ 1
2 ] SwitchingMode NAPT DefaultClassQueue 5 PrimaryLANDevice 3 PrimaryIPInterface 1
```

**Step 4** Create and enable Policy group 10 with Policy 10: In this example, typical authorized users are assigned to Policy group 10.

```
set FAPService 1 AccessMgmt PolicyGroup 10 Enable true Description Employees
PolicyIndexList [ 10 ]
```

**Step 5** Create and enable a Policy and assign the CoS levels. In this example

- Policy 20 named *VIP*
- switches traffic through *NAPT* to IP interface 1
- on Ethernet port 3 with CoS 6.

CoS 6 is treated as expedited forwarding as it has a higher priority than CoS 1 assigned to unknown users in Step 1 and CoS 5 that will be assigned to the typical authorized user in Step 5 below.

```
set FAPService 1 AccessMgmt Policy 20 Enable true Description VIP SwitchingMode NAPT
DefaultClassQueue 6 PrimaryLANDevice 3 PrimaryIPInterface 1
```

**Step 6** Create and enable Policy group 20 with Policy 20: In this example, the highest level of authorized users are assigned to Policy group 20.

```
set FAPService 1 AccessMgmt PolicyGroup 20 Enable true Description VIPs PolicyIndexList
[ 20 ]
```

**Step 7** Configure the individual member priorities by their IMSI. In these examples:

- IMSI 001010123456943, named *Employee*, has a lower priority than the IMSI 001010123456909, named *Executive*. This user's session characteristics will automatically update to reflect changes in Policy group 10.
- IMSI 001010123456909, named *Executive*, is assigned a higher priority than IMSI 001010123456943, named *Employee*. This user's session characteristics will not automatically update to reflect changes in Policy group 20.

```
set FAPService 1 AccessMgmt MemberDetail 10 Enable true IMSI 001010123456943 Description
Employee PolicyGroupIndex 10 AutoPolicyUpdate true
```

```
set FAPService 1 AccessMgmt MemberDetail 20 Enable true IMSI 001010123456909 Description
Executive PolicyGroupIndex 20 AutoPolicyUpdate false
```

**Step 8** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 0;
MemberDetail 10 {
    Enable          true;
    IMSI           001010123456943;
    Description     Employee;
    PolicyGroupIndex 10;
    AutoPolicyUpdate true;
}
MemberDetail 20 {
    Enable          true;
    IMSI           001010123456909;
    Description     Executive;
    PolicyGroupIndex 20;
    AutoPolicyUpdate false;
}
PolicyGroup 1 {
    Enable          true;
    Description     Guest_Users;
    PolicyIndexList "[ 1 ]";
}
PolicyGroup 10 {
    Enable          true;
    Description     Employees;
    PolicyIndexList "[ 10 ]";
}
PolicyGroup 20 {
    Enable          true;
    Description     VIPs;
    PolicyIndexList "[ 20 ]";
}
Policy 1 {
    Enable          true;
    Description     Guest_user;
    SwitchingMode   PassThrough;
    Action          Unspecified;
    DefaultClassQueue 1;
}
Policy 10 {
    Enable          true;
    Description     Employees;
    APNMatchList   "[ 1 2 ]";
    SwitchingMode   NAPT;
    DefaultClassQueue 5;
    PrimaryLANDevice 2;
    PrimaryIPInterface 1;
}
Policy 20 {
    Enable          true;
    Description     VIP;
    APNMatchList   "[ ] ";
    SwitchingMode   NAPT;
    DefaultClassQueue 6;
    PrimaryLANDevice 2;
    PrimaryIPInterface 1;
```

**Step 9** Issue the **run test policy <imsi>** command to test the Policy for a given IMSI. This example uses IMSI 001010123456909. Note that the configuration must be committed before running this command.

```
run test policy IMSI 001010123456909
Policy result for a master session for IMSI 001010123456909
  Policy group index: 20
  Policy trace: [ 20 ]
  Action: Accept
  Policy switching mode: NAPT
  FM Switching mode: NAPT
  Passthrough Uplink ClassificationGroup index: 0, nexthop: 0
  Passthrough Downlink ClassificationGroup index: 0, nexthop: 0
  Local-switching Uplink ClassificationGroup index: 0, nexthop: 0
  Local-switching Downlink ClassificationGroup index: 0, nexthop: 0
  Switching filter nexthop: 17
  Primary LANDevice: 2
  Primary IPInterface: 1
  Forwarding group: 0
  Default class queue: 6
  Admission priority group: 0
```

**Step 10** Use the **run test IMSI <imsi> APN <network\_name> Type data** command to test the Policy for a data session. Note that the configuration must be committed before running this command.

```
run test policy IMSI 001010123456909 APN charlie Type data
Policy result for a data session for IMSI 001010123456909, APN charlie
  Policy group index: 20
  Policy trace: [ 20 ]
  Action: Accept
  Policy switching mode: NAPT
  FM Switching mode: NAPT
  Passthrough Uplink ClassificationGroup index: 0, nexthop: 0
  Passthrough Downlink ClassificationGroup index: 0, nexthop: 0
  Local-switching Uplink ClassificationGroup index: 0, nexthop: 0
  Local-switching Downlink ClassificationGroup index: 0, nexthop: 0
  Switching filter nexthop: 17
  Primary LANDevice: 2
  Primary IPInterface: 1
  Forwarding group: 0
  Default class queue: 6
  Admission priority group: 0
```

## 12.2.1 Configuring User Blacklists

Administrators can explicitly deny access to Cisco services to defined devices or unknown users by creating a Policy that rejects traffic to the system. These devices will connect to, and authenticate through, the provider macro network and not participate in the Cisco small cell network.

To configure a user blacklist

**Step 1** From the Configuration Mode, create and enable Policy 5 with the action *Reject* to keep traffic from the local network:

```
set FAPService 1 AccessMgmt Policy 5 Enable true Description Blacklist_policy Action Reject
```

**Step 2** Create and enable Policy group 5 with Policy 5. In this example it is named *Blacklist\_group*.

```
set FAPService 1 AccessMgmt PolicyGroup 5 Enable true Description Blacklist_group PolicyIndexList [ 5 ]
```

**Step 3** Blacklist a specific IMSI by assigning it to Policy group 5 that rejects it from being locally switched. In this example the IMSI is 001010123456789.

```
set FAPService 1 AccessMgmt MemberDetail 5 Enable true IMSI 001010123456789 PolicyGroupIndex 5
```

**Step 4** Blacklist all unknown users by directing them to Policy group 5.

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 5
```

**Step 5** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 5;
MemberDetail 5 {
    Enable          true;
    IMSI           001010123456789;
    PolicyGroupIndex 5;
}
PolicyGroup 5 {
    Enable          true;
    Description    Blacklist_group;
    PolicyIndexList "[ 5 ]";
}
Policy 5 {
    Enable          true;
    Description    Blacklist_policy;
    Action         Reject;
    DefaultClassQueue
}
}
```

## 12.3 Configuring Local Switching

The small cell solution defines three IP traffic switching modes:

- **Passthrough:** disables local switching. All traffic is backhauled to the provider core network.
- **NAPT:** enables local switching, assigns the UE an IP address from the provider core network. It then translates the appropriate address in IP packets to a DHCP-provided address for traffic exchanged with the enterprise network. Since the UE receives its address from the provider core network, this method provides seamless hand-in and hand-out of data sessions.
- **CNAPT:** enables local switching, assigns the UE an IP address from the enterprise DHCP server. It then translates the appropriate address in IP packets to the core-provided address for traffic exchanged with the provider core network. Since the UE receives its address from the enterprise core network, this method does not provide seamless hand-in and hand-out of data sessions. Due to this limitation, Cisco Systems recommends NAPT for most installations.

Local switching sends enterprise intranet-bound traffic or peer-to-peer sessions to the enterprise gateway rather than the provider core network. As much of the traffic within an enterprise, such as email and file management, is targeted within the local domain, this off-loads much of the backhaul traffic from the mobile core.

With local switching, no IP packets are exchanged between UEs and the provider core network. Refer to [Section 12.4, Configuring UMTS Walled Garden Access](#) on page 183 for information about how to configure access to specific core network services while using local switching.

To configure local switching for local users

**Step 1** From the Configuration Mode, create and enable a Policy to configure local switching for unknown users. In this example, Policy 1 sets local data switching in the NAPT mode to IP interface 1 on Gigabit Ethernet port 1.

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 1 Policy 1 Enable true SwitchingMode
NAPT PrimaryLANDevice 1 PrimaryIPInterface 1
```

**Step 2** Create a local-switch Policy group with Policy 1. This example creates and enables PolicyGroup 1.

```
set FAPService 1 AccessMgmt PolicyGroup 1 Enable true PolicyIndexList [ 1 ]
```

**Step 3** Assign Policy group 1 to unknown users:

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 1
```

**Step 4** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 1;
PolicyGroup 1 {
    Enable           true;
    PolicyIndexList "[ 1 ]";
}
Policy 1 {
    Enable           true;
    SwitchingMode   NAPT;
    PrimaryLANDevice 1;
    PrimaryIPInterface 1;
}
```

## 12.4 Configuring UMTS Walled Garden Access

A walled garden service refers to a UMTS service, such as billing, in the provider's core network that is accessible to the UE only through the core network connection but not through the Internet. When local switching is enabled, access to walled garden service is disabled because all UE traffic is sent to the enterprise network, possibly to be routed to the Internet.

When a UE Policy is passthrough (the default), the UE has unrestricted access to any walled garden service. However, when the UE Policy dictates that its traffic will be locally switched, access to walled garden service is inadvertently prohibited, because the UE will attempt to connect to the service through the Internet by way of the enterprise network.

Access to the walled garden service is restored by configuring per-Access Point Name (APN) walled garden filters, where a filter identifies the IP addresses that belong to the provider services in the core network.

When a UE creates a data session, the APN it presents will be used to find the appropriate walled garden filter, which is then installed for that data session in order to restore access to the walled garden service. The APN to be used for data sessions is configured on the UE.

You can implement Classification groups or walled garden groups that define domain names that point to the provider core network:

- [Section 12.4.1, Configuring Classification Groups](#) on page 183
- [Section 12.4.2, Configuring Walled Garden DNS Support](#) on page 185

### 12.4.1 Configuring Classification Groups

A *Classification* is a rule that defines a matching criterion. A *ClassificationGroup* collects a set of Classifications into a list. A ClassificationGroup can be used to direct specific traffic to the provider core network while all other data traffic goes to the enterprise network. A *Classification* can filter traffic by the following criteria:

- Destination IP address and subnet mask

- Destination port or range of ports (for TCP and UDP)
- IP protocol number
- Source IP address and subnet mask
- Source port or range of ports (for TCP and UDP)

Administrators can define one or more of the filtering criteria for a Classification. If a filtering criteria is not defined, traffic will pass that filter. If more than one criteria is defined in a *Classification*, then the traffic must match all of the filtering criteria to route to the walled garden services in the provider core network.

If traffic matches all filters for any single defined Classification in a ClassificationGroup it passes to the provider core network. Because multi-criteria filters are restrictive, it is often more sensible to define several less specific Classifications in a group than to have a single, very specific filter in a Classification that would reject traffic that should be directed at walled garden services but only passes some of the filters.

With the following configuration, an application on the UE that creates a connection to 172.17.12.240 using APN *service.provider.com* will have that traffic sent to the provider's core network. All other traffic from that UE will be locally switched.

### To create a walled garden service by Classification groups

**Step 1** Identify the core-based service by IP-based parameters, and specify that traffic to it should be passed to the core network and not locally switched.

**Step 2** From the Configuration Mode, define a single ClassificationGroup in the configuration containing a Classification entry for each service. In this example, the ClassificationGroup and Classification are both 1.

```
set QueueManagement ClassificationGroup 1 Enable true Description Provider_service_filter
ClassificationIndexes 1
```

**Step 3** Define the Classification and enable it. In this example, the service exists at TCP port 80 at the host with address 172.17.12.240 with the passthrough switching and description *Billing\_subnet*.

```
set QueueManagement Classification 1 DestIP 172.17.12.240 DestMask 255.255.255.0
ClassificationEnable true Description Billing_subnet Protocol 6 DestPort 80 Action
PassThrough
```

**Step 4** Issue the `show QueueManagement Classification` command to verify the configuration:

```
show QueueManagement Classification
Classification 1 {
    ClassificationEnable true;
    DestIP          172.17.12.240;
    DestMask        255.255.255.0;
    Protocol        6;
    DestPort        80;
    Description     Billing_subnet;
    Action          PassThrough;
```

**Step 5** Identify the APN used for access to the core-based service, and to associate the above *ClassificationGroup* with that APN. In this example

- the APN used to access the above private service is *service.provider.com*
- with IP address 172.17.12.240
- the descriptive name *Provider*

```
set FAPService 1 APN 1 Enable true APNName service.provider.com
WalledGardenClassificationGroup 1 ResolvedGGSNIP 172.17.12.240 WalledGardenDomainNames 1
DomainName Provider Enable true
```

**Step 6** Configure the billing service. In this example, APN 2 named *Billing\_application* carries billing information to the provider core network.

```
set FAPService 1 APN 2 Enable true Description Billing_application APNName
billing.provider.com WalledGardenClassificationGroup 1 ResolvedGGSNIP 10.30.1.1
WalledGardenDomainNames 2 Enable true
```

**Step 7** Issue the `show FAPService <ServiceNumber> APN` command to verify the configuration:

```
show FAPService 1 APN 1
APN 1 {
    Enable true;
    APNName service.provider.com;
    WalledGardenClassificationGroup 1;
    WalledGardenDomainNames 1 {
        Enable true;
        DomainName Provider;
    }
}
APN 2 {
    Enable true;
    Description Billing_application;
    APNName billing.provider.com;
    ResolvedGGSNIP 10.30.1.1;
    WalledGardenClassificationGroup 1;
    WalledGardenDomainNames 2 {
        Enable true;
    }
}
```

## 12.4.2 Configuring Walled Garden DNS Support

When local switching is configured for a UE, the UE is given the IP address of the enterprise Domain Name System (DNS) server in the Packet Data Protocol (PDP) Context Activation Accept message which the controller intercepts on its way back to the UE. This server is appropriate for all DNS queries except those for walled garden services. Those queries must be directed to the provider DNS server in order to receive a proper response.

The administrator must configure queries for specific domain names to be sent to the provider DNS server instead of the enterprise DNS server. The controller will intercept all DNS queries, redirect those that match the configured walled garden domains to the provider DNS server, receive the replies, and proxy them to the UE.

Since the addresses being looked up are walled garden services, the addresses resolved in the DNS replies can be automatically added to the walled garden filter. If all access to walled garden services are done through DNS lookups, then no static walled garden filter need be configured, only the domain names of walled garden services need be configured.

To create walled garden service by domain names

**Step 1** From the Configuration Mode, define a walled garden domain, specify a domain name, and enable it. In this example walled garden domain 1 uses `www.provider1.com` as a walled garden service.

```
set FAPService 1 APN 1 APNName Providers Enable true WalledGardenDomainNames 1 Enable true
DomainName www.provider1.com
```

**Step 2** Define another walled garden domain, associate a domain name, and enable it. In this example walled garden domain 2 uses `mail.yahoo.com` as a walled garden service.

```
set FAPService 1 APN 1 WalledGardenDomainNames 2 Enable true DomainName mail.yahoo.com
```

**Step 3** Issue the `show FAPService <ServiceNumber> APN` command to verify the configuration:

```
show FAPService APN WalledGardenDomainNames
FAPService 1 {
    APN 1 {
        Enable true;
```

```
        APNName                     Providers;  
        WalledGardenDomainNames 1 {  
            Enable      true;  
            DomainName www.provider1.com;  
        }  
        WalledGardenDomainNames 2 {  
            Enable      true;  
            DomainName mail.yahoo.com;  
        }  
    }  
}
```

#### 12.4.2.1 Wildcard Support

The CLI supports wildcards when defining walled garden domain names:

Value	Matches
*	Matches any string of alphanumeric characters
?	Matches a single alphanumeric character

In the following example, `WalledGardenDomainNames 1` the expression `*.google.com` matches `www.google.com` and `mail.google.com`. For `WalledGardenDomainNames 2`, the expression `billing???.verizon.com` matches `billing01.verizon.com` but not `billing1.verizon.com`.

```
show FAPService 1 APN 1
Enable true;
APNName test;
WalledGardenDomainNames 1 {
    Enable      true
    DomainName  "*.google.com";
}
WalledGardenDomainNames 2 {
    Enable      true;
    DomainName  "billing???.verizon.com";
}
```

## 12.5 User Configuration Examples

The following configuration examples show how to define a different types of users of the small cell solution. All examples below assume that the primary LAN interface to the provider core network has been configured in the controller Gigabit Ethernet port.

To configure the IP interface to the provider core network

**Step 1** From the Configuration Mode, configure the IP interface on the Gigabit Ethernet port of the controller (*LANDevice 1*). In this example, the port IP address is *192.168.32.5* with the subnet mask of *255.255.255.0*, with the name *Core*.

```
set LANDevice 1 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress  
192.168.32.5 IPInterfaceSubnetMask 255.255.255.0 Description Core
```

**Step 2** Issue the `show LANDevice <PortNumber> LANHostConfigManagement IPInterface` command to verify the configuration:

```
show LANDevice 1 LANHostConfigManagement IPInterface  
IPInterface 1 {  
    Enable                  true;  
    IPInterfaceIPAddress   192.168.32.5;  
    IPInterfaceSubnetMask  255.255.255.0;  
    Description            Core;  
}
```

## 12.5.1 Defining Users in the RAN

Users are defined in a RAN by creating and assigning a combination of Classifications, groups, and policies to define access, rate (through a Policer), and Quality of Service (QoS).

Figure 36 displays a topology with three different users (UEs) connecting to a controller.

- UE1 is a guest
- UE2 is in the engineering group
- UE3 is in the business group

Each UE has a different profile to limit access to the Enterprise and the Internet.

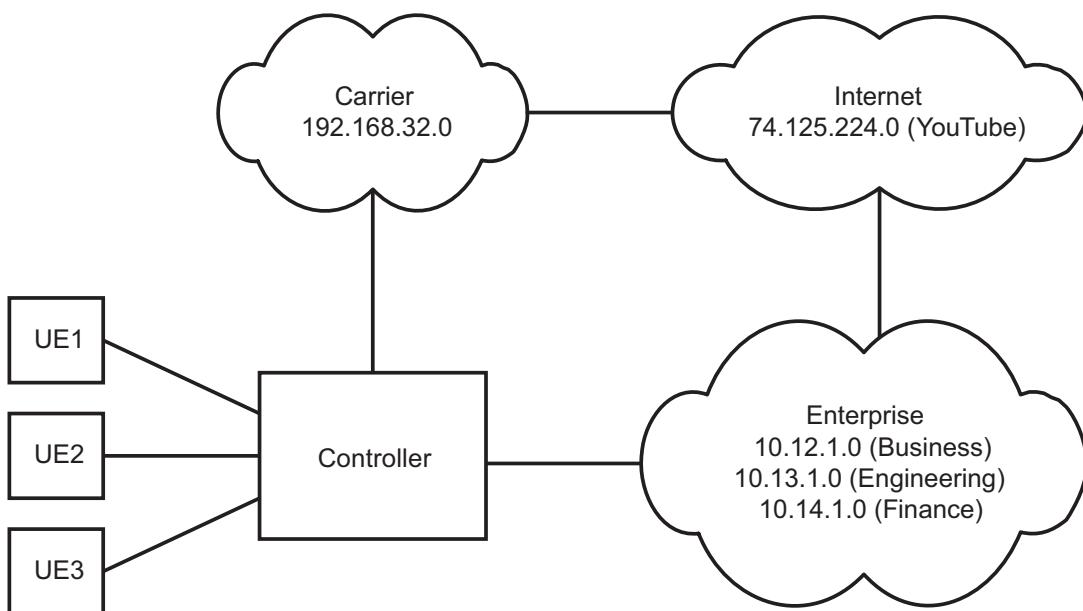


Figure 36 Example Topology

### 12.5.1.1 UE1 (Guest)

UE1 is a guest. The profile used to provide access for UE1 contains these limitations:

- Passthrough to Carrier
- No access to YouTube.

- Traffic policed at 1 Mbps.

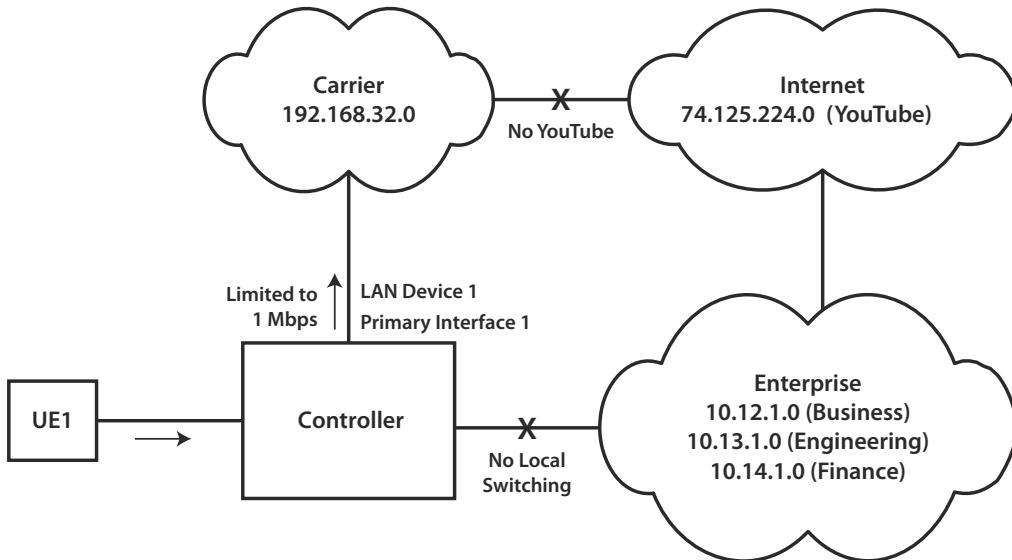


Figure 37 UE1 Access in the Sample Topology

Follow the steps below to configure and example of UE1:

**Step 1** From the Configuration Mode, create and enable a Policier that will drop packets that exceed a rate of 1 Mbps. This example uses Policier 10000.

```
set QueueManagement Policier 10000 PolicierEnable true CommittedRate 1000000
CommittedBurstSize 187500 ConformingAction Null NonConformingAction Drop
```

**Step 2** Create and enable a Classification to drop traffic to YouTube defined by the IP addresses 74.125.224.\*. This example uses Classification 74.

```
set QueueManagement Classification 74 ClassificationEnable true DestIP 74.125.224.0
DestMask 255.255.255.0 Action Drop
```

**Step 3** Create and enable a Classification and to apply Policier 10000. This example uses Classification 1000.

```
set QueueManagement Classification 1000 ClassificationEnable true ClassPolicer 10000
Action None
```

**Step 4** Create and enable a Classification group consisting of Classifications 74 and 1000. This example uses Classification group 101 and names it Guest.

```
set QueueManagement ClassificationGroup 101 Enable true Description radio_active_spider
ClassificationIndexes [ 74 1000 ]
```

**Step 5** Issue the `show QueueManagement` command to verify the configuration:

```
show QueueManagement
Enable true;
Classification 74 {
    ClassificationEnable true;
    DestIP          74.125.224.0;
    DestMask        255.255.255.0;
    Action          Drop;
}
Classification 1000 {
```

```

ClassificationEnable true;
ClassPolicer      10000;
Action           None;
}
Policer 10000 {
    PolicerEnable      true;
    CommittedRate     1000000;
    CommittedBurstSize 187500;
    ConformingAction   Null;
    NonConformingAction Drop;
}
ClassificationGroup 101 {
    Enable             true;
    Description        radio_active_spider;
    ClassificationIndexes "[ 74 1000 ]";
}

```

**Step 6** Create and enable Policy 1, set the switching mode to passthrough, and set the passthrough uplink Classification group to 101, which will cause uplink passthrough traffic to be processed by Classification group 101:

```
set FAPService 1 AccessMgmt Policy 1 Enable true SwitchingMode PassThrough
PassThroughUplinkClassificationGroup 101
```

**Step 7** Create and enable a Policy group with Policy 1.

```
set FAPService 1 AccessMgmt PolicyGroup 1 Enable true PolicyIndexList [ 1 ]
```

**Step 8** Assign unknown users to Policy group 1.

```
set FAPService 1 AccessMgmt UnknownUEPolicyGroupIndex 1
```

**Step 9** Issue the `show FAPService <ServiceNumber> AccessMgmt` command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 1;
Policy 1 {
    Enable             true;
    SwitchingMode     PassThrough;
    PassThroughUplinkClassificationGroup 101;
}
```

### 12.5.1.2 UE2 (Engineer)

UE2 is part of the engineering group. The profile used to provide access for UE2 contains these limitations:

- Uses local switching.
- No access to YouTube (Classification 74).
- No access to Enterprise business or Finance (Classification 12 and 14) areas.
- Walled Garden in Carrier Network.

Figure 38 illustrates how UE2 gains access to the Enterprise and the Carrier networks.

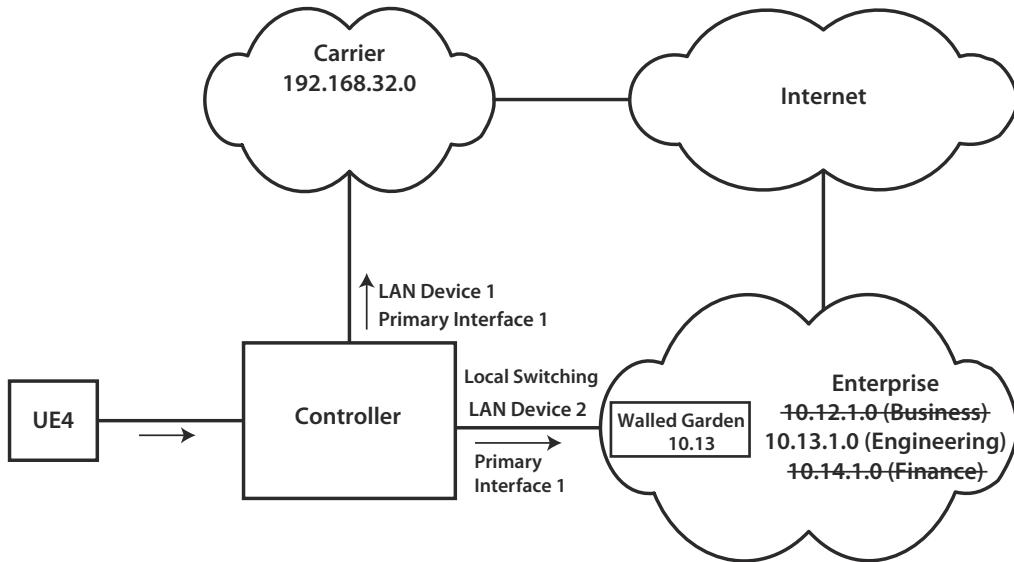


Figure 38 UE2 Access in the Sample Topology

Follow the steps below to configure an example of UE2:

**Step 1** From the Configuration Mode, configure the IP address of the controller for traffic to the Enterprise. This example uses IP address 10.15.10.\*.

```
set LANDevice 3 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress
10.15.10.5 IPInterfaceSubnetMask 255.255.255.0
```

**Step 2** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice
LANDevice 3 {
    LANHostConfigManagement {
        IPInterface 1 {
            Enable          true;
            IPInterfaceIPAddress 10.15.10.5;
            IPInterfaceSubnetMask 255.255.255.0;
        }
    }
}
```

**Step 3** Create and enable a Classification that will allow walled garden service. This example uses Classification 192 with the IP address 192.168.32.\*:

```
set QueueManagement Classification 192 DestIP 192.168.32.0 DestMask 255.255.255.0 Action
PassThrough ClassificationEnable true
```

**Step 4** Create and enable a Classification group for walled garden service. This example creates Classification group 1192 and names it *Walled\_Garden*.

```
set QueueManagement ClassificationGroup 1192 Enable true ClassificationIndexes [ 192 ]
Description Walled_Garden
```

**Step 5** Create and enable a Classification to drop traffic addressed to the business servers. This example creates Classification 12 with the IP address 10.12.1.\*.

```
set QueueManagement Classification 12 ClassificationEnable true DestIP 10.12.1.0 DestMask
255.255.255.0 Action Drop
```

**Step 6** Create and enable a Classification to drop traffic addressed to the finance servers. This example creates Classification 14 with the IP address 10.14.1.\*:

```
set QueueManagement Classification 14 ClassificationEnable true DestIP 10.14.1.0 DestMask
255.255.255.0 Action Drop
```

**Step 7** Create and enable a Classification to drop traffic to YouTube defined by the IP addresses 74.125.224.\*. This example uses Classification 74.

```
set QueueManagement Classification 74 ClassificationEnable true DestIP 74.125.224.0
DestMask 255.255.255.0 Action Drop
```

**Step 8** Create and enable a Classification group for engineering. This example creates Classification group 102 that includes Classifications 74, 12, and 14. It is named *Engineering*.

```
set QueueManagement ClassificationGroup 102 Enable true ClassificationIndexes [ 74 12 14 ]
] Description Engineering
```

**Step 9** Issue the `show QueueManagement` command to verify the configuration:

```
show QueueManagement
Enable true;
Classification 12 {
    ClassificationEnable true;
    DestIP          10.12.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 14 {
    ClassificationEnable true;
    DestIP          10.14.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 74 {
    ClassificationEnable true;
    DestIP          74.125.224.0
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 192 {
    ClassificationEnable true;
    DestIP          192.168.32.0;
    DestMask         255.255.255.0;
    Action           PassThrough;
}
ClassificationGroup 102 {
    Enable           true;
    Description      Engineering;
    ClassificationIndexes "[ 74 12 14 ]";
}
ClassificationGroup 1192 {
    Enable           true;
    Description      Walled_Garden;
    Description      "";
    ClassificationIndexes "[ 192 ]";
}
```

**Step 10** Create and enable an APN and associate it with the walled garden Classification group. This example creates APN 1 with the name *internet.provider.apn* and associate it with walled garden Classification group 1192.

```
set FAPService 1 APN 1 Enable true APNName internet.provider.apn
WalledGardenClassificationGroup 1192
```

**Step 11** Issue the **show FAPService <ServiceNumber> APN** command to verify the configuration:

```
show FAPService 1 APN
APN 1 {
    Enable           true;
    APNName         internet.provider.apn;
    WalledGardenClassificationGroup 1192;
}
```

**Step 12** Create and enable Policy 2 that sets the switching mode to NAPT and sets the local switch uplink for Configuration group 102, which will cause uplink local switch traffic to be processed by Classification group 102:

```
set FAPService 1 AccessMgmt Policy 2 Enable true SwitchingMode NAPT PrimaryLANDDevice 3
PrimaryIPInterface 1 LocalSwitchUplinkClassificationGroup 102
```

**Step 13** Create and enable Policy group 2 with Policy 2.

```
set FAPService 1 AccessMgmt PolicyGroup 2 Enable true PolicyIndexList [ 2 ]
```

**Step 14** Create a member detail, associate it with an IMSI, and assign it to a Policy group. This example creates member 1 with IMSI 020202020202020 and assigns it to Policy group 2.

```
set FAPService 1 AccessMgmt MemberDetail 2 Enable true IMSI 020202020202020
PolicyGroupIndex 2
```

**Step 15** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```
show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 1;
MemberDetail 2 {
    Enable           true;
    IMSI            020202020202020;
    PolicyGroupIndex 2;
}
PolicyGroup 2 {
    Enable           true;
    PolicyIndexList "[ 2 ]";
}
Policy 2 {
    Enable           true;
    SwitchingMode   NAPT;
    LocalSwitchUplinkClassificationGroup 102;
    PrimaryLANDDevice 2;
    PrimaryIPInterface 1;
}
```

### 12.5.1.3 UE3 (Business)

UE3 is part of the business group. The profile used to provide access for UE3 contains these limitations:

- Uses local switching.
- Traffic policed at 1 Mbps.
- No access to the Finance or Engineering (Classification 13 and 14) and areas in the Enterprise network.

Figure 39 illustrates how UE3 gains access to the Enterprise and Carrier networks.

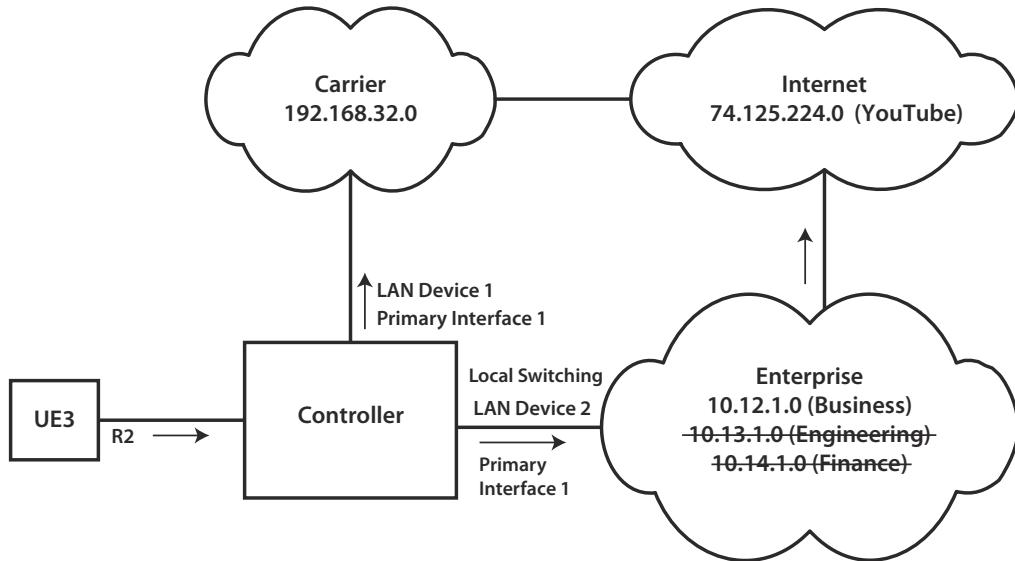


Figure 39 UE3 Access in the Sample Topology

**Step 1** From the Configuration Mode, configure the IP address of the controller for traffic to the Enterprise. This example uses IP address 10.15.10.\*.

```
set LANDevice 3 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress 10.15.10.5 IPInterfaceSubnetMask 255.255.255.0
```

**Step 2** Issue the `show LANDevice` command to verify the configuration:

```
show LANDevice
LANDevice 3 {
    LANHostConfigManagement {
        IPInterface 1 {
            Enable           true;
            IPInterfaceIPAddress 10.15.10.5;
            IPInterfaceSubnetMask 255.255.255.0;
        }
    }
}
```

**Step 3** Create and enable a Policer that will drop packets that exceed a rate of 1 Mbps. This example uses Policer 10000.

```
set QueueManagement Policer 10000 CommittedRate 1000000 CommittedBurstSize 187500
ConformingAction Null NonConformingAction Drop PolicerEnable true
```

**Step 4** Create and enable a Classification to drop traffic addressed to the engineering servers. This example creates Classification 13 with the IP address 10.13.1.\*.

```
set QueueManagement Classification 13 ClassificationEnable true DestIP 10.13.1.0 DestMask 255.255.255.0 Action Drop
```

**Step 5** Create and enable a Classification to drop traffic addressed to the finance servers. This example creates Classification 14 with the IP address 10.14.1.\*.

```
set QueueManagement Classification 14 ClassificationEnable true DestIP 10.14.1.0 DestMask 255.255.255.0 Action Drop
```

**Step 6** Create and enable a Classification and to apply Policer 10000. This example uses Classification 2000.

```
set QueueManagement Classification 2000 ClassificationEnable true ClassPolicer 10000
```

**Step 7** Create and enable a Classification group consisting of Classifications 1000, 13, and 14. This example uses Classification group 103 and names it Garden\_Spider.

```
set QueueManagement ClassificationGroup 103 Description Garden_Spider Enable true
ClassificationIndexes [ 2000 13 14 ]
```

**Step 8** Issue the `show QueueManagement` command to verify the configuration:

```
show QueueManagement
Enable true;
Classification 13 {
    ClassificationEnable true;
    DestIP          10.13.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 14 {
    ClassificationEnable true;
    DestIP          10.14.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 2000 {
    ClassificationEnable true;
    ClassPolicer     10000;
    Action           None;
}
Policer 10000 {
    PolicerEnable   true;
    CommittedRate   1000000;
    CommittedBurstSize 187500;
    NonConformingAction Drop;
}
ClassificationGroup 103 {
    Enable          true;
    Description     Garden_Spider;
    ClassificationIndexes "[ 1000 13 14 ]";
}
```

**Step 9** Create and enable Policy 3 that sets the switching mode to NAPT and sets the local switch uplink for Configuration group 103, which will cause uplink local switch traffic to be processed by Classification group 103.

```
set FAPService 1 AccessMgmt Policy 3 Enable true SwitchingMode NAPT PrimaryLANDevice 3
PrimaryIPInterface 1 LocalSwitchUplinkClassificationGroup 103
```

**Step 10** Create and enable Policy group 3 with Policy 3:

```
set FAPService 1 AccessMgmt PolicyGroup 3 Enable true PolicyIndexList [ 3 ]
```

**Step 11** Create a member detail, associate it with an IMSI, and assign it to a Policy group. This example creates member 1 with IMSI 03030303030303 and assigns it to Policy group 3.

```
set FAPService 1 AccessMgmt MemberDetail 3 Enable true IMSI 03030303030303
PolicyGroupIndex 3
```

**Step 12** Issue the `show FAPService <ServiceNumber> AccessMgmt` command to verify the configuration:

```
show FAPService 1 AccessMgmt
MemberDetail 3 {
    Enable          true;
    IMSI           03030303030303;
    PolicyGroupIndex 3;
}
PolicyGroup 3 {
```

```

        Enable          true;
PolicyIndexList "[ 3 ]";
}
Policy 3 {
    Enable          true;
    SwitchingMode NAPT;
    LocalSwitchUplinkClassificationGroup 103;
    PrimaryLANDevice 3;
    PrimaryIPInterface 1;
}

```

#### 12.5.1.4 UE4 (Engineer)

UE4 is part of the engineering group. The profile used to provide access for UE4 contains these limitations:

- Uses local switching.
- No access to Enterprise business or Finance (Classification 12 and 14) areas.
- Walled Garden in Enterprise business.

Figure 40 illustrates how UE4 gains access to the Enterprise and the Carrier networks.

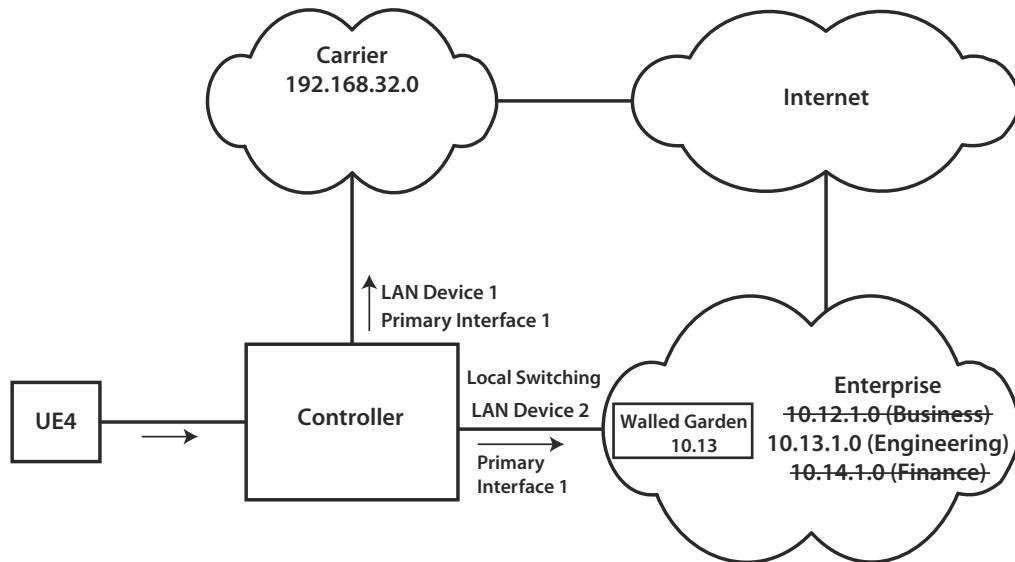


Figure 40 UE4 Access in the Sample Topology

Follow the steps below to configure an example of UE4:

- Step 1** From the Configuration Mode, configure the IP address of the controller for traffic to the Enterprise. This example uses IP address 10.15.10.\*.

```
set LANDevice 3 LANHostConfigManagement IPInterface 1 Enable true IPInterfaceIPAddress 10.15.10.5 IPInterfaceSubnetMask 255.255.255.0
```

- Step 2** Issue the **show LANDevice** command to verify the configuration:

```
show LANDevice
LANDevice 3 {
    LANHostConfigManagement {
        IPInterface 1 {
            Enable          true;
            IPInterfaceIPAddress 10.15.10.5;
            IPInterfaceSubnetMask 255.255.255.0;
```

```

        }
    }
}
```

**Step 3** Create and enable a Classification that will allow walled garden service to the engineering domain. This example uses Classification 10 with the IP address 10.13.1.\*:

```
set QueueManagement Classification 192 DestIP 10.13.1.0 DestMask 255.255.255.0 Action PassThrough ClassificationEnable true
```

**Step 4** Create and enable a Classification group for walled garden service. This example creates Classification group 10 and names it *Walled\_Garden\_Engineering*.

```
set QueueManagement ClassificationGroup 10 Enable true ClassificationIndexes [ 192 ] Description Walled_Garden_Engineering
```

**Step 5** Create and enable a Classification to drop traffic addressed to the business servers. This example creates Classification 12 with the IP address 10.12.1.\*.

```
set QueueManagement Classification 12 ClassificationEnable true DestIP 10.12.1.0 DestMask 255.255.255.0 Action Drop
```

**Step 6** Create and enable a Classification to drop traffic addressed to the finance servers. This example creates Classification 14 with the IP address 10.14.1.\*.

```
set QueueManagement Classification 14 ClassificationEnable true DestIP 10.14.1.0 DestMask 255.255.255.0 Action Drop
```

**Step 7** Create and enable a Classification group for engineering. This example creates Classification group 102 that includes Classifications 12 and 14. It is named *Engineering*.

```
set QueueManagement ClassificationGroup 102 Enable true ClassificationIndexes [ 74 12 14 ] Description Engineering
```

**Step 8** Issue the **show QueueManagement** command to verify the configuration:

```
show QueueManagement
Enable true;
Classification 10 {
    ClassificationEnable true;
    DestIP          192.168.32.0;
    DestMask         255.255.255.0;
    Action           PassThrough;
}
Classification 12 {
    ClassificationEnable true;
    DestIP          10.12.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
Classification 14 {
    ClassificationEnable true;
    DestIP          10.14.1.0;
    DestMask         255.255.255.0;
    Action           Drop;
}
```

**Step 9** Create and enable an APN and associate it with the walled garden Classification group. This example creates APN 10 with the name *Engineering* and associate it with walled garden Classification group.

```
set FAPService 1 APN 1 Enable true APNName internet.provider.apn
WalledGardenClassificationGroup 1192
```

**Step 10** Issue the **show FAPService <ServiceNumber> APN** command to verify the configuration:

```
show FAPService 1 APN
APN 1 {
    Enable           true;
```

```

APNName           internet.provider.apn;
WalledGardenClassificationGroup 1192;
}

```

**Step 11** Create and enable Policy 2 that sets the switching mode to NAPT and sets the local switch uplink for Configuration group 102, which will cause uplink local switch traffic to be processed by Classification group 102:

```
set FAPService 1 AccessMgmt Policy 2 Enable true SwitchingMode NAPT PrimaryLANDevice 3
PrimaryIPInterface 1 LocalSwitchUplinkClassificationGroup 102
```

**Step 12** Create and enable Policy group 2 with Policy 2.

```
set FAPService 1 AccessMgmt PolicyGroup 2 Enable true PolicyIndexList [ 2 ]
```

**Step 13** Create a member detail, associate it with an IMSI, and assign it to a Policy group. This example creates member 1 with IMSI 0202020202020 and assigns it to Policy group 2.

```
set FAPService 1 AccessMgmt MemberDetail 2 Enable true IMSI 0202020202020
PolicyGroupIndex 2
```

**Step 14** Issue the **show FAPService <ServiceNumber> AccessMgmt** command to verify the configuration:

```

show FAPService 1 AccessMgmt
UnknownUEPolicyGroupIndex 1;
MemberDetail 2 {
    Enable          true;
    IMSI            0202020202020;
    PolicyGroupIndex 2;
}
PolicyGroup 2 {
    Enable          true;
    PolicyIndexList "[ 2 ]";
}
Policy 2 {
    Enable          true;
    SwitchingMode  NAPT;
    LocalSwitchUplinkClassificationGroup 102;
    PrimaryLANDevice 3;
    PrimaryIPInterface 1;
}
```



# 13 IP QoS and Filtering

This chapter contains the following sections:

- [Section 13.1, Configuring IP Quality of Service on page 199](#)
- [Section 13.2, Configuring Egress IP Quality of Service on page 203](#)
- [Section 13.3, Configuring IP Interface Filtering on page 205](#)

## 13.1 Configuring IP Quality of Service

Configuring IP Quality of Service (QoS) consists of defining classes of service and configuring packet queuing and scheduling.

### 13.1.1 Class of Service

The small cell solution differentiates network traffic by assigning each voice and data packet a Class of Service (CoS) with a DSCP value that contains a code point that associates it with one of the service classes. The system supports eight classes of service, each of which maps into a defined queue for Quality of Service (QoS) processing. For VLAN-tagged interfaces, by default the 802.1Q Priority Code Point (PCP) value on each packet will take the same value as the IP DSCP CoS value.

The system contains four system default classes of service:

- **Network Control (NC):** Time critical network control and wireless control protocol packets. For example, RLC STATUS PDUs and PTP packets.
- **Expedited Forwarding/Voice (EF):** R99 voice traffic and other VoIP traffic.
- **Assured Forwarding 1 (AF1):** Uplink data traffic is given priority over downlink traffic since precious wireless resources have already been expended to transmit it. It is also likely to include TCP ACKs which should be preferred over TCP retransmissions on the downlink.
- **Best Effort (BE):** Other user data and non-critical control information such as batch RF monitoring information.

### 13.1.2 Configuring Packet Queuing and Scheduling

Packet queuing and scheduling involves selecting a queue and an associated scheduling Policy based on a packet's class of service. All packets are queued on ingress based on CoS code points. This Classification determines the ingress queue and therefore the scheduling applied to the packet. A per-queue drop mechanism ensures that the system will be able to accommodate high priority traffic.

On egress, the final packet Classification determines from which queue the packet is scheduled. Queues are scheduled by Weighted Round-Robin (WRR) with strict priority.

[Table 23](#) shows the default system configuration of the CoS number, TR-index, queue name and description, and the drop pass and drop threshold values. The drop pass buffer defines the occupancy (expressed as a percentage) where the system will start to drop packets. At a buffer occupancy below this value, no packets are dropped (0% drop probability).

The drop threshold buffer defines the occupancy (expressed as a percentage) at which all packets will be dropped. At a buffer occupancy above this value, all packets are dropped (100% drop probability). The drop threshold must be larger than drop pass buffer occupancy.

The drop probability increases from 0 to 100% as the buffer occupancy increases from the drop pass to the drop threshold. In this case, the buffers are the set of buffers available to all CoSs. By configuring CoS in this way, lower priority traffic can be given a lower occupancy numbers at which Random Early Detect (RED) activates in than higher priority traffic. In general, no CoS should ever completely exhaust the available buffers.

All traffic is scheduled with the WRR scheduling algorithm and dropped as needed using the Weighted Random Early Detection (WRED) queue management algorithm.

**Table 23: Code Point Classifications**

CoS	TR-Index	Queue Name	Description	Drop Pass%	Drop Threshold%
0	1	BE	Best Effort	70	85
1	2	AF1	Assured Forwarding 1	50	60
2	3	AF2	Assured Forwarding 2	50	60
3	4	AF3	Assured Forwarding 3	50	60
4	5	AF4	Assured Forwarding 4	75	90
5	6	EF	Expedited Forwarding (voice)	90	95
6	7	NC1	Network Control 1	50	60
7	8	NC2	Network Control 2	90	95

The class to queue scheduler mapping is system-wide, applying to the controller and all managed small cells.

### To configure packet queuing and scheduling

**Step 1** From the Configuration Mode, configure each queue. This example configures the parameters of Queue 1.

```
set QueueManagement Queue 1 QueueEnable true QueueWeight 5 REDThreshold 85 REDPercentage
70 DropAlgorithm WRED SchedulerAlgorithm WRR QueueCodePoint [ 5 ] QueueMarking 0
```

**Step 2** Issue the `show QueueManagement Queue` command to verify the configuration:

```
show QueueManagement Queue 1
Queue 1 {
    QueueEnable      true;
    QueueWeight      5;
    REDThreshold     85;
    REDPercentage   70;
    DropAlgorithm    WRED;
    SchedulerAlgorithm WRR;
    QueueCodePoint   "[ 5 ]";
    QueueMarking     0;
```

### 13.1.3 Default CoS Markings for Output Traffic

The following table lists the default CoS markings for the different types of network traffic sent by the controller:

**Table 24: Default CoS Markings**

Traffic Type	CoS Marking	Example
Operations and management	AF2	SSH, SNMP
Signalling	NC1	SIGTRAN
UE voice	EF	RTP
UE packet data	BE or policy override <sup>a</sup>	GTP
Other control	NC2	NTP

- a. Policy override refers to the feature whereby a Policy can assign traffic to a specific class queue, either by setting the default class queue in the policy or by setting the class queue in a classification group. In this case the DSCP value configured in the queue configuration will be used.

### 13.1.4 Editing Default Control Plane CoS Markings

On rare occasions, it may be necessary to edit the default CoS code point classifications for control plane traffic.



Cisco Systems does not recommend modifying the default control plane CoS values. If you must modify the control plane CoS values, ensure that your system has been backed up to a secure location.

#### 13.1.4.1 Configuring Control Plane CoS code point classifications

The following control plane CoS objects can be edited:

- **DefaultOAMClassQueue:** Default class queue used for operations, administration, and management IP traffic such as SNMP and SSH packets.
- **DefaultSignalingClassQueue:** Default class queue used for signaling IP traffic such as SCTP packets that carry UMTS signalling.

To configure control plane CoS code point classification values

- Step 1** From the Configuration mode, issue the `set QueueManagement ControlPlaneCos` command to edit the default CoS code point classification values. This example sets the DefaultOAMClassQueue to 2 and the DefaultSignalingClassQueue to 6.

```
set QueueManagement ControlPlaneCos DefaultOAMClassQueue 2 DefaultSignalingClassQueue 6
```

- Step 2** Issue the following command to verify the configuration:

```
show QueueManagement ControlPlaneCos
DefaultSignalingClassQueue      6;
DefaultOAMClassQueue           2;
```

#### 13.1.4.2 Configuring Control Plane Classification Groups

Similar to [Section 12.4.1, Configuring Classification Groups](#) on page 183, you can create a classification group for control plane IP traffic that consists of the *DefaultOAMClassQueue* and *DefaultSignalingClassQueue*.

A classification group can be used to override the default class queue used for the IP traffic specified by this classification group. A value of zero is used to specify the absence of such a classification group.

### To create a CoS classification group

**Step 1** Enter the `set QueueManagement Classification` command to create the classification. In this example:

- all controller HTTP traffic is directed to the destination port 80
- using protocol 6 (TCP)
- it creates classification 1
- assigns it the CoS code point classification 4 (assured forwarding 2).

```
set QueueManagement Classification 1 ClassQueue 4 ClassificationEnable true DestPort 80
DestPortRangeMax 80 Protocol 6
```

**Step 2** Issue the following command to verify the configuration:

```
show QueueManagement Classification 1
ClassificationEnable true;
Protocol          6;
DestPort          80;
DestPortRangeMax 80;
ClassQueue        4;
```

**Step 3** Issue the `set QueueManagement ClassificationGroup 5 ClassificationIndexes` command to create classification group 5 and associate it with classification 1.

```
set QueueManagement ClassificationGroup 5 ClassificationIndexes [ 1 ] Enable true
```

**Step 4** Issue the following command to verify the configuration:

```
show QueueManagement ClassificationGroup 5
Enable           true;
ClassificationIndexes "[ 1 ]";
```

**Step 5** Issue the `set QueueManagement ControlPlaneCoS ControlPlaneClassificationGroup` command to create the CoS classification group. This example:

- creates classification group 5
- assigns it default signaling class queue of 6
- and assigns it to the default OAM class queue of 4

```
set QueueManagement ControlPlaneCoS ControlPlaneClassificationGroup 5
DefaultSignalingClassQueue 6 DefaultOAMClassQueue 4
```

**Step 6** Issue the following command to verify the configuration:

```
show QueueManagement ControlPlaneCoS
ControlPlaneClassificationGroup 5;
DefaultSignalingClassQueue     6;
DefaultOAMClassQueue          4;
```

## 13.1.5 LTE QoS Differentiation

When implementing LTE service it is important to recognize that different types of traffic to and from the core network are assigned different priority levels to ensure the targeted quality of service. For example, network control on the management plane is assigned the highest priority when bandwidth is allocated to ensure the stability and functionality of the service itself. In an IP network, traffic priorities are differentiated by their DSCP values as discussed in [Section 13.1.1, Class of Service](#) on page 199. And to ensure call clarity, voice traffic in LTE is assigned the highest priority other than network control.

The small cell system supports IP DSCP marking of LTE traffic based on the nine Quality of Service Code Identifier (QCI) values received from the core network. The controller has eight class of service queues. Each CoS queue is

configured with a default DSCP marking to mark the outgoing traffic, and a set of DSCP values to determine which queue will receive an incoming packet. CoS queues 7 and 8 are generally reserved for network control traffic.

**Table 25** shows the GSMA recommended mapping of QCI to DSCP values on the IP network, along with the corresponding value of the CLI CoS queue and default DSCP marking of the controller for each queue. Note that:

- The CoS queues for QCI values 5 and 6 are identical. The corresponding DSCP marking by the controller are also identical.
- The controller DSCP marking differs from the GSMA-recommended value for QCI values 4 through 8.

**Table 25: Code Point Classifications**

QCI	GSMA Recommended DSCP Class	GSMA Recommended DSCP Marking	CLI CoS Queue	Default DSCP Marking for the CoS Queue
1	EF	46	6	46 (EF)
2	EF	46	6	46 (EF)
3	EF	46	6	46 (EF)
4	AF41	34	5	32 (CS4)
5	AF31	26	4	24 (CS3)
6	AF32	28	4	24 (CS3)
7	AF21	18	3	16 (CS2)
8	AF11	10	2	8 (CS1)
9	BE	0	1	0

To match the controller default DSCP marking to the GSMA-recommended value, change the corresponding CoS queue to DSCP mapping using the CLI or eRMS to modify the value of the **ClassQueue** parameter. Note that UMTS and LTE services share the same settings and that CoS queues 7 and 8 are not available for QCI to CoS queue mapping.

#### To modify the QCI to CoS queue mapping

**Step 1** From the Configuration Mode, issue the following command to modify the controller QCI to CoS queue mapping. This example maps QoS 1 to CoS queue 4.

```
set FAPService 1 CellConfig LTE EPC QoS 1 Enable true QCI 1 ClassQueue 4
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE EPC
QoS 1 {
    Enable      true;
    QCI         1;
    ClassQueue  4;
}
```

## 13.2 Configuring Egress IP Quality of Service

You can configure a traffic rate limit from the controller to the mobile provider security gateway and maintain Class of Service (CoS) priorities of egress traffic flows when there is limited bandwidth backhaul. Traffic exceeding the configured rate limit will be queued and shaped to the defined rate. The core network connection can then be

provisioned to a specific rate, and the controller will work within that bandwidth budget. This feature mitigates against unexpected priority packets drops.

First create an *EgressQoSProfile* that defines the rate limit and queue weights for weighted fair queueing. The rate limit can range from 2 to 1000 Mbps. Upon the creation of an *EgressQoSProfile*, the queue weights are set to their default values shown in [Table 26](#). Cisco Systems strongly recommends not changing queue weights unless instructed to do so by technical support. The system supports up 16 egress queue profiles.

**Table 26: Default Queue Weights**

Queue Number	Queue Weight
1	3
2	6
3	8
4	11
5	14
6	17
7	19
8	22

Next, enable traffic shaping on an IP interface by assigning the *EgressQoSProfile* to it. The system supports up to 15 IP interfaces. Each interface can support 0 or 1 profile. Assigning the *EgressQoSProfile* the value of 0 removes any existing profile and returns the IP interface to its default values.

### To enable backhaul rate limiting

**Step 1** From the Configuration mode, issue the **set QueueManagement EgressQoSProfile** command to create an egress QoS profile. This example creates and enables profile 10, and names it *Backhaul\_RateLimiting\_Profile*.

```
set QueueManagement EgressQoSProfile 10 Enable true Description
Backhaul_RateLimiting_Profile RateLimit 20
```

**Step 2** Issue the following command to verify the configuration:

```
show QueueManagement EgressQoSProfile 10
Enable      true;
Description Backhaul_RateLimiting_Profile;
RateLimit   20;
```

**Step 3** Issue the following command to apply the profile to the IP interface. This example applies profile 10 to IP interface 1 on Gigabit Ethernet port 1 of the controller:

```
set LANDevice 1 LANHostConfigManagement IPInterface 1 EgressQoSProfile 10
```

**Step 4** Issue the following command to verify the configuration:

```
show LANDevice 1 LANHostConfigManagement IPInterface 1
Enable          true;
IPInterfaceIPAddress    10.1.194.21;
IPInterfaceSubnetMask  255.255.255.0;
EgressQoSProfile    10;
```

### 13.2.1 Configuring 802.1Q Priority Code Point Behavior

By default, the 802.1Q Priority Code Point (PCP) value on each packet for VLAN-tagged interfaces, will take the same value as the IP DSCP CoS value. To set this value to zero, set the `VLANCoS` parameter to `zero`.

To configure the 802.1Q priority code point behavior

**Step 1** From the Configuration Mode, issue the following command. This example sets the 802.1Q PCP value to zero.

```
set QueueManagement VLANCoS Zero
```

**Step 2** Issue the following command to verify the configuration:

```
show QueueManagement VLANCoS
Zero;
```

## 13.3 Configuring IP Interface Filtering

You can create custom ingress and egress filters on an Ethernet port IP interface that connects to the provider core network. The ingress filter is applied to the packet after IPsec decapsulation. The egress filter is applied to the packet before IPsec encapsulation. This helps to mitigate Denial of Service (DoS) attacks to and from the core network and can control the types of traffic coming in and going out of the port.

Filters are defined in classifications and classification groups that are then applied to the Ethernet port IP interface. When creating the classification, you must configure it to drop or allow (Classification Action: `None`) traffic. Passthrough mode is not valid for IP interface filtering. The following example disallows ping traffic on Ethernet port 1 IP interface 1.

To create and apply ingress and egress IP interface filters

**Step 1** From the Configuration Mode, issue the `set QueueManagement Classification` command to create and enable the classification and classification groups. The first example:

- creates and enables classification 5 and enables it
- names it `Ping_Deny_Filter`
- sets the action to `Drop` for protocol 1, which is the protocol number for ICMP.

The second example creates and enables ClassificationGroup 5 that includes Classification 5.

```
set QueueManagement Classification 5 Description Ping_Deny_Filter ClassificationEnable
true Protocol 1 Action Drop
```

```
set QueueManagement ClassificationGroup 5 ClassificationIndexes [ 5 ] Enable true
```

**Step 2** Issue the `show QueueManagement Classification` command to verify the configuration:

```
show QueueManagement Classification
Classification 5 {
    ClassificationEnable true;
    Protocol          1;
    Description       Ping_Deny_Filter;
    Action            Drop;
}
```

**Step 3** Issue the following command to assign classification group 5 as the ingress and egress filter for the IP interface for LANDevice 1:

```
set LANDevice 1 LANHostConfigManagement IPIInterface 1 Enable true
IngressClassificationGroup 5 EgressClassificationGroup 5
```

**Step 4** Issue the following command to verify the configuration:

```
show LANDevice 1 LANHostConfigManagement
IPInterface 1 {
    Enable                  true;
    IPInterfaceIPAddress    10.1.193.6;
    IPInterfaceSubnetMask   255.255.255.0;
    IngressClassificationGroup 5;
    EgressClassificationGroup 5;
}
```

**Step 5** (Optional) Issue the **set FAPService <ServiceNumber> Transport Tunnel VirtualInterface** command to apply the same IP filtering rules to all ingress and egress traffic within the IPsec tunnel:

```
set FAPService 1 Transport Tunnel VirtualInterface 1 IngressClassificationGroup 5
EgressClassificationGroup 5 Enable true
```

**Step 6** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface
VirtualInterface 1 {
    Enable                  true;
    IngressClassificationGroup 5;
    EgressClassificationGroup 5;
}
```

**Step 7** Ping any device reachable from the Ethernet port. The ping will fail.

**Step 8** Issue the **show Forwarding NextHop NextHopID <FilterId> Detail** command to verify the counters *NumPacketsMatched* and *NumPacketsDropped* for the filter. This example uses filter 5.

```
show Forwarding NextHop NextHopID 5 Detail
```



# 14 UMTS Mobility

This chapter contains the following sections:

- [Section 14.1, Cell Connection States](#) on page 207
- [Section 14.2, Handover](#) on page 209
- [Section 14.3, Multiple Ingress Macro Hand-In](#) on page 210
- [Section 14.4, Target Cell ID-Based Hand-In](#) on page 213
- [Section 14.5, Cell Selection and Re-Selection](#) on page 213
- [Section 14.6, Enabling Cell Re-Selection from UMTS to LTE](#) on page 215
- [Section 14.7, Creating UMTS Proximity Detection Cells](#) on page 216

## 14.1 Cell Connection States

A user session can be in one of four connection states relative to the RAN. The small cell solution supports the following three of those four connection states:

- **CELL\_DCH** (Dedicated Cell Channel): UE has a dedicated physical channel allocated to the uplink and downlink, and dedicated and shared transport channels. The UE location is known at the cell level. This dedicated channel consumes the most radio bandwidth and battery power.
- **CELL\_FACH** (Cell Forward Access Channel): UE has no dedicated physical channel. It uses common channels FACH for downlink and RACH for uplink. The UE location is known at the cell level according to the last cell update. This state consumes less power than CELL\_DCH.
- **CELL\_PCH** (Cell Paging Channel): UE has no dedicated physical channel. No uplink activity is possible. The UE location is known at cell level according to the last cell update while in the CELL\_FACH state. This semi-sleep state consumes less power than CELL\_FACH since it is not transmitting data.

When a UE enters into the system with a voice or data session, it is placed into the CELL\_DCH state, and assigned a dedicated uplink and downlink physical channel. If the UE does not send or receive any data traffic for a specified period of time, the session is placed in the CELL\_FACH state to free resources and reduce battery power consumption in the UE.

If the UE has no data activity for an additional, separately specified, period of time, the session is placed in the CELL\_PCH state. A further period of data inactivity transitions the session into the IDLE state. When in the CELL\_PCH state, the session transitions to the CELL\_FACH state when requesting service and sends an update message to the controller.

In the CELL\_DCH state, the system monitors UE location and evaluates the quality of the signal and relative capacity of cells that can offer service. If a different cell can offer better service, the system triggers a mobility event and passes that UE to the new cell. In the CELL\_FACH or CELL\_PCH states, mobility is governed by UE. In these states, the UE selects a new cell based on its own measurements and triggers a cell change by sending a cell update message.

## To configure cell inactivity timers

**Step 1** From the Configuration Mode, set the DCH inactivity period (in units of 100ms, from 0 through 60 seconds). This example sets the inactivity period for transition from CELL\_DCH to CELL\_FACH to 5 seconds. The default is 0, for disabled.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH DCHInactivityTimer 50
```

**Step 2** Set the FACH inactivity timer (in units of 100ms, from 0 through 60 seconds). This example sets the inactivity period for transition from CELL\_FACH to CELL\_PCH to 10 seconds. The default is 0, for disabled.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH FACHInactivityTimer 100
```

**Step 3** Set the idle timer (in seconds, from 0 through 3600). This sets the inactivity period for transition from CELL\_PCH to IDLE of ten minutes. The default is 0, for disabled.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH DisconnectInactivityTimer 600
```

**Step 4** Specify the maximum number of UEs in CELL\_FACH or CELL\_PCH sessions allowed in the system. The default value is 0 because CELL\_FACH is disabled by default. The recommended value is 16 when enabled. This example uses the recommended 16 sessions.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH MaxNumCellFACHUEs 16
```

**Step 5** Issue the `show FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellFACH` command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellFACH
DCHInactivityTimer      50;
FACHInactivityTimer     100;
DisconnectInactivityTimer 600;
MaxNumCellFACHUEs       16
```

### 14.1.1 Enabling Fast Dormancy

The OS supports 3GPP Release 8 fast dormancy that allows user devices to transition to battery efficient states such as CELL\_DCH and CELL\_PCH. Fast dormancy reduces power consumption compared to UE in CELL\_DCH state and reduces call setup time and signaling overhead compared to UE in CELL\_IDLE state.

When a user device does not have data to send for a prolonged period, it sends a Signaling Connection Release Indication (SCRI) to the network with the cause set to *UE Requested PS Data session end*. The fast dormancy feature is disabled by default.

You can enable this feature and configure the T323 timer that sets the delay between SCRIs from UE. The T323 timer is measured in seconds. Valid options are 0 (fast dormancy disabled), 5, 10, 20, 30, 60, 90, 120. The default is 0.

#### To enable fast dormancy

**Step 1** From the Configuration Mode, issue the following command to enable fast dormancy and set the T323 timer. This example sets the timer to 5 seconds.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RRCTimers T323 5
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RRCTimers T323
T323 5;
```

### To disable fast dormancy

Step 1 From the Configuration Mode, issue the following command to disable fast dormancy by setting the T323 timer to 0.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP RRCTimers T323 0
```

Step 2 Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP RRCTimers T323  
T323 0;
```

### 14.1.2 CELL\_FACH and Admission Control

A session in CELL\_FACH or CELL\_PCH state does not consume any admission control resources. When it transitions from CELL\_DCH to CELL\_FACH, the codes and radio links associated with the user are freed up. When a user needs to transition from CELL\_FACH to CELL\_DCH, the transition is treated as a mobility event from the admission control perspective.

## 14.2 Handover

In a radio network, handover is the transfer of existing voice or data traffic from a channel in a cell to a channel in a different cell. In a soft handover, a UE establishes a link with one or more new cells before dropping the link to an existing cell. In a hard handover, the link to an existing cell is dropped before establishing a link to a second cell. There are three types of hard handover of a UE session from the provider core network to the cluster, and back again:

- **Intra-Frequency Hard Handover** is performed when the target cell is a UMTS cell being controlled by a different controller or external small cell controller that is operating at the same frequency as the small cell. Intra-frequency hard handover is triggered by Event 1A.

If intra-frequency hard handover is disabled, an Event 1A received for an external neighbor will be ignored and the controller will not initiate a handover to it. This feature is disabled by default. If the *enable* parameter is changed, the update will take effect processing the next Event 1A from a UE.

- **Inter-Frequency Hard Handover** is performed when the target cell is a UMTS cell being controlled by a different controller or external small cell controller that is operating on a different frequency than the small cell. Inter-frequency hard handover is triggered by Event 2B or can be initiated by the controller in the form of a blind handover.

If inter-frequency hard handover is disabled, the controller will not instruct the UE to perform inter-frequency measurements. This feature is enabled by default. If the *enable* parameter is changed, it will take effect when the next Event 2B is received from an already connected UE or when a new UE connects.

- **Inter-RAT Hard Handover** is performed when the target cell belongs to different Radio Access Technology (RAT) such as GSM. Inter-RAT hard handover is triggered by Event 3A or can be initiated by the controller in the form of a blind handover.

If inter-RAT hard handover is disabled, the controller will not instruct the UE to perform GSM measurements. This feature is enabled by default. If the *enable* parameter is changed, it will take effect when the next Event 3A is received from an already connected UE or when a new UE connects.

All three types of handover have default values. Modifying these default values is optional.

To configure handover parameters

**Step 1** From the Configuration Mode, set the threshold at which a call is handed over to GSM network. The value sets the Event 3A threshold in the Measurement Control Message (MCM). This example uses the default threshold of -98 dBm.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterRATMeas ThresholdOtherSystem  
-98
```

**Step 2** Enable the use of Intra-Frequency hard handover by setting the value of **IntraFreqHardHandoverEnable** to *true*. The default is *false*.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP IntraFreqHardHandoverEnable true
```

**Step 3** Enable the use of Inter-Frequency hard handover by setting the value of **IntraFreqHardHandoverEnable** to *true*. The default is *true*, so unless this value has been changed to *false*, this step is not necessary.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterFreqHardHandoverEnable true
```

**Step 4** Enable the use of Inter-RAT Hard Handover by setting the value of **InterRATHardHandoverEnable** to *true*. The default is *true*, so unless this value has been changed to *false*, this step is not necessary.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterRATHardHandoverEnable true
```

**Step 5** Enable the hard handover for Intra-Frequency and Inter-Frequency for packet-switched traffic by setting the value of **PSHardHandoverEnable** to *true*. The default is *false*.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP PSHardHandoverEnable true
```

**Step 6** Issue the **show FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP** command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP  
IntraFreqHardHandoverEnable true;  
InterFreqHardHandoverEnable true;  
InterRATHardHandoverEnable true;  
PSHardHandoverEnable true;  
InterRATMeas {  
    ThresholdOtherSystem -98;  
}
```

## 14.3 Multiple Ingress Macro Hand-In

Hand-in of a UMTS call from macro network to the small cell solution is normally triggered to a specific target cell in the small cell solution. The small cell solution is identified by a unique cell ID. The target cell is identified by a unique primary scrambling code. For each small cell solution, this allows the macro network to be configured with a single primary scrambling code.

However, it is desirable to allow multiple macro-handover ingress points within an small cell solution without making configuration changes or enhancements on the macro network or HNB gateway solutions. With this multi-ingress CS macro hand-in, the small cell solution will allow up to four cells to be designated as hand-in cells. All such cells will be configured with the same primary scrambling code. The small cell solution will continue to use a single cell ID to register itself with the HNB gateway. Therefore, as far as the HNB gateway and macro RNC are concerned, this solution is no different from a single hand-in cell solution.

### 14.3.1 Disambiguation of Target Hand-in Cell

When a macro hand-in request is received by the small cell solution, the message will contain a single primary scrambling code. Since multiple cells designated for hand-in can have the same primary scrambling code, the services

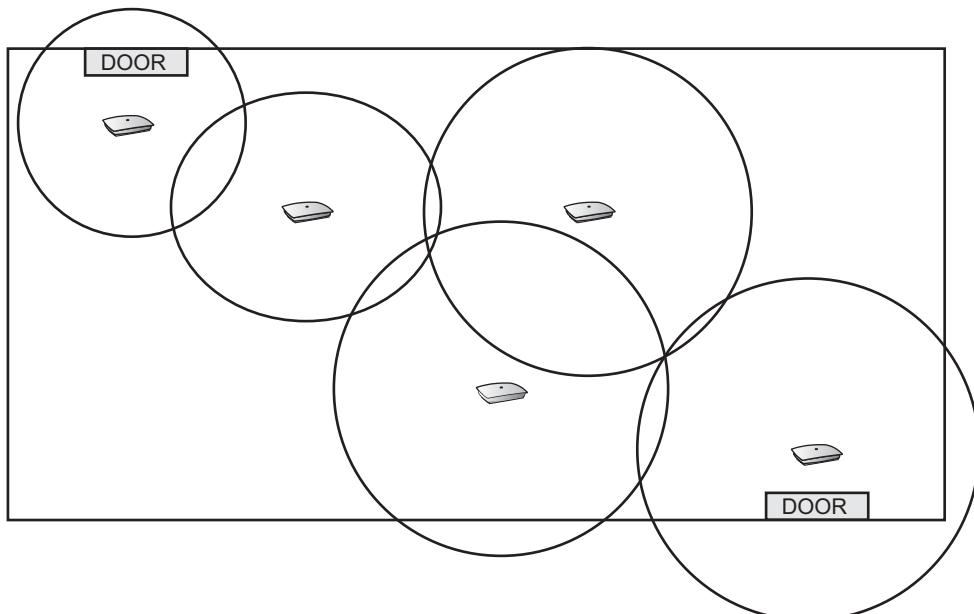
cannot determine the target cell solely based on the received primary scrambling code. The solution is to establish a radio link on all the hand-in cells configured with the received primary scrambling code.

Even though radio links are established on all hand-in small cells, the UE will achieve physical layer synchronization with only a single hand-in cell (the closest small cell). The controller will receive the RRC Radio Bearer Reconfiguration Complete message from the UE through a single cell. Having identified the target cell, the controller will delete the radio links established on the remaining hand-in small cells.

There will be no changes required on the UE to support this solution. As far as the UE is concerned, it will receive configuration information for a single radio link. This is made possible by ensuring that the radio links established across all hand-in small cells are created with the same RF configuration. This will require that a set of RF resources (such as OVSF codes) be reserved on the hand-in small cells. When the hand-in is complete, the reserved resources will be released to allow for more hand-ins.

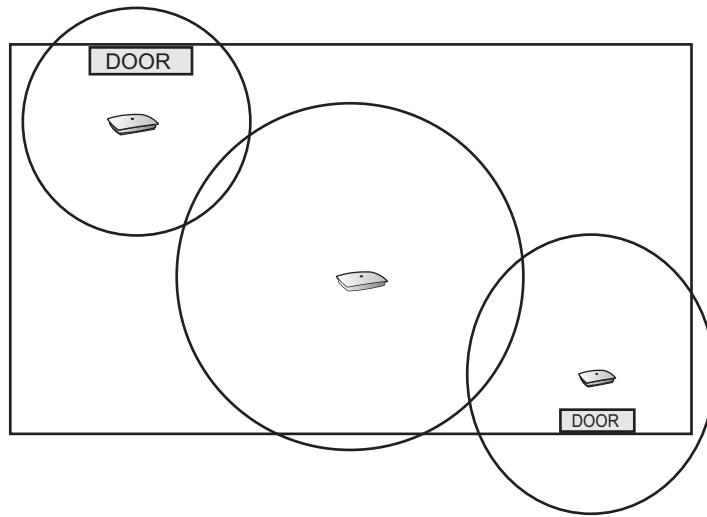
### 14.3.2 Configuring Multiple Ingress Hand-In

The provider network views the entire small cell solution as a single cell with one cell ID. For locations with multiple ingress points covered with separate ingress cells, all ingress cells must be provisioned with the same primary scrambling code but different cell IDs. The small cell solution supports up to four ingress points using the same primary scrambling code as long as the ingress points are not first or second tier neighbors. [Figure 41](#) shows a topology that supports multiple ingress hand-ins as there are two cells between the ingress points, making them third tier neighbors:



**Figure 41** Permitted Topology

[Figure 42](#) shows a topology that is not permitted for multiple ingress hand-ins as there is only one cell between the ingress points, making them second tier neighbors:



**Figure 42** Unsupported Topology

As a UE with an active voice call approaches the ingress cell, the UE begins to report the primary scrambling code to the macro cell. The macro cell should be provisioned with the hand-in primary scrambling code as an external neighbor cell mapped to the global cell ID used by the small cell solution to register with the HNB gateway. The macro cell will then send a handover request to the HNB gateway via the core network.

The gateway directs the hand-in request to the small cell solution. Within the small cell solution, the system configures a radio connection on all ingress cells with that primary scrambling code, using the same radio resources, and sends the handover command back to the macro cell. After successful hand-In completion on the actual ingress cell on which the UE is camped, the small cell solution tears down the other, unused connections.

Use the following high-level steps to configure multiple ingress hand-in:

#### To configure multiple ingress hand-in

- Step 1** Identify the hand-in cells based in ingress locations at the site.
- Step 2** Identify the alternate primary scrambling code to be used for hand-in. This is the same primary scrambling code provisioned on the macro network with mapping to small cell solution cell ID.
- Step 3** Ensure the *HandInTargetCellDetermination* attribute is set to *MeasReportPSC*.
- Step 4** Ensure that the pool of primary scrambling codes does not include the hand-in alternate primary scrambling code.
- Step 5** If you have not previously run a REM scan, issue the **request umts rem start** command from the Operational Mode with the controller in maintenance mode to initiate a REM scan:

```
request umts rem start
```

The controller will auto assign primary scrambling codes to all cells as part of REM scan. As part of the REM scan, the hand-in cells will also be assigned primary scrambling codes from the configured pool of primary scrambling codes.

- Step 6** Manually review the REM scan topology results from Step 5 to ensure pre-identified hand-in cells are not first or second tier neighbors of each other.
- Step 7** Based on confirmation from Step 6, from the Configuration Mode manually provision the hand-in cells with the alternate primary scrambling code selected in Step 2 and to ensure that their neighbor lists are not modified during future REM scan neighbor list changes:

```
set Cell <CellNumber> CellConfig UMTS RAN FDDFAP PrimaryScramblingCodeConfigured
<HandInPSC> PrimaryScramblingCodeLockEnable true
```

**Step 8** Issue the following command to set the *LocationType* attribute on each hand-in cell to *Handin*. If the cell already has a configured *LocationType* attribute, enter the existing one as well.

```
set cell <CellNumber> LocationType [ HandIn ]
```

**Step 9** From the Operational Mode, issue the `request umts self-config neighborlist-create` command to update the neighbor lists.

```
request umts self-config neighborlist-create
```

## 14.4 Target Cell ID-Based Hand-In

When connected to the core network through an HNB gateway, you can configure the small cell solution to use a single cell for hand-in by setting the cell ID to the same value as the global cell ID used in the HNB of the hand-in cell Register Request message. This cell cannot be marked as *HandIn* cell in the location type.

To configure target cell ID-based hand-in

**Step 1** From the Configuration Mode, issue the following command to verify that the cell location type is not set to *HandIn*. Change the location type if needed.

Show Cell

**Step 2** Issue the following command to set the hand-in target cell to *TargetCellID*:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP HandInTargetCellDetermination TargetCellID
```

**Step 3** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP HandInTargetCellDetermination
HandInTargetCellDetermination TargetCellID;
```

## 14.5 Cell Selection and Re-Selection

Cell selection is the process by which the UE identifies a cell for service and selects it. Once camped on this cell, called the serving cell, it registers on the PLMN and continues to monitor common and shared downlink channels from this cell for service.

The UE continually evaluates the cell selection criterion by monitoring the signal quality of the serving cell and applies measurement rules or triggers for cell re-selection to start making signal quality measurements of neighbor cells. When measurement is triggered, the UE ranks all cells based on their measured signal quality and re-selects to a neighbor cell if it outranks the serving cell over a period of time.

The OS RF management suite detects intra-frequency, inter-frequency, and GSM macro neighbors during the network monitor phase. These external neighbors are then consolidated with the internal cluster neighbors based on signal strength and broadcast by each cell in the cluster. This process ensures that any boundary cells in the cluster are highly likely to include the macro neighbors in the neighbor lists, thereby facilitating cell re-selection out of the cluster into the macro network.

The UMTS standard-defined parameters used for cell selection and re-selection can be configured from the `set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellSelection` hierarchy. All of these parameters have default values. Changing the default values is optional.

## To view the UMTS standard parameters

Step 1 From the Configuration Mode, issue the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellSelection** command and press the **Tab** key to view the UMTS standard parameters and their descriptions:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
```

Possible completions:

InterFreqQOffset1sn	- Bias against reselection to an inter-freq cell in dB when QualityMeasureCPICH is set to CPICH RSCP
InterFreqQOffset2sn	- Bias against reselection to an inter-freq cells in dB when QualityMeasureCPICH is set to CPICH RSCP
InterRatQOffset1sn	- Bias against reselection to an inter-RAT cell in dB
IntraFreqQOffset1sn	- Bias against reselection to an intra-freq neighbor cell in dB when QualityMeasureCPICH is set to CPICH RSCP
IntraFreqQOffset2sn	- Bias against reselection to an intra-freq neighbor cell in dB when QualityMeasureCPICH is set to CPICH Ec/No
QHyst1s	- Cell reselection hysteresis if QualityMeasureCPICH is set to CPICH RSCP
QHyst2s	- Cell reselection hysteresis if QualityMeasureCPICH is set to CPICH Ec/No
QRxLevMin	- Minimum required CPICH RSCP by UE in dBm to meet cell selection criterion
QQualMin	- Minimum required CPICH Ec/No by UE in dB to meet cell selection criterion
QualityMeasureCPICH	- Metric used by UE for CPICH quality measurements
SIntersearch	- Threshold in dB on CPICH Ec/No of current cell for inter-frequency measurements
SIntrasearch	- Threshold in dB on CPICH Ec/No of current cell for intra-frequency measurements
SSearchRAT	- Threshold in dB on CPICH Ec/No of current cell for inter-RAT measurements
TReselections	- Time interval in seconds in which criteria must stay fulfilled for a UE to trigger a cell reselection
UETxPwrMaxRACH	- UE maximum transmit power level for RACH in dBm

## To view the currently configured cell selection values

Step 1 From the Configuration Mode, issue the following command to view the currently configured cell selection values:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
QualityMeasureCPICH "CPICH Ec/No";
QQualMin          -19;
QRxLevMin         -105;
QHyst1s           0;
QHyst2s           4;
TReselections     2;
SIntrasearch       10;
SIntersearch       2;
SSearchRAT         2;
UETxPwrMaxRACH   21;
IntraFreqQOffset1sn 0;
IntraFreqQOffset2sn 4;
InterFreqQOffset1sn 0;
InterFreqQOffset2sn 50;
InterRatQOffset1sn 50;
```

## 14.6 Enabling Cell Re-Selection from UMTS to LTE

Re-selection from a UMTS to LTE serving cell, when enabled, provides the support that the UE needs to perform cell re-selection from WCDMA to LTE. The LTE frequencies and the parameters for cell re-selection are sent on the broadcast channel in System Information Block type 19 (SIB19). Cell reselection to LTE is supported by E-UTRAN capable UEs in Idle Mode or in Cell\_PCH.

In Step 1 below, the **SPrioritySearch1** parameter is the threshold used in the measurement rules for cell re-selection when absolute priorities are used. It specifies the value of *Srxlev* in the serving cell controlling the rate of inter-frequency and inter-RAT measurements. **ThreshServingLow** is the threshold used in the measurement rules for cell re-selection to lower priority neighbors when absolute priorities are used. It specifies the limit for *Srxlev* in the serving cell below which the UE may perform cell reselection to a cell on a lower absolute priority layer.

### To enable cell re-selection from UMTS to LTE

**Step 1** From the Configuration Mode, issue the following command to set the parameters for the Information Element UTRA priority information list sent in SIB19 messages. This example sets the:

- **ServingCellPriority**: absolute priority of the service cell to 2.
- **SPrioritySearch1**: threshold in the measurement rules for cell re-selection to 8 dB.
- **ThreshServingLow**: RSCP threshold for the Serving cell re-selection to lower priority neighbors to 8. A value of 8 translates to  $-100\text{dBm} \leq \text{RSCP} < -99\text{dBm}$ .

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection ServingCellPriority 3
SPrioritySearch1 8 ThreshServingLow 8
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
ServingCellPriority 2;
SPrioritySearch1 8;
ThreshServingLow 8;
```

**Step 3** Issue the following command to set the parameters for the inter-RAT reselection to an LTE serving cell. This example sets the:

- **EUTRACarrierARFCN**: ARFCN of this frequency carrier to 65535.
- **QRxLevMinEUTRA**: required minimum received RSRP level on this E-UTRA frequency carrier to -62 dBm.
- **CellReselectionPriority**: absolute priority of this E-UTRA frequency to 7.
- **ThreshXHigh**: the RSRP threshold for a neighbor on a higher priority E-UTRAN frequency to 30 dB. A value of 30 maps to  $-81\text{dBm} \leq \text{RSRP} < -80\text{dBm}$ .
- **ThreshXLow**: the RSRP threshold for a neighbor on a lower priority E-UTRAN frequency to 20 dB. A value of 20 maps to  $-101\text{dBm} \leq \text{RSRP} < -100\text{dBm}$ .

```
set FAPService 1 CellConfig UMTS RAN FDDFAP Mobility IdleMode IRAT LTE Carrier 2
EUTRACarrierARFCN 65535 QRxLevMinEUTRA -62 CellReselectionPriority 7 ThreshXHigh 30
ThreshXLow 20
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP Mobility IdleMode IRAT LTE Carrier
Carrier 2 {
    EUTRACarrierARFCN      65535;
    QRxLevMinEUTRA        -62;
    CellReselectionPriority 7;
    ThreshXHigh            30;
    ThreshXLow             20;
}
```

## 14.7 Creating UMTS Proximity Detection Cells

The small cell solution permits provisioning a small cell with a proximity detection cell at a particular location to provide near field communication services. The proximity detector is similar to a standard UMTS cell except that it can be configured to transmit at very low power. A UE must be within inches or feet to establish a session on the proximity detection cell.

When the controller detects a session on proximity detection cell, it generates a syslog event that contains the IMSI and the proximity detection cell location information. This syslog event can then be sent to a syslog target server integrated with an application residing on the controller or in the cloud. The syslog message includes the IMSI, cell ID, cell geographic location (when configured), and Radio Network Controller ID (RNCID) of the controller. No syslog event generates when the IMSI leaves the proximity detection cell. Example use cases include sending a text message to the UE, integrating with a security system to unlock a door, or validating the user's presence at a given time.

The proximity detection cell integrates with a UMTS radio network system identically as a standard UMTS cell. The UE can be in RRC idle or connected mode when it is close to the proximity detection cell. In connected mode, the UE will go in soft handoff with the proximity detection cell.

In connected mode, the UE will go in soft hand-off with the proximity detection cell. An event can be raised when a proximity detection cell is added to the UE's active set. To trigger the UE to initiate a session when in idle mode, each proximity detection cell is assigned a unique LAC/RAC. The LAC/RAC values must be known to the MSC/SGSN. Upon re-selecting, the UE initiates a location update procedure that can then be used to trigger the syslog event.

### To create a proximity detection cell

**Step 1** From the Configuration mode, issue the following command to configure the LAC/RAC of the proximity detection cell. This example sets the LAC/RAC of cell 77 to 4660:86.

```
set Cell 77 CellConfig UMTS CN LACRAC [4660:86]
```

**Step 2** Issue the following command to verify the configuration:

```
show cell 77 CellConfig UMTS CN  
LACRAC [4660:86];
```

**Step 3** Issue the following command to enable location reporting on this cell:

```
set Cell 77 CellConfig LocationReportingEnable true
```

**Step 4** Issue the following command to verify the configuration:

```
show cell 77 CellConfig LocationReportingEnable  
LocationReportingEnable true;
```

**Step 5** Issue the following command to set the cell power level. This example sets cell 77 power level to -30 dBm.

```
set Cell 77 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerConfigured -300
```

**Step 6** Issue the following command to lock the cell power level to prevent changes during a REM scan:

```
set Cell 77 CellConfig UMTS RAN FDDFAP RF MaxFAPTxPowerLockEnable true
```

**Step 7** Issue the following command to verify the configuration:

```
show Cell 77 CellConfig UMTS RAN FDDFAP RF  
MaxFAPTxPowerConfigured -300;  
MaxFAPTxPowerLockEnable true;
```



# 15 LTE Mobility

This chapter contains the following sections:

- [Section 15.1, Handover](#) on page 217
- [Section 15.2, Cell Selection and Re-Selection](#) on page 218
- [Section 15.3, Enabling Cell Re-Selection from UMTS to LTE](#) on page 219
- [Section 15.4, Enabling LTE Idle Mode Cell Re-Selection](#) on page 220
- [Section 15.5, Creating LTE Proximity Detection Cells](#) on page 222

## 15.1 Handover

In a radio network, handover is the transfer of existing voice or data traffic from a channel in a cell to a channel in a different cell. In a soft handover, a UE establishes a link with one or more new cells before dropping the link to an existing cell. In a hard handover, the link to an existing cell is dropped before establishing a link to a second cell. There are four types of hard handover of a UE session from the provider core network to the cluster, and back again:

All types of handover have default values. Modifying these default values is optional.

To configure handover parameters

**Step 1** From the Configuration Mode, set the threshold at which a call is handed over to GSM network. The value sets the Event 3A threshold in the Measurement Control Message (MCM). This example uses the default threshold of -98 dBm.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterRATMeas ThresholdOtherSystem -98
```

**Step 2** Enable the use of Intra-Frequency hard handover by setting the value of `IntraFreqHardHandoverEnable` to `true`. The default is `false`.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP IntraFreqHardHandoverEnable true
```

**Step 3** Enable the use of Inter-Frequency hard handover by setting the value of `IntraFreqHardHandoverEnable` to `true`. The default is `true`, so unless this value has been changed to `false`, this step is not necessary.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterFreqHardHandoverEnable true
```

**Step 4** Enable the use of Inter-RAT Hard Handover by setting the value of `InterRATHardHandoverEnable` to `true`. The default is `true`, so unless this value has been changed to `false`, this step is not necessary.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP InterRATHardHandoverEnable true
```

**Step 5** Enable the hard handover for Intra-Frequency and Inter-Frequency for packet-switched traffic by setting the value of `PSHardHandoverEnable` to `true`. The default is `false`.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP PSHardHandoverEnable true
```

**Step 6** Issue the **show FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP** command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP
IntraFreqHardHandoverEnable    true;
InterFreqHardHandoverEnable    true;
InterRATHardHandoverEnable    true;
PSHardHandoverEnable          true;
InterRATMeas {
    ThresholdOtherSystem -98;
}
```

## 15.2 Cell Selection and Re-Selection

Cell selection is the process by which the UE identifies a cell for service and selects it. Once camped on this cell, called the serving cell, it registers on the PLMN and continues to monitor common and shared downlink channels from this cell for service.

The UE continually evaluates the cell selection criterion by monitoring the signal quality of the serving cell and applies measurement rules or triggers for cell re-selection to start making signal quality measurements of neighbor cells. When measurement is triggered, the UE ranks all cells based on their measured signal quality and re-selects to a neighbor cell if it outranks the serving cell over a period of time.

The OS RF management suite detects intra-frequency, inter-frequency, and GSM macro neighbors during the network monitor phase. These external neighbors are then consolidated with the internal cluster neighbors based on signal strength and broadcast by each cell in the cluster. This process ensures that any boundary cells in the cluster are highly likely to include the macro neighbors in the neighbor lists, thereby facilitating cell re-selection out of the cluster into the macro network.

The UMTS standard-defined parameters used for cell selection and re-selection can be configured from the **set FAPService <ServiceNumber> CellConfig RAN CellSelection** hierarchy. All of these parameters have default values. Changing the default values is optional.

To view the LTE standard parameters

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> CellConfig UMTS RAN FDDFAP CellSelection** command and press the **Tab** key to view the UMTS standard parameters and their descriptions:

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
```

Possible completions:

InterFreqQOffset1sn	- Bias against reselection to an inter-freq cell in dB when QualityMeasureCPICH is set to CPICH RSCP
InterFreqQOffset2sn	- Bias against reselection to an inter-freq cells in dB when QualityMeasureCPICH is set to CPICH Ec/No
InterRatQOffset1sn	- Bias against reselection to an inter-RAT cell in dB
IntraFreqQOffset1sn	- Bias against reselection to an intra-freq neighbor cell in dB when QualityMeasureCPICH is set to CPICH RSCP
IntraFreqQOffset2sn	- Bias against reselection to an intra-freq neighbor cell in dB when QualityMeasureCPICH is set to CPICH Ec/No
QHyst1s	- Cell reselection hysteresis if QualityMeasureCPICH is set to CPICH RSCP
QHyst2s	- Cell reselection hysteresis if QualityMeasureCPICH is set to CPICH Ec/No
QRxLevMin	- Minimum required CPICH RSCP by UE in dBm to meet cell selection criterion
QqualMin	- Minimum required CPICH Ec/No by UE in dB to meet cell selection criterion
QualityMeasureCPICH	- Metric used by UE for CPICH quality measurements
SIntersearch	- Threshold in dB on CPICH Ec/No of current cell for inter-frequency measurements

SIntrasearch	- Threshold in dB on CPICH Ec/No of current cell for intra-frequency measurements
SPrioritySearch1	- Used for cell re-selection, specified in dB, value of (SPrioritySearch1 * 2) yields the actual value
SSearchRAT	- Threshold in dB on CPICH Ec/No of current cell for inter-RAT measurements
ServingCellPriority	- Absolute priority of the serving cell
TReselections	- Time interval in seconds in which criteria must stay fulfilled for a UE to trigger a cell reselection
ThreshServingLow	- Threshold used for cell reselection to lower priority neighbors, specified in dB, value of (ThreshServingLow * 2) yields the actual value
UETxPwrMaxRACH	- UE maximum transmit power level for RACH in dBm

To view the currently configured cell selection values

**Step 1** From the Configuration Mode, issue the following command to view the currently configured cell selection values:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
QualityMeasureCPICH "CPICH Ec/No";
QqualMin           -19;
QRxLevMin          -105;
QHyst1s             0;
QHyst2s             4;
TReselections       2;
SIntrasearch         10;
SIntersearch         2;
SSearchRAT           2;
UETxPwrMaxRACH     21;
IntraFreqQOffset1sn 0;
IntraFreqQOffset2sn 4;
InterFreqQOffset1sn 0;
InterFreqQOffset2sn 50;
InterRatQOffset1sn  50;
```

## 15.3 Enabling Cell Re-Selection from UMTS to LTE

Re-selection from a UMTS to LTE serving cell, when enabled, provides the support that the UE needs to perform cell re-selection from WCDMA to LTE. The LTE frequencies and the parameters for cell re-selection are sent on the broadcast channel in System Information Block type 19 (SIB19). Cell reselection to LTE is supported by E-UTRAN capable UEs in Idle Mode or in Cell\_PCH.

In Step 1 below, the **SPrioritySearch1** parameter is the threshold used in the measurement rules for cell re-selection when absolute priorities are used. It specifies the value of Srxlev in the serving cell controlling the rate of inter-frequency and inter-RAT measurements. **ThreshServingLow** is the threshold used in the measurement rules for cell re-selection to lower priority neighbors when absolute priorities are used. It specifies the limit for Srxlev in the serving cell below which the UE may perform cell reselection to a cell on a lower absolute priority layer.

To enable cell re-selection from UMTS to LTE

**Step 1** From the Configuration Mode, issue the following command to set the parameters for the Information Element UTRA priority information list sent in SIB19 messages. This example sets the:

- **ServingCellPriority:** absolute priority of the service cell to 2.
- **SPrioritySearch1:** threshold in the measurement rules for cell re-selection to 8 dB.
- **ThreshServingLow:** RSCP threshold for the serving cell re-selection to lower priority neighbors to 8. A value of 8 translates to  $-100\text{dBm} \leq \text{RSCP} < -99\text{dBm}$ .

```
set FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection ServingCellPriority 3
SPrioritySearch1 8 ThreshServingLow 8
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP CellSelection
ServingCellPriority 2;
SPrioritySearch1 8;
ThreshServingLow 8;
```

**Step 3** Issue the following command to set the parameters for the inter-RAT reselection to an LTE serving cell.

This example sets the:

- **EUTRACarrierARFCN:** ARFCN of this frequency carrier to 65535.
- **QRxLevMinEUTRA:** required minimum received RSRP level on this E-UTRA frequency carrier to -62 dBm.
- **CellReselectionPriority:** absolute priority of this E-UTRA frequency to 7.
- **ThreshXHigh:** the RSRP threshold for a neighbor on a higher priority E-UTRAN frequency to 30 dB. A value of 30 maps to -81dBm<=RSRP<-80dBm.
- **ThreshXLow:** the RSRP threshold for a neighbor on a lower priority E-UTRAN frequency to 20 dB. A value of 20 maps to -101dBm<=RSRP<-100dBm.

```
set FAPService 1 CellConfig UMTS RAN FDDFAP Mobility IdleMode IRAT LTE Carrier 2
EUTRACarrierARFCN 65535 QRxLevMinEUTRA -62 CellReselectionPriority 7 ThreshXHigh 30
ThreshXLow 20
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP Mobility IdleMode IRAT LTE Carrier
Carrier 2 {
    EUTRACarrierARFCN      65535;
    QRxLevMinEUTRA        -62;
    CellReselectionPriority 7;
    ThreshXHigh            30;
    ThreshXLow             20;
}
```

## 15.4 Enabling LTE Idle Mode Cell Re-Selection

There are four types of idle mode cell re-selection for a UE in motion in an LTE session:

- **Intra-frequency:** to an LTE session on a cell with the same frequency
- **Inter-frequency:** to an LTE session with a different frequency
- **Inter-RAT:** to a UMTS cell
- **Inter-RAT:** to a GSM cell

Intra-frequency cell re-selection default settings will work well in most situations. They rarely need adjusting.

When configuring idle mode re-selection for other types of cell changes, the key parameter is assigning the cell re-selection priority each other cell type. This priority determines when re-selection occurs and to which cell a UE is handed off to.

When a UE enters coverage of a cell with a higher assigned priority relative to the serving cell, the UE will reselect to the higher priority cell if the candidate cell's Reference Signal Received Power (RSRP) minus its *QRxLevMinSIB* parameter is higher than its *ThreshXHigh*.

When the serving cell's priority is higher than that of the new cell, if the serving cell's *RSRP* minus its *QRxLevMinSIB* is less than its *ThreshServingLow* and the candidate cell's *RSRP* minus its *QRxLevMinSIB* is greater than its *ThreshXLow*, the UE camps on the candidate cell.

## To configure LTE idle mode cell re-selection

**Step 1** From the Configuration Mode, issue the following command to configure idle mode inter-frequency cell reselection. This example set and enables:

- the carrier to 1
- E-UTRA Absolute Radio Frequency Channel Number to 2350
- RSRP threshold to -60
- the cell re-selection to 3
- the high threshold to 10
- the low threshold to 23

```
set FAPService 1 CellConfig LTE RAN Mobility IdleMode InterFreq Carrier 1 Enable true
EUTRACarrierARFCN 2350 QRxLevMinSIB5 -60 CellReselectionPriority 3 ThreshXHigh 10
ThreshXLow 23
```

**Step 2** Issue the following command to configure the idle mode intra-frequency cell reselection for UMTS traffic. This example sets and enables:

- number of seconds in which the criteria must stay fulfilled for a UE to trigger a cell reselection to 1
- the UMTS channel frequency to 1
- the UMTS channel number to 662
- RSRP threshold to -60
- the reselection priority to 1
- the high threshold to 0
- the low threshold to 0

```
set FAPService 1 CellConfig LTE RAN Mobility IdleMode IRAT UTRA TReselectionUTRA 1
UTRANFDDFreq 1 Enable true UTRACarrierARFCN 662 QRxLevMin -60 CellReselectionPriority 1
ThreshXHigh 0 ThreshXLow 0
```

**Step 3** Issue the following command to configure the idle mode intra-frequency cell reselection for GSM traffic. This example sets and enables:

- number of seconds in which the criteria must stay fulfilled for a UE to trigger a cell reselection to 1
- the GSM channel frequency to 1
- the GSM band to 850
- the ARFCN to 180
- RSRP threshold to -60
- the reselection priority to 1
- the high threshold to 0
- the low threshold to 0

```
set FAPService 1 CellConfig LTE RAN Mobility IdleMode IRAT GERAN TReselectionGERAN 1
GERANFreqGroup 1 Enable true BandIndicator GSM\ 850 BCCHARFCN 180 QRxLevMin -60
CellReselectionPriority 1 ThreshXHigh 0 ThreshXLow 0
```

**Step 4** Issue the following command to verify the configuration:

```
show FAPService 1 CellConfig LTE RAN Mobility
IdleMode {
    IntraFreq {
        QRxLevMinSIB1      -60;
        QRxLevMinSIB3      -60;
        QRxLevMinOffset     4;
        TReselectionEUTRA   1;
        SNonIntraSearch     0;
        CellReselectionPriority 2;
        PMax                23;
        ThreshServingLow    31;
        SIntrasearch         31;
    }
}
```

```

InterFreq {
    Carrier 2 {
        Enable true;
        EUTRACarrierARFCN 2350;
        QRxLevMinsIB5 -60;
        CellReselectionPriority 3;
        ThreshXHigh 0;
        ThreshXLow 10;
    }
}

IRAT {
    UTRA {
        TReselectionUTRA 1;
        UTRANFDDFreq 1 {
            Enable true;
            UTRACarrierARFCN 662;
            QRxLevMin -60;
            CellReselectionPriority 1;
            ThreshXHigh 0;
            ThreshXLow 0;
            QQualMinSIB6 0;
        }
    }
}

GERAN {
    TReselectionGERAN 1;
    GERANFreqGroup 1 {
        Enable true;
        BandIndicator "GSM 850";
        BCCHARFCN 180;
        QRxLevMin -60;
        CellReselectionPriority 1;
        ThreshXHigh 0;
        ThreshXLow 0;
    }
}
}
}

```

## 15.5 Creating LTE Proximity Detection Cells

The small cell solution permits provisioning a small cell as a proximity detection cell. When the controller detects a session on proximity detection cell, it generates a syslog event that contains the IMSI and the proximity detection cell location information. This syslog event can then be sent to a syslog target server integrated with an application residing on the controller or in the cloud.

The syslog message includes the IMSI, cell ID, cell geographic location (when configured), and eNodeB ID of the controller. No syslog event generates when the IMSI leaves the proximity detection cell. Example use cases include sending a text message to the UE, integrating with a security system to unlock a door, or validating the user's presence at a given time.

The proximity detection cell integrates with a LTE radio network system identically as a standard LTE cell. The UE can be in RRC idle or connected mode when it is close to the proximity detection cell. In connected mode, the UE will go in hard handover with the proximity detection cell.

An event can be raised when a proximity detection cell is added to the UE's active set. To trigger the UE to initiate a session when in idle mode, each proximity detection cell is assigned a unique TAC. The TAC values must be known to the EPC. Upon re-selecting, the UE initiates a location update procedure that can then be used to trigger the syslog event.

## To create a proximity detection cell

**Step 1** From the Configuration mode, issue the following command to configure the TAC of the proximity detection cell. This example enables location reporting on this cell and sets the TAC of cell 66 to 2.

```
set LTECell 66 CellConfig LTE LocationReportingEnable true EPC TACConfigured 2
```

**Step 2** Issue the following command to verify the configuration:

```
show LTECell 66 CellConfig LTE
LocationReportingEnable true;
EPC {
    TACConfigured 2;
}
```





# 16 System Scaling

This chapter contains the following sections:

- [Section 16.1, Configuring UMTS System Session Rates](#) on page 225
- [Section 16.2, Adjusting the UMTS TCP MSS](#) on page 226
- [Section 16.3, Adjusting the LTE TCP MSS](#) on page 228

## 16.1 Configuring UMTS System Session Rates

### 16.1.1 Configuring UMTS Maximum Session Rates

For system stability, Cisco Systems recommends limiting the system-wide number of new UMTS session connections per minute. Once the maximum session rate is reached, additional packet switched sessions are rejected through an RCC Connection Reject message. The default session rate is 1000 sessions per minutes. Setting the session rate below 10 disables the *SYSTEM\_MAX\_SESSION\_RATE\_EXCEEDED* alarm.

Additionally, there is a configurable session rate threshold that is a percentage of the configured system session rate. If this threshold is exceeded, the system rejects all packet switched sessions that are initiated by the user. Packed switched sessions initiated as a response to paging are accepted. The default threshold is 90%. When the *SYSTEM\_MAX\_SESSION\_RATE\_EXCEEDED* multiplied by the *SYSTEM\_NEARING\_MAX\_SESSION\_RATE* parameter is less than 10, the *SYSTEM\_NEARING\_MAX\_SESSION\_RATE* alarm disables. Circuit-switched registration, voice, and emergency calls are always accepted even if the session rate exceeds the rate limit or threshold.

Sessions that exceed the system session rate and session rate threshold trigger a major alarm. The alarm clears when the session rate and threshold drop below their limits.

To configure UMTS system session rates

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> AccessMgmt SessionRateLimiting** command to configure UMTS session rate limiting. This examples sets the number of sessions to 900 and the threshold to 90 percent of the rate limit.

```
set FAPService 1 AccessMgmt SessionRateLimiting MaxSessionRate 900 SessionRateThreshold 90
```

**Step 2** Issue the **show FAPService <ServiceNumber> AccessMgmt SessionRateLimiting** command to verify the configuration:

```
show FAPService 1 AccessMgmt SessionRateLimiting
MaxSessionRate      900;
SessionRateThreshold 90;
```

## 16.1.2 Configuring UMTS System Session Transition Rates

The controller can enforce a maximum RRC transition rate in the system by setting the maximum RRC state transition sessions per minute and whether or not to drop RRC state transition events upon exceeding the threshold. If the rate of RRC transitions exceeds this maximum transmission rate, all RRC transition events to and from the DCH are ignored. The rate monitoring is done at a granularity of 6 second intervals.

To configure UMTS system session transition rates

**Step 1** From the Configuration Mode, issue the following command to enable session transition drops. This example sets the maximum transition rate at 2000 sessions per minute.

```
set FAPService 1 AccessMgmt SessionRateLimiting MaxTransitionRate 2000 EnableTransitionDrop true
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 AccessMgmt SessionRateLimiting
MaxTransitionRate 2000
EnableTransitionDrop true
```

## 16.2 Adjusting the UMTS TCP MSS

Cisco enterprise small cell deployments use IPsec encapsulation between controllers and the security gateway at the mobile operator core network. In addition to IPsec tunneling, user plane voice and data traffic is also encapsulated using RTP and GTP protocols respectively.

With voice traffic, the cost of having a tunnel inside a tunnel is increased overhead. With data traffic there is the added probability that the additional headers could cause packet fragmentation issues due to packets exceeding the maximum MTU size supported by network elements in the traffic path. Packet fragmentation causes throughput degradation and should be avoided.

Each device on a TCP connection agrees upon a packet Maximum Segment Size (MSS) it can receive. The controller supports lowering the TCP MSS of the transiting UE data packets to avoid fragmentation. The packet TCP MSS size applies to all GTP-encapsulated data traffic to the core network, such as UE passthrough or walled garden locally switched traffic. The MSS adjustment is enforced on all new TCP sessions. You can also disable the ability to adjust the TCP MSS.

To automatically adjust the TCP maximum segment size for UE traffic to the core network

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl UMTS PSData** command to adjust the TCP maximum segment size for UE traffic to the core network. This example:

- enables maximum segment size auto-adjusting
- allocates 50 bytes of additional space to account for unknown encapsulation

```
set FAPService 1 FAPControl UMTS PSData TCPMSSAdjustAutoEnable true
TCPMSSAdjustAutoAddEncapOverhead 50
```

**Step 2** Issue the **show FAPService <ServiceNumber> FAPControl UMTS PSData** command to verify the configuration:

```
show FAPService 1 FAPControl UMTS PSData
TCPMSSAdjustAutoEnable          true;
TCPMSSAdjustAutoAddEncapOverhead 50;
```

To adjust the TCP maximum segment size for UE traffic to the core network to a specific size

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl UMTS PSData** command to adjust the TCP maximum segment size for UE traffic to the core network. This example:

- sets the maximum segment size to 500
- disables maximum segment size auto-adjusting

```
set FAPService 1 FAPControl UMTS PSData TCPMSSAdjust 500 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the **show FAPService <ServiceNumber> FAPControl UMTS PSData** command to verify the configuration:

```
show FAPService 1 FAPControl UMTS PSData
TCPMSSAdjust          500;
TCPMSSAdjustAutoEnable    false;
```

To disable all TCP MSS Adjustment for UE traffic to the core network

**Step 1** From the Configuration Mode, issue the following command to disable all TCP MSS adjustment for UE traffic to the core network:

```
set FAPService 1 FAPControl UMTS PSData TCPMSSAdjust 0 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS PSData
TCPMSSAdjust          0;
TCPMSSAdjustAutoEnable    false;
```

To adjust the TCP maximum segment size for locally switched UE traffic

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl UMTS LocalSwitching** command to adjust the TCP maximum segment size for locally switched UE traffic. This example:

- sets the maximum segment size to 500
- disables maximum segment size auto-adjusting

```
set FAPService 1 FAPControl UMTS LocalSwitching TCPMSSAdjust 500 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the **show FAPService <ServiceNumber> FAPControl UMTS LocalSwitching** command to verify the configuration:

```
show FAPService 1 FAPControl UMTS LocalSwitching
TCPMSSAdjust          500;
TCPMSSAdjustAutoEnable    false;
```

To disable all TCP MSS Adjustment for locally switched UE traffic

**Step 1** From the Configuration Mode, issue the following command to disable all TCP MSS adjustment for all locally switched UE traffic:

```
set FAPService 1 FAPControl UMTS LocalSwitching TCPMSSAdjust 0 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl UMTS LocalSwitching
PDPContextTimeout      3600;
TCPMSSAdjust          0;
TCPMSSAdjustAutoEnable    false;
```

To adjust the TCP maximum segment size for non-UE traffic to the core network

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> Transport Tunnel VirtualInterface** command to adjust the TCP maximum segment size for non-UE traffic to the core. This example:

- enables virtual interface 1
- sets the maximum segment size to 500
- disables maximum segment size auto-adjusting
- allocates 50 bytes of additional space to account for unknown encapsulation

```
set FAPService 1 Transport Tunnel VirtualInterface 1 Enable true TCPMSSAdjust 500
TCPMSSAdjustAutoEnable true TCPMSSAdjustAutoAddEncapOverhead 50
```

**Step 2** Issue the **show FAPService <ServiceNumber> Transport Tunnel VirtualInterface** command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface 1
Enable                      true;
DSCPMarkPolicy              -1;
CryptoProfileIndex          1;
SecGWServerIndex            1;
TCPMSSAdjust                500;
TCPMSSAdjustAutoEnable      false;
TCPMSSAdjustAutoAddEncapOverhead 0;
```

To disable all TCP MSS adjustment for non-UE traffic to the core network

**Step 1** From the Configuration Mode, issue the following command to disable all TCP MSS adjustment for non-UE traffic to the core network:

```
set FAPService 1 Transport Tunnel VirtualInterface 1 TCPMSSAdjust 0
TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface 1
TCPMSSAdjust                0;
TCPMSSAdjustAutoEnable      false;
```

## 16.3 Adjusting the LTE TCP MSS

Cisco small cell deployments use IPsec encapsulation between controllers and the security gateway at the mobile operator core network. In addition to IPsec tunneling, user plane voice and data traffic is also encapsulated using RTP and GTP protocols respectively.

With voice traffic, the cost of having a tunnel inside a tunnel is increased overhead. With data traffic there is the added probability that the additional headers could cause packet fragmentation issues due to packets exceeding the maximum MTU size supported by network elements in the traffic path. Packet fragmentation causes throughput degradation and should be avoided.

Each device on a TCP connection agrees upon a packet Maximum Segment Size (MSS) it can receive. The controller supports lowering the TCP MSS of the transiting UE data packets to avoid fragmentation. The packet TCP MSS size applies to all GTP-encapsulated data traffic to the core network, such as UE passthrough or walled garden locally switched traffic. The MSS adjustment is enforced on all new TCP sessions. You can also disable the ability to adjust the TCP MSS.

To automatically adjust the TCP maximum segment size for UE traffic to the core network

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl UMTS PSData** command to adjust the TCP maximum segment size for UE traffic to the core network. This example:

- enables maximum segment size auto-adjusting
- allocates 50 bytes of additional space to account for unknown encapsulation

```
set FAPService 1 FAPControl LTE PSData TCPMSSAdjustAutoEnable true
TCPMSSAdjustAutoAddEncapOverhead 50
```

**Step 2** Issue the **show FAPService <ServiceNumber> FAPControl UMTS PSData** command to verify the configuration:

```
show FAPService 1 FAPControl LTE PSData
TCPMSSAdjustAutoEnable      true;
TCPMSSAdjustAutoAddEncapOverhead 50;
```

To adjust the TCP maximum segment size for UE traffic to the core network to a specific size

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> FAPControl UMTS PSData** command to adjust the TCP maximum segment size for UE traffic to the core network. This example:

- sets the maximum segment size to 500
- disables maximum segment size auto-adjusting

```
set FAPService 1 FAPControl LTE PSData TCPMSSAdjust 500 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the **show FAPService <ServiceNumber> FAPControl LTE PSData** command to verify the configuration:

```
show FAPService 1 FAPControl LTE PSData
TCPMSSAdjust              500;
TCPMSSAdjustAutoEnable     false;
```

To disable all TCP MSS Adjustment for UE traffic to the core network

**Step 1** From the Configuration Mode, issue the following command to disable all TCP MSS adjustment for UE traffic to the core network:

```
set FAPService 1 FAPControl LTE PSData TCPMSSAdjust 0 TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 FAPControl LTE PSData
TCPMSSAdjust              0;
TCPMSSAdjustAutoEnable     false;
```

To adjust the TCP maximum segment size for non-UE traffic to the core network

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> Transport Tunnel VirtualInterface** command to adjust the TCP maximum segment size for non-UE traffic to the core. This example:

- enables virtual interface 1
- sets the maximum segment size to 500
- disables maximum segment size auto-adjusting
- allocates 50 bytes of additional space to account for unknown encapsulation

```
set FAPService 1 Transport Tunnel VirtualInterface 1 Enable true TCPMSSAdjust 500
TCPMSSAdjustAutoEnable true TCPMSSAdjustAutoAddEncapOverhead 50
```

**Step 2** Issue the **show FAPService <ServiceNumber> Transport Tunnel VirtualInterface** command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface 1
Enable                      true;
DSCPMarkPolicy               -1;
CryptoProfileIndex           1;
```

```
SecGWServerIndex          1;
TCPMSSAdjust              500;
TCPMSSAdjustAutoEnable    false;
TCPMSSAdjustAutoAddEncapOverhead 0;
```

To disable all TCP MSS adjustment for non-UE traffic to the core network

**Step 1** From the Configuration Mode, issue the following command to disable all TCP MSS adjustment for non-UE traffic to the core network:

```
set FAPService 1 Transport Tunnel VirtualInterface 1 TCPMSSAdjust 0
TCPMSSAdjustAutoEnable false
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 Transport Tunnel VirtualInterface 1
TCPMSSAdjust          0;
TCPMSSAdjustAutoEnable false;
```



# 17 System Management

This chapter contains the following sections:

- [Section 17.1, Overview](#) on page 231
- [Section 17.2, The Local Configuration Interface](#) on page 231
- [Section 17.3, Fault Management](#) on page 232
- [Section 17.4, User Administration](#) on page 238
- [Section 17.5, SNMP](#) on page 241
- [Section 17.6, Syslog](#) on page 257
- [Section 17.7, Performance Management](#) on page 260

## 17.1 Overview

The small cell solution provides Fault, Configuration, Administration, Performance, and Security (FCAPS) management features required to install, configure, surveil, test, and maintain a network comprised of a controller and its subtended small cells. FCAPS management provides the following services in the small cell solution:

- **Fault:** to identify and isolate existing and potential problems, log their occurrence, and use historical data for trend analysis. Fault is managed through SNMP, syslog, and the CLI as discussed in this chapter.
- **Configuration:** to gather and store information about system components and their configuration, track changes in the network, and provision services. Configuration is managed through the CLI as discussed throughout this manual.
- **Administration:** to configure authorization privileges for internal users, set passwords, and perform software upgrade, backup, and restore. Administration is managed through the CLI as discussed in [Section 17.4, User Administration](#) on page 238.
- **Performance:** to monitor the health of the network and maximize overall performance, minimize down time, identify problems, plot trends, remove bottlenecks, and store historical records of network performance. Performance is monitored through SNMP, XML reports uploads through SCP and FTP, and the CLI as discussed in [Section 17.7, Performance Management](#) on page 260.
- **Security:** to protect the system from unauthorized users and sabotage, authenticate users, control access to the network and its components, and maintain confidentiality of user information. Security is managed through the CLI as discussed in [Chapter 10, "Access Control Topics"](#) on page 161.

## 17.2 The Local Configuration Interface

The Local Configuration Interface (LCI) is a browser-based Graphical User Interface (GUI) intended to assist third-party installers with executing the initial system installation and commissioning process of the Cisco small cell solution. It is a graphical method for configuring objects in the Cisco data model that control the small cell solution. Refer to the *Cisco 8000 Series OS Data Model Reference Guide* for more detailed information about the objects and parameters of the

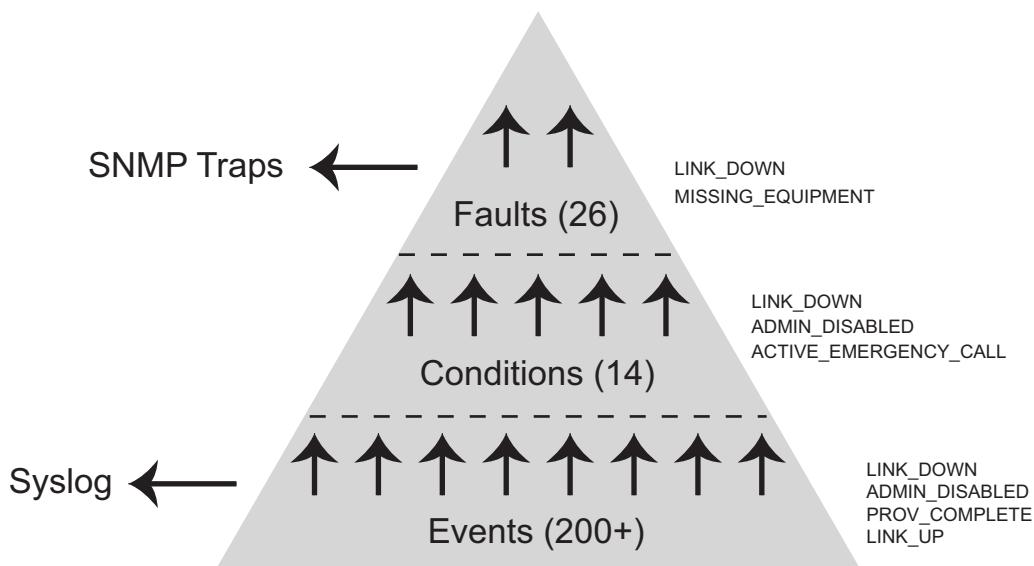
data model. Refer to the *Cisco USC 8000 Series System Commissioning Guide* for information about turning up a Cisco small cell solution with the LCI graphical user interface.

## 17.3 Fault Management

Fault management consists of administering events, conditions, and faults. Some events raise conditions, and some conditions raise faults that trigger alarms. Events, conditions, and faults can be monitored through the CLI.

- **Events:** are notifications that something of interest has happened in the system. All events are transient and have no state. For example, a fan may change speeds. This is important to know, but it does not affect the system operation. Events can be monitored externally through syslog.
- **Conditions:** describe a deviation of the system from normal operation. A condition does not necessarily result in loss of operational capabilities in the system. For example, when an emergency call becomes active, this is a deviation from normal operation but will not result in any loss of operation.
- **Faults:** are conditions that may result in the loss of operational capabilities of the system and requires notifying the administrator. All faults generate SNMP traps and alarms. For example, if the Radio Access Network Application Part (RANAP) connection to the core goes down, this is a deviation from normal operation that results in a complete loss of operation. This would trigger either the RANAP\_CS\_CONNECTION\_TERM or RANAP\_PS\_CONNECTION\_TERM alarm. Faults can be monitored externally through SNMP.

[Figure 43](#) shows the relationship between events, conditions, and faults along with examples:



**Figure 43** Event, Condition, and Fault Relationship

All events, conditions, and alarms have an associated severity. [Table 27](#) shows system severities, their display indicators, and descriptions:

**Table 27: System Severities**

Enumeration	Display	Description
Critical	C	The object associated with the report event is believed to be in a critical condition. Immediate attention is required.
Major	M	A major error condition has occurred. Urgent attention is required.
Minor	m	A minor error condition has occurred. Attention is required.
Warning	W	A warning condition has occurred. Some attention is required.
Info	I	An informational event has occurred.
Trace	T	An event for tracing (debugging) purposes has occurred.

### 17.3.1 Events

All events sent by small cells and applications in the controller are reported to the controller event manager where they are stored. The system supports a list of event groups that are predefined according to the event functions, areas, or natures. An event can belong to more than one event group.

The primary purpose of these groups is to aid the filtering of events during the capturing and/or viewing process. A single event can belong to more than one group. [Table 28](#) contains a list of the predefined groups. Refer to the *Cisco 8000 Series OS Faults, Conditions, and Events Reference Guide* for a list of events in these groups.

**Table 28: Event Groups**

Event Groups	Coverage Descriptions
AdminAAA	Functions related to administrative Authentication, Authorization, and Accounting (AAA).
CBS	Events related to the cell broadcast system of emergency notifications.
CoreNetwork	Functions related to the core network, including both voice and data connections.
Database	Events related to the system configuration.
Diagnostics	Events related to system testing.
Environmental	Events related to fans, equipment temperature, and other environmental aspects of the system.
Equipment	Hardware, ports, controllers, small cells, and firmware.
FileMgmt	Events related to file management.
IP	Events related to IP networking and the controller DHCP server.
LBS	UE location related events (not currently implemented).
LTECallRecord	Events related to LTE call performance events.
PWS	Events related to public warning systems.
RFMgmt	Functions related to the RF aspects of the system.
Routing	Functions related to Layer 3 routing.

**Table 28: Event Groups (continued)**

Event Groups	Coverage Descriptions
Security	Events related to the security of the system.
Session	Functions such as session setup, tear-down, and failure facing user device.
Service	Functions related to Cisco small cell services such as LTE.
TRClient	Events related to the eRMS TR client element management system.
UMTSCallRecord	Events related to UMTS call performance events.
Webmgmt	Events related to web management.

Issue the CLI **show System Event** command from the Operational Mode to retrieve and view the recorded events from the system. This command retrieves and displays the records filtered in the following ways:

- new events to old events
- by event group
- by managed object
- by severity

Events can also be retrieved through syslog. Refer to [Section 17.6, Syslog](#) on page 257 for more information.

### To view current events

**Step 1** From the Operational Mode, issue the **show System Event** command:

#### **show System Event**

```
2012-10-29T22:12:57.865364Z I EVENT_RFMGMT_NLSCE_DISABLED [MOI="System"]
2012-10-29T22:12:53.162351Z W EVENT_RANAP_PS_CONNECTION_TERM [MOI="ServicesNode.1025" IPAddress=0.0.0.0 Port="0"]
2012-10-29T22:12:53.164469Z I EVENT_OPERATIONAL_STATE_CHANGE [MOI="ServicesNode.1025" State="OOS-FAULT"]
2012-10-29T22:12:53.162149Z M EVENT_RANAP_CS_CONNECTION_TERM [MOI="ServicesNode.1025" IPAddress=0.0.0.0 Port="0"]
2012-10-29T22:12:43.215738Z I EVENT_OPERATIONAL_STATE_CHANGE [MOI="LANDevice.1.IPInterface.1" State="IS-NORMAL"]
2012-10-29T22:12:43.212741Z I EVENT_PROV_COMPLETE [MOI="LANDevice.1.IPInterface.1"]
2012-10-29T22:12:43.076580Z I EVENT_OPERATIONAL_STATE_CHANGE [MOI="LANDevice.1" State="IS-NORMAL"]
2012-10-29T22:12:43.076484Z I EVENT_OPERATIONAL_STATE_CHANGE [MOI="LANDevice.1.IPInterface.1" State="OOS-PROVING"]
2012-10-29T22:12:43.073935Z m EVENT_LINK_UP [MOI="LANDevice.1"]
```

The following example filters the current event list to display only events related to the core network connection.

### To filter the current event list

**Step 1** From the Operational Mode, issue the command to view events related to the connection to the core network:

#### **show System Event Groups CoreNetwork**

```
2013-02-04T23:21:58.272330Z I EVENT_RANAP_PS_CONNECTION_EST [MOI="ServicesNode.1025" IPAddress=10.1.11.46 Port="1702"]
2013-02-04T23:21:58.272255Z I EVENT_RANAP_CS_CONNECTION_EST [MOI="ServicesNode.1025" IPAddress=10.1.11.46 Port="1705"]
2013-02-04T23:21:58.194779Z m EVENT_RANAP_PS_CONNECTION_TERM [MOI="ServicesNode.1025" IPAddress=0.0.0.0 Port="0"
CauseString="Unknown"]
2013-02-04T23:21:58.194536Z M EVENT_RANAP_CS_CONNECTION_TERM [MOI="ServicesNode.1025" IPAddress=0.0.0.0 Port="0"
CauseString="Unknown"]
2013-02-04T23:05:10.573809Z I EVENT_RANAP_PS_CONNECTION_EST [MOI="ServicesNode.1025" IPAddress=10.1.11.46 Port="1702"]
2013-02-04T23:05:10.573735Z I EVENT_RANAP_CS_CONNECTION_EST [MOI="ServicesNode.1025" IPAddress=10.1.11.46 Port="1705"]
```

### 17.3.1.1 Anatomy of an Event

All events have the same structural format. For example, the following event:

```
2011-06-29T22:12:43.215738Z I EVENT_OPERATIONAL_STATE_CHANGE
[MOI="LANDevice.1.IPInterface.1" State="IS-NORMAL"]
```

contains the following components:

- **Timestamp:** 2011-06-29T22:12:43.215738Z
- **Severity:** I (informational)

- **Name:** EVENT\_OPERATIONAL\_STATE\_CHANGE
- **Managed object identifier:** MOI="LANDevice.1.IPIInterface.1"
- (Optional) **Argument:** State="IS-NORMAL"

### 17.3.2 Conditions

All conditions have a state and are defined by two events:

- one or more for entering the condition
- one or more for exiting the condition

All conditions contain the following information:

- **Object:** The system object the condition affects.
- **Severity:** The perceived severity as indicated in the event.
- **Name:** The cause for the fault specified in the condition definition file.
- **State:** The current state of the condition.

**Change Time:** Starts out equal to RaisedTime but is updated if the criticality of the alarm changes. By default all conditions are auto-detect/auto-clear: the system automatically detects the presence or absence of the abnormal operation. And when the system exits the abnormal operation the system is allowed to automatically return back to normal operation without administrator control.

#### To view conditions

**Step 1** From the Operational Mode, issue the **show System Condition** command to view the current system conditions:

Object	Severity	Name	State	Change Time
ServicesNode.1025	Major	POWER_SUPPLY_MISSING	Active	2013-03-07T20:22:01Z
LANDevice.3	Major	LINK_DOWN	Active	2013-03-07T20:21:25Z
LANDevice.4	Major	LINK_DOWN	Active	2013-03-07T20:21:25Z
Cell.6	Warning	ADMIN_DISABLED	Active	2013-03-08T01:55:11Z
Cell.9	Warning	ADMIN_DISABLED	Active	2013-03-08T01:55:45Z

### 17.3.3 Alarms

The small cell solution has a hierarchical alarm profile, an alarm higher in the hierarchy masks alarms lower in the hierarchy. The system generates a single alarm for the faulty entity, the other associated lower-level alarms will be suppressed. When the higher alarm is cleared, the system looks at the active faults and re-computes any necessary alarms. If a lower level alarm was posted before a higher level alarm, the lower level alarm will remain active.

Alarm severities are predefined and static. They cannot be changed. You cannot manually clear an alarm, but can prevent an alarm type from being logged and displayed.

If an object is deleted from the system (removed from the configuration), all conditions, faults, and alarms for that object are cleared. Faults and alarms do not persist across a reboot. When a controller boots, it will re-learn and re-post all conditions and faults. From the Operational Mode, issue the **show status OpState System FaultManagement SupportedAlarm** command to display the supported system alarms. [Table 29](#) shows alarms supported in the small

cell solution. Note that OVER\_TEMPERATURE supports three different severities. Refer to the *Cisco 8000 Series OS Faults, Conditions, and Events Reference Guide* for more detailed information about supported alarms.

**Table 29: Supported Alarms**

Alarm	Number	Severity
CALIBRATION_INVALID	106	Major
CELL_MAX_TX_POWER_DELTA_EXCEED	195	Warning
CONFIG_MISMATCH	122	Major
CORE_IPSEC_TERM	130	Major
DB_INVALID	274	Major
DHCP_ALLOCATION_FAILURE	220	Warning
IPSEC_DOWN	74	Major
LINK_DOWN	154	Major
LTE_S1AP_CONNECTION_TERM	346	Major
LOSS_OF_SYNC	98	Major
MISSING_EQUIPMENT	34	Major
MULTIPLE_COOLING_FAN_FAILURES	289	Major
NEIGHBORHOOD_REFERENCE_DELTA	210	Minor
OVER_TEMPERATURE	9	Critical
OVER_TEMPERATURE	10	Major
OVER_TEMPERATURE	11	Minor
POWER_SUPPLY_FAILED	314	Major
POWER_SUPPLY_MISSING	306	Major
PROV_FAULT	50	Major
RANAP_CS_CONNECTION_TERM	58	Major
RANAP_PS_CONNECTION_TERM	67	Minor
RANAP_PS_CONNECTION_TERM	68	Warning
RFMGMT_FAULTED	146	Major
RFMGMT_NLC_REQUIRED	330	Major
RFMGMT_Rem_REQUIRED	322	Major
SOFTWARE_MISMATCH	82	Major
SYSTEM_MAX_SESSION_RATE_EXCEEDED	236	Warning
SYSTEM_NEARING_MAX_SESSION_RATE	228	Warning
UARFCNDL_CHANGED	298	Major

## To view current alarms

**Step 1** From the Operational Mode, issue the **show System Alarm** command to view the current system alarms:

```
show System Alarm
```

Object	Name	ID	Severity	Time
ServicesNode.1025	RANAP_CS_CONNECTION_TERM	806355975	Major	2011-06-29T22:12:53Z
ServicesNode.1025	RANAP_PS_CONNECTION_TERM	806355976	Minor	2011-06-29T22:12:53Z

## To view historical alarms

**Step 1** From the Operational mode, issue the **show System Alarm History** command to view historical alarms. The historical alarm buffer is a fixed size. Once this buffer is full, the oldest alarm data is dropped when new alarms are raised.

```
show System Alarm History
```

Object	ID	Severity	Type	Time
LANDevice.1	553665555	Cleared	ClearedAlarm	2012-08-11T21:09:20.128440Z
LANDevice.1	553665555	Major	NewAlarm	2012-08-11T21:09:15.126453Z
ServicesNode.1025	806355972	Major	NewAlarm	2012-08-11T16:47:11.759171Z
ServicesNode.1025	806355976	Warning	NewAlarm	2012-08-10T16:35:27.244609Z
ServicesNode.1025	806355975	Major	NewAlarm	2012-08-10T16:35:27.244495Z
ServicesNode.1025	806355976	Warning	NewAlarm	2012-08-10T12:19:18.457350Z
ServicesNode.1025	806355975	Major	NewAlarm	2012-08-10T12:19:18.457228Z
RadioNode.555.Radio.1	277529615	Cleared	ClearedAlarm	2012-08-10T12:15:49.841195Z
RadioNode.555.Radio.1	277529615	Major	NewAlarm	2012-08-10T12:15:38.139366Z
RadioNode.555	134786052	Cleared	ClearedAlarm	2012-08-10T12:15:38.111517Z
RadioNode.555	134786052	Major	NewAlarm	2012-08-10T12:14:22.298578Z
ServicesNode.1025	806355972	Major	NewAlarm	2012-08-10T12:10:50.609663Z
RadioNode.108	134328324	Major	NewAlarm	2012-08-10T12:10:50.608646Z
LANDevice.1	553665555	Cleared	ClearedAlarm	2012-08-10T10:15:21.097423Z

[output truncated]

## To disable logging and display of a specified alarm

You can disable the logging of a specific alarm. When logging is disabled, it will not be accounted for in reporting or performance management statistics, and does not display in the output of the **show System Alarm** command. It does display in the output of the **show System Condition** command.

**Step 1** From the Configuration Mode, issue the following command to disable display of a specific alarm. In this example it is alarm number 11, a minor OVER\_TEMPERATURE alarm.

```
set system FaultManagement SupportedAlarm 11 ReportingMechanism Disabled
```

**Step 2** From the Operational Mode, issue the **show status OpState System FaultManagement SupportedAlarm** command to validate the configuration:

```
show status OpState System FaultManagement SupportedAlarm
SupportedAlarm 11 {
    Name          OVER_TEMPERATURE;
    EventType     "Equipment Alarm";
    ProbableCause Indeterminate;
    SpecificProblem "A significant over-temperature condition exists";
    PerceivedSeverity Minor;
    ReportingMechanism Disabled;
}
```

## To re-enable logging and display of a specified alarm

You can re-enable logging and display of a previously disabled alarm.

**Step 1** From the Configuration Mode, issue the following command to re-enable logging of a specific alarm. In this case it is alarm number 11, a minor OVER\_TEMPERATURE alarm.

```
set system FaultManagement SupportedAlarm 11 ReportingMechanism Logged
```

**Step 2** From the Operational Mode, issue the **show status OpState System FaultManagement SupportedAlarm** command to validate the configuration:

```
show status OpState System FaultManagement SupportedAlarm
SupportedAlarm 11 {
    Name          OVER_TEMPERATURE;
    EventType    "Equipment Alarm";
    ProbableCause Indeterminate;
    SpecificProblem "A significant over-temperature condition exists";
    PerceivedSeverity Minor;
    ReportingMechanism Logged;
}
```

## 17.4 User Administration

The small cell solution has two types of users: administrators that configure, surveil, and manage the equipment and services in the network; and the end-user devices that consume voice and data services through UE devices. This section discusses administrative users. Refer to [Chapter 10, “Access Control Topics”](#) on page 161 for information about configuring end-users.

The controller ships with three predefined administrative users: operator administrator, enterprise administrator, and read-only administrator. Each administrative user has its own user group. [Table 30](#) shows the predefined users and their user and group numbers:

**Table 30: Predefined Users and Groups**

User	CLI Name	User Number	Group Number
Operator administrator	admin	9000	900
Read-only administrator	roadmin	9050	905
Enterprise administrator	eadmin	9100	910

The operator administrator can execute all commands. The read-only administrator is restricted to the Operational Mode, and can view configuration, statistical, and log information, and perform a limited number of file management tasks. All read-only administrator tasks are captured in the audit log. [Table 31](#) shows the read-only administrator CLI command permissions:

**Table 31: Read Only Admin Command Permissions**

Commands Allowed	Commands Not Allowed
exit	configure (cannot enter configuration mode)
file archive	display
file copy	file storage
file delete	request airlink
file get	request clear-debug
file list	request core
file match	request lte
file put	request management-server
file show	request port-mirroring

**Table 31: Read Only Admin Command Permissions (continued)**

Commands Allowed	Commands Not Allowed
id	request radionode replace
ping	request scheduled actions
quit	request statistics cell reset
request interface	request statistics delete all
request log bundle	request statistics reset
request log mark	request statistics serviceavailability
request log rotate	request statistics session reset
request log tail	request statistics session rollsnapshot
request message	request statistics syslog
request radionode led	request statistics system reset
request radionode replace	request statistics ue
request set-debug	request system
request statistics cell refresh	request system bootloader update
request statistics refresh all	request system certificate CACert delete
request statistics session refresh	request system database backup
request statistics system refresh	request system database restore
request test mem-dump	request system diagnostics print-mfg-data
request test nmc-dump	request system diagnostics tlv-write
request umts debug	request system
request umts ue	request test add-cell
set autowizard	request test detectedextcell
set complete-on-space	request test detectedneighbor
set idle-timeout	request test ip
set paginate	request test stop-scw
set show	request umts
set system password username roadmin	request umts cell
show	request umts core
source	request umts rem
	request umts self-config
	show configuration
	test

## 17.4.1 Enabling the Read-Only Administrator

The read-only administrator has been created by default but must be enabled before the account becomes active.

To enable the read-only administrator

**Step 1** From the Configuration Mode, issue the following command to enable the read-only administrator:

```
set System AdminAAA User 9050 Enable true
```

**Step 2** Issue the following command to commit the configuration:

```
commit
```

**Step 3** Issue the following command to verify the configuration:

```
show System AdminAAA User
User 9050 {
    Enable          true;
    Description    "Operator administrator";
    Username       roadmin;
    GroupID        905;
}
```

**Step 4** From the Operational Mode, issue the following command to set the read-only administrator password.

```
run set system password username roadmin
Enter new password:
Re-enter new password:
```

## 17.4.2 Editing User Attributes

Users and groups cannot be added or deleted. You can modify user attributes such as password and SNMP community permissions.

To edit user SNMP community attributes

**Step 1** From the Configuration Mode, issue the **set System AdminAAA User** command to edit the user SNMP community attributes. This example sets:

- ♦ the SNMP authentication to the SHA protocol
- ♦ uses the default password of *roadminv3*,
- ♦ sets the SNMP version to *SNMPv3*

```
set System AdminAAA User 9000 Enable true SNMPAuthKeySHA roadminv3 SNMPAuthProtocol
HMACSHAAuthProtocol SNMPPrivProtocol AESCFB128Protocol SNMPPrivKeyDES roadminv3
SNMPVersion [ v3 ]
```

**Step 2** Issue the **show System AdminAAA User** command to verify the configuration:

```
show System AdminAAA User
User 9000 {
    Enable          true;
    SNMPAuthProtocol HMACSHAAuthProtocol;
    SNMPAuthKeySHA $obf$ekkhYPVjAw1TDGA2bg5c;
    SNMPPrivProtocol AESCFB128Protocol;
    SNMPPrivKeyDES $obf$xw+9Eo4qEBFPSnwIBElBWhMJ;
    SNMPVersion     "[ v3 ]";
```

### 17.4.3 Changing User Passwords

Valid user passwords include printable alphanumeric characters. Cisco Systems recommends passwords of at least eight characters with a mixture of numbers and letters. Note that the output of show commands does not return the actual password. It returns an obfuscated text string.

The *admin* user can change its own password, that of *roadmin* and the LCI password. The *roadmin* user can only change its own password.



User names and passwords are case-sensitive.

#### Note

To change a user password

**Step 1** From the Operational Mode, enter the **set system password username** command to change the user password. This example changes the password for the *PWr4Admin* user.

```
set system password username PWr4Admin
```

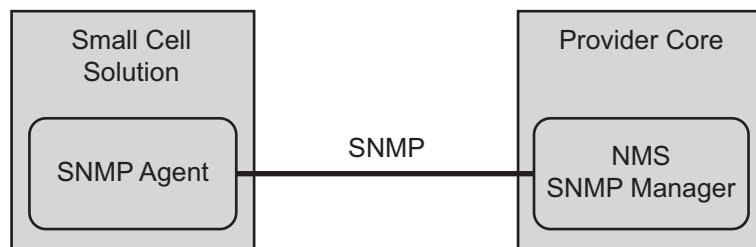
**Step 2** Enter and reenter the new password:

```
Enter new password: <NewPassword>
Re-enter new password: <NewPassword>
```

## 17.5 SNMP

Simple Network Management Protocol (SNMP) is an industry standard, UDP-based protocol for managing and monitoring equipment in an IP network. The controller supports both SNMPv2c and SNMPv3.

One or more devices called managers in the provider core network monitor devices in the Cisco small cell network. The controller in the small cell solution contains an agent that scans for events that require administrative action. The agent translates the appropriate events into SNMP specific format and sends them to the SNMP managers.

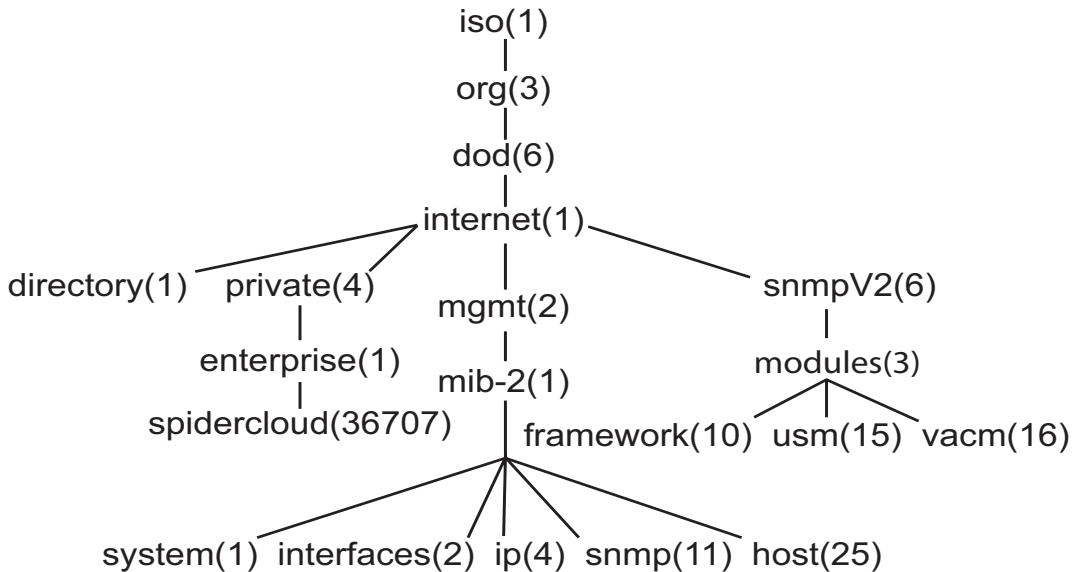


**Figure 44** SNMP Agent and Manager Relationship

Information for the SNMP agent is defined in Management Information Bases (MIBs) that the agent is configured to, recognizes, and supports. A MIB is a database that describes management data structure of the supervised equipment. It contains a set of related managed objects that represent entities in the RAN, such as controllers, small cells, cells, and user equipment. All SNMP data is collected and managed in the controller.

An SNMP manager monitors these entities by reading the values of the MIB objects. The SNMP agent controls access to MIBs through defined communities, groups, and users.

A MIB describes the structure of the RAN using a hierarchical structure of object identifiers, where each object identifier is uniquely associated with a physical component of the RAN. The object identifier is a sequence of integers separated by periods, where each successive integer identifies an object further down in the hierarchy. [Figure 45](#) shows a graphic representation of the MIB tree. In this example, the object identifier `1.3.6.1.2.1.1.1` identifies the `system` object, which is in `mib-2`, which in itself resides in `mgmt` and so forth up to the top level `iso`.



**Figure 45** MIB Tree

### 17.5.1 Supported Standard MIBs

The small cell solution supports the following standard MIBs:

**Table 32: Supported Standard MIBs**

MIB	Description	Filename
ifXTable (RFC-1573)	IP interfaces and statistics.	rfc1573.mib
Ether-MIB (RFC-1643)	Ethernet interface details.	rfc1643.mib
HOST-RESOURCES-MIB (RFC-2790)	Controller hardware status information.	rfc2790.mib
Interfaces MIB (RFC-2863)	IP interfaces and statistics.	rfc2863.mib
MIB-II (RFC-1213)	System details and enterprise OIDs.	rfc1213.mib
SNMP MIB v2 (RFC-1907)	SNMPv2 details and statistics.	rfc1907.mib
SNMP MIB v3 (RFC-3411)	SNMPv3 details and statistics.	rfc3411.mib
SNMP-FRAMEWORK MIB (RFC-3411)	SNMPv3 user creation and security.	rfc3411.mib
SNMP-USM-MIB (RFC-3414)	User security model.	rfc3414.mib
SNMP-VACM-MIB (RFC-3415)	User-based access control.	rfc3415.mib

### 17.5.2 Standard Supported Traps

The small cell solution supports the following standard traps as per RFC 1215:

- authenticationFailure

- coldStart
- linkDown
- linkUp
- warmStart

The system automatically generates these traps when SNMP is enabled and at least one trap target is active. They can be enabled or disabled globally, and are enabled by default. The CLI does not display these standard traps and they are not logged in the system. Refer to [Section 17.5.3, Standard Trap Details](#) on page 243 for more information about the supported standard traps. Refer to [Table 29](#) on page 236 and the *Cisco 8000 Series OS Faults, Conditions, and Events Reference Guide* for more information about supported alarms related to SNMP traps.

## 17.5.3 Standard Trap Details

This section provides details about standard RFC 1215 traps supported by the small cell solution.

### 17.5.3.1 authenticationFailure

- **Alarm Number/Registered at OID:** .1.3.6.1.6.3.1.1.5.5 (SNMP MIB v2)
- **Description:** The message received from the SNMP manager cannot be authenticated due to an invalid community string, username, password, or encryption key.
- **Default Severity:** None, configurable through the eRMS management system.
- **Entered Event:** None
- **Exit Event:** None
- **Managed Objects:** ServicesNode
- **System Actions:** Records details in the debug log.
- **Operational State Changes:** None
- **Corrective Action:** Ensure that there are no password violations.

### 17.5.3.2 coldStart

- **Alarm Number/Registered at OID:** .1.3.6.1.6.3.1.1.5.1 (SNMP MIB v2)
- **Description:** The SNMP agent re-initialized itself with possible changes to the configuration.
- **Default Severity:** None, configurable through the eRMS management system.
- **Entered Event:** None
- **Exit Event:** None
- **Managed Objects:** ServicesNode
- **System Actions:** Re-sends all current alarms to configured trap targets.
- **Operational State Changes:** Returns to in service or maintenance state.
- **Corrective Action:** Inspect the controller log to determine the cause of the cold start.

### 17.5.3.3 linkDown

- **Alarm Number/Registered at OID:** .1.3.6.1.6.3.1.1.5.3 (IF-MIB)
- **Description:** Link is not available on a front panel port.
- **Default Severity:** Major

- **Entered Event:** LINK\_DOWN
- **Exit Event:** LINK\_UP
- **Managed Objects:** LANDevice, IPInterface, ifIndex
- **System Actions:** The LANDevice is faulted, an alarm is raised, and an SNMP trap is sent out.
- **Operational State Changes:** The port will enter OOS-FAULT. Child objects are set to OOS-INHERITED.
- **Corrective Action:** Check connectivity and cabling of Ethernet port.

#### 17.5.3.4 linkUp

- **Alarm Number/Registered at OID:** .1.3.6.1.6.3.1.1.5.4 (IF-MIB)
- **Description:** The state of a network adapter on the SNMP agent changed from down to up.
- **Default Severity:** None, configurable through the eRMS management system.
- **Entered Event:** LINK\_UP
- **Exit Event:** LINK\_DOWN
- **Managed Objects:** LANDevice, IPInterface, ifIndex
- **System Actions:** The linkDown alarm clears.
- **Operational State Changes:** The port will enter an IS state.
- **Corrective Action:** None

#### 17.5.3.5 warmStart

- **Alarm Number/Registered at OID:** .1.3.6.1.6.3.1.1.5.2 (SNMP MIB v2)
- **Description:** The SNMP agent re-initialized itself with no changes to the configuration.
- **Default Severity:** None, configurable through the eRMS management system.
- **Entered Event:** None
- **Exit Event:** None
- **Managed Objects:** ServicesNode
- **System Actions:** Sends warmStart trap to defined trap targets.
- **Operational State Changes:** Returns to in service or maintenance state.
- **Corrective Action:** Inspect the controller log to determine the cause of the warm start.

### 17.5.4 Small Cell Solution Proprietary MIBs

The small cell solution supports the following proprietary MIBs:

**Table 33: USC 8088 Controller Proprietary MIBs**

MIB	Description	Filename
ERAN-CONFIG-MIB	Controller system configuration data.	ERAN-CONFIG-MIB.txt
ERAN-MIB	Root MIB for specific product release.	ERAN-MIB.txt
ERAN-SMI-MIB	Root MIB for product specific hooks enterprise.	ERAN-SMI-MIB.txt
ERAN-STATS-MIB	UMTS and LTE KPI, air interfaces, controllers, small cells, cells.	ERAN-STATS-MIB.txt

**Table 33: USC 8088 Controller Proprietary MIBs**

MIB	Description	Filename
ERAN-SYSTEM-MIB	Current UMTS and LTE alarm list and system configuration.	ERAN-SYSTEM-MIB.txt
ERAN-TC	Cisco product specific textual conventions.	ERAN-TC.txt
ERAN-TRAP-MIB	UMTS, LTE and controller alarms.	ERAN-TRAP-MIB.txt

Contact your Cisco representative for copies of the standard and any proprietary MIBs.

### 17.5.5 Small Cell Solution Traps Parameters

The OS enterprise traps are defined in the ERAN-TRAP-MIB that contains the following parameters:

**Table 34: ERAN-TRAP-MIB Parameters**

Trap Parameters	Definition
additionalInformation	Additional trap information including System.Name and System.Location
additionalText	Vendor defined text string
alarmChangedTime	Date and time alarm was last changed
alarmIdentifier	Unique alarm identifier
alarmRaisedTime	Date and time alarm was first raised
eventType	Type of system event
extTrapDet	Information about the alarm being forwarded from a non-Cisco enterprise small cell device, such as a router
managedObjectInstance	Object against which the alarm was raised
perceivedSeverity	Indicates the level of alarm urgency
probableCause	Qualifies the alarm and adds additional information to eventType
specificProblem	Further qualifies the alarm and adds additional information to eventType and probableCause

### 17.5.6 Small Cell Solution Trap Messages

It also supports the following proprietary ERAN-TRAP-MIB trap messages from controllers. These events contain the additionalInformation Value: "System.Name=<value>" and " System.Location=<value>".

- eranNotifCalibrationInvalid
- eranNotifCellMaxPowerDeltaExceeded
- eranNotifConfigMismatch
- eranNotifCoreIpsecTerm
- eranNotifDbInvalid
- eranNotifDhcpAllocationFailure
- eranNotifFwdMsg

- eranNotifIpsecDown
- eranNotifLinkDown
- eranNotifLteS1APConnectionTerm
- eranNotifLossOfSync
- eranNotifMissingEquipment
- eranNotifMultipleCoolingFanFailures
- eranNotifNeighborhoodReferenceDelta
- eranNotifOverTemperature
- eranNotifPowerSupplyFailed
- eranNotifPowerSupplyMissing
- eranNotifProvFault
- eranNotifRanapCsConnectionTerm
- eranNotifRanapPsConnectionTerm
- eranNotifRfMgmtFaulted
- eranNotifRfMgmtNlcRequired
- eranNotifRfMgmtRemRequired
- eranNotifRfMgmtRfmgmtSuboptimalAssignmentOfPcisDetected
- eranNotifSoftwareMismatch
- eranNotifRfMgmtSuboptimalAssignmentOfPcisDetected
- eranNotifSystemMaxSessionRateExceeded
- eranNotifSystemNearingMaxSessionRate
- eranNotifTestTrap
- eranNotifUarfndlChanged

## 17.5.7 Supported SNMP Operations

The system supports the following SNMP Operations:

- SNMPv2c and SNMPv3 asynchronous event notifications (Traps)
- SNMPv2c and SNMPv3 Get Requests (GetRequest, GetNextRequest, GetBulkRequest)
- InformRequestv2
- InformRequestv3 engineld, authentication and encryption
- ReportPDU
- ResponsePDU
- SNMPv2-Trap
- SNMPv3-Trap engineld, authentication and encryption

## 17.5.8 Enabling SNMP and Setting the SNMP Version

Administrators can enable SNMP and set the version that the controller uses to generate traps. The controller can be configured to use SNMPv2c only, SNMPv3 only, or both SNMPv2c and SNMPv3.

To set the SNMP version

**Step 1** From the Configuration Mode, issue the **set System SNMP Version** command to enable SNMP and set the system-wide SNMP version. This example sets the version to both v2c and v3.

```
set System SNMP Enable true Version [ v2c v3 ]
```

**Step 2** Issue the **show System SNMP** command to verify the configuration:

```
show System SNMP
Enable true;
Version "[ v2c v3 ]";
```

## 17.5.9 Configuring SNMP System Parameters

Set the values of the following MIB 2 system parameters for each controller:

**Table 35: MIB 2 System Parameters**

Trap	Definition
sysContact	System contact information
sysName	Name of the system. It defaults to system host name.
sysLocation	System location

To configure MIB 2 system parameters for a controller

**Step 1** From the Configuration Mode, issue the **set System** command to configure the system parameters. In this example, the description is *ERAN OS Ver:2.1.0*, contact *Kim*, name *SCW1*, and location *Main\_Office*.

```
set System Description ERAN OS Ver:3.0.0 Contact Kim Name SCW1 Location Main
_Office
```

**Step 2** Issue the **show System** command to verify the configuration:

```
show System
Description ERAN OS Ver:3.3.0;
Contact Kim;
Name SCW1;
Location Main_Office;
```

## 17.5.10 Viewing SNMP Parameters

To view SNMP parameters

**Step 1** From the Operational Mode, issue the following command to display the SNMP parameters:

```
show status OpState System SNMP
Enable true;
Version "[ v2c ]";
LocalEngine 0x80001f8803002448003120;
```

## 17.5.11 Viewing the SNMP Configuration

The system supports configuration monitoring with any standard MIB browser or walk tool using the Get commands listed in [Section 17.5.7, Supported SNMP Operations](#) on page 246.

## 17.5.12 Trap Forwarding for Third-Party Devices

The controller acts as an SNMP proxy agent by forwarding traps from managed third-party devices such as routers and switches to its defined trap targets in the operator core network. The controller accepts SNMPv2c traps and forwards them to the target in the format configured for the trap target. This feature is automatically enabled and requires no configuration on the controller. Third-party devices may need to be configured to send traps to the controller in SNMPv2c format.

## 17.5.13 Disabling and Reactivating the SNMP Agent

SNMP is active by default. You can disable the SNMP agent if needed and re-enable it at a later time. Disabling the SNMP agent will stop the system from responding to SNMP Gets, but does not affect SNMP trap notifications. Refer to [Section 17.5.20, Disabling SNMP Trap Notifications](#) on page 255 for information about disabling SNMP trap notifications.

To disable the SNMP agent

**Step 1** From the Configuration Mode, issue the **set System SNMP Enable false** command to disable SNMP notifications:

```
set System SNMP Enable false
```

**Step 2** Issue the **commit** command to commit the changes:

```
commit
```

**Step 3** Issue the **show System SNMP Enable** command to verify the configuration:

```
show System SNMP Enable
Enable false;
```

To reactivate the SNMP agent

**Step 1** From the Configuration Mode, issue the **set System SNMP Enable true** command to reactivate SNMP Gets:

```
set System SNMP Enable true
```

**Step 2** Issue the **commit** command to commit the changes:

```
commit
```

**Step 3** Issue the **show System SNMP Enable** command to verify the configuration:

```
show System SNMP Enable
Enable true;
```

## 17.5.14 Monitoring Ports and Interfaces

From the network management system or operations center, assign ports to be monitored on the controller. This adds the ports and IP interfaces to the *ifTable*, *ifXTable*, and *ipAddrTable* of MIB-II. Deleting ports removes this information.

The controller supports up to 512 logical IP interfaces, each with a unique IP address. Each port and interface has a unique *ifIndex* number, which is assigned using the following formulas:

- **Port:** Actual port number multiple of 256. For example, Port 1 is 256. Port 2 is 512. Port 8 is 2048.

- **Logical interface:** Port interface number plus the number of the interface. For example, Port 1, logical interface 1 is 257 (256 + 1). Port 1, logical interface 2 is 258 (256 + 2). Port 5, interface 15 is 1295 (1280 + 15).

View the status of the interface through the *LANHostConfigManagement* of the ifIndex. Setting the *LANHostConfigManagement* to up in the CLI brings activates service to the port. Setting the *LANHostConfigManagement* to down removes the port from service. All port status changes are reported as linkUp or linkDown.

If the port is administratively placed into maintenance state, the SNMP status is *unknown*. Ports with an unknown status have no write access, and cannot be restored or removed.

## 17.5.15 Configuring SNMP Trap Targets

SNMP traps are asynchronous messages that report significant events in the system. An SNMP management system can receive traps that represent alarms by registering as a listener. It then receives traps for all standing conditions reported to the system. The administrator can then take corrective action to return the system to optimal performance.

Configure the controller to send SNMP traps on remote servers by defining the IP address, port, community string, and SNMP version number (SNMPv2c or SNMPv3) of the receiving trap servers. The system defaults to SNMPv2c, port 162, and community string *public*. Up to ten trap servers can be defined, but only four can be enabled at one time.

The following six parameters apply to the SNMPv3 remote trap target:

- InformAuthKey
- InformAuthProtocol
- InformPrivKey
- InformPrivProtocol
- RemoteEngine
- RemoteUser

Provide the *RemoteEngine* parameter value if possible. If it is not provided, the SNMP agent will try to discover the NMS identifier.

Every alarm will generate a trap to all enabled trap targets. All trap targets receive all generated traps.

### To enable SNMP trap targets

**Step 1** From the Configuration Mode, issue the **set System EventManagement Target** command to configure the parameters of the remote server that will receive the SNMP traps. The value of the target is an positive integer. In this example:

- trap target 22
- with the IP address 10.22.1.1
- on port 162
- uses SNMP version 3
- with MD5 authentication.

Note that the output of show commands does not returns the actual authentication keys. It returns an obfuscated text string.

```
set System EventManagement Target 22 SNMPTrap Enable true Community public RemoteUser
admin RemoteEngine 0x8000270f0401 IPAddress 10.22.1.1 Port 162 Version v3 NotifyType
Inform InformAuthKeyMD5 roadminv3 InformAuthProtocol HMACMD5AuthProtocol
InformPrivKeyAES roadminv3 InformPrivProtocol AESCFB128Protocol
```

**Step 2** Issue the **show configuration System EventManagement Target** command from the Operational Mode to display information about the SNMP trap remote host configuration:

```
show System EventManagement Target
Target 22 {
    SNMPTrap {
        Enable          true;
        IPAddress      10.22.1.1;
        Port            162;
        Community       public;
        RemoteUser      admin;
        RemoteEngine    0x8000270f0401;
        Version         v3;
        InformAuthProtocol HMACMD5AuthProtocol;
        InformAuthKeyMD5 $obf$0/fGiJ0MQkAHIwQjXjsD;
        InformPrivProtocol AESCFB128Protocol;
        InformPrivKeyAES $obf$uyV8yq5wBxY3XBQYwFG;
        NotifyType      Inform;
    }
}
```

**Step 3** Issue the **set System SNMP Enable true** to enable SNMP in the controller:

```
set System SNMP Enable true
```

**Step 4** Issue the **show System SNMP** command to verify the configuration:

```
show System SNMP
Enable true;
```

To enable SNMP trap targets when using a forwarding group

**Step 1** From the Configuration Mode, issue the **set System EventManagement Target** command to configure the parameters of the remote server that will receive the SNMP traps. The value of the target is an positive integer. In this example:

- trap target 22
- with the IP address 10.22.1.1
- with forwarding group 3
- on port 162
- uses SNMP version 3
- with *MD5* authentication.

Note that the output of show commands does not returns the actual authentication keys. It returns an obfuscated text string.

```
set System EventManagement Target 33 SNMPTrap Enable true ForwardingGroupIndex 3 IPAddress
10.33.1.1 Port 162 Community public RemoteUser admin RemoteEngine 0x8000270f0401 Version
v3 InformAuthProtocol HMACMD5AuthProtocol InformAuthKeyMD5 $obf$0/fGiJ0MQkAHIwQjXjsD
InformPrivProtocol AESCFB128Protocol InformPrivKeyAES $obf$uyV8yq5wBxY3XBQYwFG
NotifyType Inform
```

**Step 2** Issue the **show configuration System EventManagement Target** command from the Operational Mode to display information about the SNMP trap remote host configuration:

```
show System EventManagement Target
Target 33 {
    SNMPTrap {
        Enable          true;
        Description     "";
        IPAddress      10.33.1.1;
        ForwardingGroupIndex 3;
        Port            162;
        Community       public;
        RemoteUser      admin;
        RemoteEngine    0x8000270f0401;
```

```

    Version          v3;
    InformAuthProtocol HMACMD5AuthProtocol;
    InformAuthKeyMD5 $obf$0/fGiJ0MQkAHIwQjXjsD;
    InformAuthKeySHA "";
    InformPrivProtocol AESCFB128Protocol;
    InformPrivKeyDES "";
    InformPrivKeyAES $obf$uyV8yq5wBxY3XBQYWwFG;
    NotifyType      Inform;
}
}

```

**Step 3** Issue the **set System SNMP Enable true** to enable SNMP in the controller:

```
set System SNMP Enable true
```

**Step 4** Issue the **show System SNMP** command to verify the configuration:

```
show System SNMP
Enable true;
```

## 17.5.16 Example Trap Target Configurations

The following examples show typical trap target configurations.

### 17.5.16.1 Example SNMP v2c Traps or Inform Targets

```
show System EventManagement Target 1 SNMPTrap
Enable           true;
IPAddress       10.1.11.37;
ForwardingGroupIndex 3;
Port             162;
Community       public;
Version          v2c;
InformAuthProtocol NoAuthProtocol;
InformPrivProtocol NoPrivProtocol;
NotifyType      [Trap/Infrom];
```

### 17.5.16.2 Example SNMP v3 Trap Targets

```
show System EventManagement Target 2 SNMPTrap
Enable           true;
IPAddress       10.1.11.38;
Port             162;
Community       public;
RemoteUser      admin;
InformAuthProtocol HMACMD5AuthProtocol;
InformAuthKeyMD5 $obf$yRzGB2FPLT8VFyNBNScWIB52;
InformPrivProtocol AESCFB128Protocol;
InformPrivKeyAES $obf$BUpZgbxrFjgfCgYRCwUtJxRo;
Version          v3;
NotifyType      Trap;
```

The SNMP v3 trap uses the following parameters from the AAA admin user that were configured in [Section 17.4.2, Editing User Attributes](#) on page 240. These values should match the values configured in [Section 17.5.15, Configuring SNMP Trap Targets](#) on page 249.

```
show System AdminAAA User 9000
Enable           true;
SNMPAuthProtocol HMACMD5AuthProtocol;
SNMPAuthKeyMD5  $obf$ZiJiTQZKAYrDTk/Pyxp;
SNMPAuthKeySHA  $obf$3hU6kOGVQQc0UgYmKSAA;
SNMPPrivProtocol DESPrivProtocol;
SNMPPrivKeyDES  $obf$5KsXFLQ4RyQSPCs1P0IG;
```

```
SNMPPrivateKeyAES      $obf$GBLtWgoZNS0tEDoOASx0;
SNMPVersion           "[ v2c v3 ]";
```

### 17.5.16.3 Example SNMP v3 Inform Targets

```
show System EventManagement Target 3 SNMPTrap
Enable          true;
IPAddress       10.1.11.39;
ForwardingGroupIndex 3;
Port            162;
RemoteUser      admin;
RemoteEngine    0x8000270f0401;
Version         v3;
InformAuthProtocol HMACMD5AuthProtocol;
InformAuthKeyMD5 $obf$cnBULpd0EQEjMSEZCh1Q;
InformPrivProtocol DESPrivProtocol;
InformPrivKeyDES $obf$8vi+s14EShkITx5YWjML;
NotifyType      Inform;
```

## 17.5.17 Generating Test SNMP Traps

You can generate SNMP traps between the controller and the northbound NMS. This can be a handy way to test the path to the trap target without the disruption of creating a condition that generates an actual alarm.

You can generate any single trap, generate all system traps, or generate supported RFC 1215 standard traps to verify that the trap target receives them. Traps are sent in SNMPv2c or SNMPv3 format based upon the format selected in [Section 17.5.15, Configuring SNMP Trap Targets on page 249](#).

### 17.5.17.1 Generating a Test SNMP Trap for All Trap Targets

You can generate a test SNMP trap that is sent to all defined SNMP trap targets.

To generate a test SNMP trap

**Step 1** From the Operational Mode, issue the following command to send a test trap to all defined trap targets:

```
request test snmp trap name EranNotifTest
status : snmp test trap(s) sent
```

### 17.5.17.2 Generating a Test SNMP Trap to a Defined Trap Target

You can generate a test SNMP trap that is sent to a designated trap target.

To generate a test SNMP trap to a defined target

**Step 1** From the Operational Mode, issue the following command to generate a test SNMP trap to a single defined target. The following example sends the test trap to trap target 1.

```
request test snmp trap name EranNotifTest target 1
status : snmp test trap(s) sent
```

### 17.5.17.3 Generating All SNMP Traps

You can generate all SNMP traps and have them forwarded to one or all defined trap targets.

To generate all SNMP traps

**Step 1** From the Operational Mode, issue the following command to generate all SNMP traps and send them to trap targets. This example sends all traps to trap target 1.

```
request test snmp trap name EranNotifAll target 1
status : snmp test trap(s) sent
```

#### 17.5.17.4 Generating SNMP Traps of a Defined Severity

You can generate one or all SNMP traps of a defined severity.

##### To generate all SNMP traps of a defined severity

- Step 1** From the Operational Mode, issue the following command to generate SNMP traps of a given severity. The following example uses the severity *Critical* and sends them to all trap targets.

```
request test snmp trap severity Critical name EranNotifAll
status : snmp test trap(s) sent
```

#### 17.5.17.5 Clearing All SNMP Traps

For troubleshooting purposes it is handy to clear all SNMP traps.

##### To clear all SNMP traps

- Step 1** From the Operational Mode, issue the following command to clear all SNMP traps.

```
request test snmp trap name EranNotifAll severity Clear
status : snmp test trap(s) sent
```

#### 17.5.17.6 Clearing a Defined SNMP Trap

You can clear an individual SNMP trap.

##### To clear a defined SNMP trap

- Step 1** From the Operational Mode, issue the following command to clear a specific trap. The following example clears the missing power supply trap.

```
request test snmp trap name EranNotifPowerSupplyMissing severity Clear
status : snmp test trap(s) sent
```

#### 17.5.17.7 Generating Standard Traps

You can generate a single standard trap or all standard traps supported from RFC 1215. Refer to [Section 17.5.15, Configuring SNMP Trap Targets](#) on page 249 for a list of standard traps supported by the small cell solution.

##### To generate RFC 1215 standard traps

- Step 1** From the Operational Mode, issue the following command to generate RFC 1215 standard traps. The following example generates all supported standard traps and sends them to trap target 1.

```
request test snmp trap name EranNotifStdAll target 1
status : snmp test trap(s) sent
```

#### 17.5.18 Configuring SNMP Source Address Filtering

Administrators can filter requests for SNMP services by defining an access control filter that specifies one virtual interface and/or one or more source host and subnet that are allowed access while ignoring requests that are not on the filter list. If the access control list is not created or enabled, the controller responds to all requests.

If one parameter is specified, only traffic from that virtual interface or host is allowed. If multiple parameters are specified, the filter internally uses the logical AND operation. This means that when multiple parameters are defined, requests must match all parameters to have access to the SNMP services.

The virtual interface associates the IPsec tunnel with the crypto profile and security gateway. Any specified virtual interface must be previously configured with the **set FAPService 1 Transport Tunnel VirtualInterface** command as shown in [Section 4.3, Configuring IPsec to the Core Network](#) on page 56. You can provision up to 3 virtual

interfaces and 16 allowed source subnets.

### To configure SNMP source address filtering

- Step 1** From the Configuration Mode, issue the **set System SNMP AccessControl** command to configure the access control list. This example defines virtual interface 1, and specifies a single host and subnet pair with an IP address 172.17.3.0 and subnet mask of 255.255.255.0.

```
set System SNMP AccessControl VirtualInterface [ 1 ] AllowedSource 1 SourceIP 172.17.3.0
SourceMask 255.255.255.0 Enable true
```

- Step 2** Issue the **show System SNMP AccessControl** command to verify the configuration:

```
show System SNMP AccessControl
VirtualInterface "[ 1 ]";
AllowedSource 1 {
    Enable      true;
    SourceIP   172.17.3.0;
    SourceMask 255.255.255.0;
}
```

## 17.5.19 Viewing SNMP Inform Statistics

SNMPv2c and SNMPv3 statistics can be viewed with the **show status OpState System EventManagement Target** command. The output includes the following inform statistics:

- **InformsDropped:** Dropped internally without attempting to send due to reasons such as queue full, thread count, too many targets or target not reachable.
- **InformsFailed:** Acknowledgement is not received after a timeout or given number of retries.
- **InformsSent:** Successfully sent and acknowledged Inform trap messages.

### To view the SNMP Inform statistics

- Step 1** From the Operational Mode, issue the **show status OpState System EventManagement Target** command to view the status of all configured SNMP informs:

```
show status OpState System EventManagement Target
Target 1 {
    SNMPTrap {
        Enable      true;
        NotifyType  Inform;
        Community   public;
        Version     v2c;
        InformsSent 12;
        InformsFailed 5;
        InformsDropped 8;
    }
}
Target 2 {
}
SNMPTrap {
    Enable      true;
    Community   public;
    Version     v3;
    NotifyType  Inform;
    InformsSent 0;
    InformsFailed 2;
    InformsDropped 7;
}
}
Target 3 {
    SNMPTrap {
        Enable      true;
```

```

        Community      public;
        Version        v2c;
        NotifyType     Inform;
        InformsSent    0;
        InformsFailed  1;
        InformsDropped 8;
    }
}
Target 4 {
    SNMPTrap {
        Enable         true;
        Community     public;
        Version        v2c;
        NotifyType     Inform;
        InformsSent    0;
        InformsFailed  1;
        InformsDropped 8;
    }
}

```

## 17.5.20 Disabling SNMP Trap Notifications

Disabling SNMP trap notifications for a given target halts the sending of traps to that trap target. This does not affect the SNMP agent from responding to SNMP Gets to the SNMP manager. Refer to [Section 17.5.13, Disabling and Reactivating the SNMP Agent](#) on page 248 for information about disabling and reactivating the SNMP agent.

To disable SNMP trap notifications

**Step 1** From the Configuration Mode, issue the **set System EventManagement Target <TrapNumber> SNMPTrap Enable false** command to disable SNMP trap notifications for a specific trap. This example uses trap 22.

```
set System EventManagement Target 22 SNMPTrap Enable false
```

**Step 2** Issue the **show System EventManagement Target** command to verify the configuration:

```
show System EventManagement Target
Target 22 {
    SNMPTrap {
        Enable         false;
    }
}
```

## 17.5.21 SNMP Authentication, Authorization, and Accounting

The OS supports two types of SNMP administrator:

- **admin:** The service provider administrator that has read-only permissions to all SNMP system objects, services, and supported MIBs. This type of administrator accesses the controller from the provider core network through the core IPsec tunnel.
- **e-admin:** The enterprise administrator that has read-only permissions to a defined set of SNMP system objects, services, and supported MIBs. This type of administrator accesses the controller from the enterprise network.

The admin user has access to the following MIB information:

**Allowed (Standard MIBs):**

- .iso(1).org(3).dod(6).internet(1).directory(1)

- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip (4).ipAddrTable(20)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).icmp(5)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).tcp(6)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).udp(7)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).snmp(11)

#### Host-RESOURCES::CPU

- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrSystem(1)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrStorage(2)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrDevice(3)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrSwRunPerf(5)

#### Private MIBs

- .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).spidercloud(36707).products(1).servicesNode(1).eranMIB(1)

The e-admin user has access to a subset of the following MIB information:

#### Allowed (Standard MIBs):

- .iso(1).org(3).dod(6).internet(1).directory(1)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip (4).ipAddrTable(20)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).snmp(11)

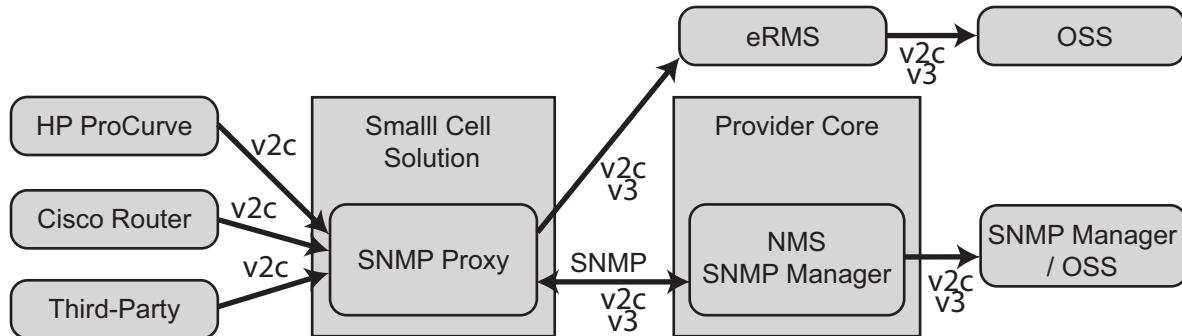
#### Host-RESOURCES::CPU

- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrSystem(1)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrStorage(2)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrDevice(3)
- .iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).host(25).hrSwRunPerf(5)

### 17.5.22 SNMP Proxy

The SNMP proxy is used to receive traps from third-party devices such as HP ProCurve switches and Cisco routers and forwards them northbound to the eRMS management system and the operator OSS in the core network. The trap sending device must be configured to send traps to the controller in 2vc format. The controller can forward traps in either 2vc or v3 format and forwarded as an event message *eranNotifFwdMsg*.

If there are multiple trap targets configured for the controller, the forwarded traps are converted to the format configured for that target. Messages can be suppressed at the controller or eRMS level. Refer to documentation from the third-party device for information about configuring the device to forward traps in v2c format.



**Figure 46** SNMP Proxy Logical Configuration

## 17.6 Syslog

The system can be configured to enable the delivery of its captured events to one or more remote syslog servers. The controller syslog client uses UDP transport for delivery of messages to any reachable defined target over port 514 or proprietary configured port. The syslog client has user-configurable event filters, which can be defined differently for each target.

Syslog messages are delivered in a best effort fashion, without any guarantee of delivery. Similarly, the order of messages at the server is not guaranteed. The system syslog messages can be delivered over a secure IPsec tunnel to the mobile-core or openly over a local enterprise LAN interface to the enterprise network, with no encryption, certification, or authentication.

The system invokes the syslog client whenever an event is generated. The client forwards events to targets according to filtering rules. Since filtering information is specific for each target specific event may be forwarded to one target but not to another.

A forwarded event is converted to the format defined in RFC 5424, as shown below. RFC 5424 is backwardly compatible to previous syslog implementations.

```

<30>1 2011-05-26T21:51:56.808260Z ws-pat -- EVENT_SCSN_STARTED [scos@36707
MOI="ServicesNode.1025" Name="ws-nova.int.spidercloud.com"
SCOSVersion="1.6.0.DevBld.6272" BuildTime="Wed May 25 15:19:20 2011 PDT"]

<30>1 2011-05-26T21:51:56.808260Z --- EVENT_SCSN_STARTED [scos@36707
MOI="ServicesNode.1025" Name="ws-kim.int.spidercloud.com"
SCOSVersion="1.6.0.DevBld.6272" BuildTime="Wed May 25 15:19:20 2011 PDT"]

<30>1 2011-08-24T18:50:57.456399Z ws-lava -- EVENT_ADMIN_AAA_LOGIN [scw@36707
MOI="ServicesNode.1025" Username="admin" MgmtSessID="0" Description="logged in over ssh
from 10.1.11.52" ]

```

**Table 36** shows the mapping between system severity levels and syslog levels. The severity value for syslog messages equals 24 plus the syslog severity code.

**Table 36: Syslog Severity**

System Severity	Syslog Severity	Syslog Severity Code	Severity Value
Critical	Critical	2	26
Major	Error	3	27
Minor	Error	3	27
Warning	Warning	4	28
Info	Informational	6	30
Trace	Debug	7	31

## 17.6.1 Defining Syslog Filters

You can filter events by three criteria: severity, group, or event identifier. You can define up to 24 separate filters using one or more of the criteria. Up to five filters can be assigned to a syslog target. By default, newly defined syslog targets filter for severities of *Info* or higher. *Trace* syslog events can be enabled for debugging purposes.

Each filter can contain up to the following number of each criterion:

- one severity ([Table 27](#) on page 233)
- three groups ([Table 28](#) on page 233)
- ten event identifiers (the *Cisco 8000 Series OS Faults, Conditions, and Events Reference Guide*)

Individual filters internally use the logical AND operation. This means that if multiple rules are defined, events must match all rules within the filter to be forwarded to the syslog destination.

Matching between different filters uses the logical OR operation. When multiple filters are used, events that match any ONE of the filters are forwarded to the syslog destination. Therefore it is often more sensible to define several less specific filters than one very specific filter.

### To define a syslog filter

**Step 1** From the Configuration Mode, issue the **set System EventManagement Filter** command to create the first filter. You must specify at least one filtering criterion. This example uses filter 1 with a severity of *Critical*.

```
set System EventManagement Filter 1 Severity Critical
```

**Step 2** (Optional) Create additional filters as needed. The first example below creates Filter 2 that filters all events that belong to group type *Session*. The second example creates Filter 3 that filters on events with the ID *ACTIVE\_EMERGENCY\_CALL*.

```
set System EventManagement Filter 2 Group [ Session ]
```

```
set System EventManagement Filter 3 EventID [ ACTIVE_EMERGENCY_CALL ]
```

**Step 3** Issue the **show System EventManagement Filter** command to verify the configuration:

```
show System EventManagement Filter
Filter 1 {
    Severity Critical;
}
Filter 2 {
    Group      "[ Session ]";
```

```

}
Filter 3 {
    EventID  "[ ACTIVE_EMERGENCY_CALL ]";
}

```

Alternatively, specify all three filtering criteria above in a single filter:

```
set System EventManagement Filter 1 Severity Critical Group [ Session ] EventID [ ACTIVE_EMERGENCY_CALL ]
```

**Step 4** Issue the **show System EventManagement Filter** command to verify the configuration:

```

show System EventManagement Filter
Filter 1 {
    Severity Critical;
    Group      "[ Session ]";
    EventID   "[ ACTIVE_EMERGENCY_CALL ]";
}

```

## 17.6.2 Configuring Syslog Targets

The system supports up to four simultaneously enabled syslog targets. When creating the target, you must specify at least one attribute (IP address, port, or filter). You must specify the IP address when setting the *Enable* attribute of this target to *true*.

To configure a syslog target

**Step 1** From the Configuration Mode, issue the **set System EventManagement Target Syslog** command to configure the first syslog target. This example defines a target at IP address 10.20.30.0 on port 514 and applies defined filters 1 and 2.

```
set System EventManagement Target 1 Syslog Enable true IPAddress 10.20.30.0 Port 514
Filter [ 1 2 ]
```

**Step 2** Repeat Step 1 as needed to define additional syslog targets. This example defines a target at IP address 10.20.30.1 on port 514.

```
set System EventManagement Target 2 Syslog Enable true IPAddress 10.20.30.1 Port 514
```

**Step 3** Issue the **show System EventManagement Target** command to verify the configuration:

```

show System EventManagement Target
Target 1 {
    Syslog {
        Enable      true;
        IPAddress 10.20.30.0;
        Port       514;
        Filter     "[ 1 2 ]";
    }
Target 2 {
    Syslog {
        Enable      true;
        IPAddress 10.20.30.1;
        Port       514;
    }
}
```

To configure a syslog target when using a forwarding group

**Step 1** From the Configuration Mode, issue the **set System EventManagement Target Syslog** command to configure the syslog target 4. This example defines a target at IP address 10.20.30.4 with forwarding group 4 using port 514 and applies defined filters 1 and 2.

```
set System EventManagement Target 4 Syslog Enable true ForwardingGroupIndex 4 IPAddress
10.20.30.4 Port 514 Filter [ 1 2 ]
```

**Step 2** Issue the **show System EventManagement Target** command to verify the configuration:

```
show System EventManagement Target
Target 4 {
    Syslog {
        Enable           true;
        IPAddress       10.20.30.4;
        ForwardingGroupIndex 4;
        Port            514;
        Filter          "[ 1 2 ]";
    }
}
```

### 17.6.3 Viewing Configured Syslog Targets

You can view the configured syslog targets in tabular format with the **show System Syslog** command.

To view configured syslog targets

**Step 1** From the Operational Mode, issue the **show System Syslog** command to display a tabular view of all configured syslog targets:

show System Syslog					
Target	Enable	IPAddress	TxMsgs	DiscardMsgs	Filter
1	true	10.20.30.0	100	44	[ 1 2 ]
2	true	10.20.30.1	144	0	[ ]

### 17.6.4 Resetting Syslog Counters

Administrators can reset all syslog counters. This is a system-wide command affecting all syslog counters of all the configured syslog targets.

To reset syslog counters

**Step 1** From the Operational Mode, issue the **request Statistics syslog reset** command to reset the transmit and discard syslog counters:

```
request Statistics syslog reset
```

## 17.7 Performance Management

Performance management enables system administrators and network operators to monitor the health of the network, detect and locate problems in radio components, and determine long-term performance trends. The small cell solution supports the collection of a wide-range of performance counters needed to remotely monitor and manage the performance of the system.

These counters span various subsystems and interfaces (such as IP networking, platform, and radio) and include also standard UMTS measurements as defined in the *3GPP TS 32.405* show standard. The performance measurements are aggregated at the controller according to the *3GPP TS 32.401 Performance Management Concepts and Requirements* specification, and are stored into database records that are accessible even after a system reboot.

Performance measurements can be retrieved either through CLI commands or uploaded to a remote server for mediation. Administrators can configure the interval that 3GPP-compliant Performance Monitoring (PM) statistics are collected and the number of those intervals collected into a report that can be uploaded through the FTP or SCP protocol to an external device for analysis and storage.

UMTS measurements are reported in XML in accordance with the *3GPP TS 32.435 XML File Format Definition*. The performance management framework provides all of the hooks and counters required for standard Key Performance Indicator (KPI) computation as defined in *3GPP TS 32.410*. In the current software release, KPIs are calculated off-box. Statistics can also be reformatted to the appropriate SNMP MIB for real-time monitoring.

Administrators can view system and cell statistics for any period within the past 60 minutes. The system stores the following statistics:

- **Real time:** statistics at the time of query
- **Active session:** statistics at the time of last update
- **Historical session statistics:** statistics at the time the session was deleted

Administrators can reset system, cell, or UE, snapshot counter statistics, or all statistics. After resetting the session statistics, a new snapshot is automatically created, and the snapshot number is incremented so that new data is stored in a new snapshot.

Additionally, administrators display real-time controller CPU and memory resource usage data.

### 17.7.1 Configuring Data Collection

PM data collection frequency and level of detail are configurable through the CLI. This section discusses the recommended settings for small cell solutions with a large number of users.

For systems with a large number of users and mobility events, administrators may elect to disable disk storage of session snapshots to reduce the system input/output churn and increase performance through the statistics parameters that enable or disable the storage of the following snapshot statistics:

- StoreSessionStatistics
- StoreEDMStatistics
- StoreSystemStatistics
- StoreCellStatistics
- StoreUEStatistics
- StoreSessionSnapshotStatistics

When setting the *Enable* parameter:

- If **true**, all snapshot statistics for each session are collected and stored in the logging database for retrieval. The **show Session UMTS SessionID <SessionId> Verbose** command returns detailed airlink statistics for the session.
- If **false**, no snapshot statistics are written into the logging database for any session. A limited number of snapshot statistics for the session are still collected in RAM.

To configure PM data collection parameters

**Step 1** From the Configuration Mode, issue the **set FAPService <ServiceNumber> PerfMgmt Collection Frequency** command to enable performance monitoring and configure how frequently the statistics are collected (in seconds). This example uses session snapshots with the default 60 seconds. It also disables statistical snapshots.

```
set FAPService 1 PerfMgmt Collection CollectRLCStatistics true Enable true Frequency 60
StoreSessionSnapshotStatistics false
```

**Step 2** Issue the **show FAPService <ServiceNumber> PerfMgmt** command to verify the configuration:

```
show FAPService 1 PerfMgmt
```

```

Collection {
    Enable           true;
    Frequency       60;
    CollectRLCStatistics true;
    StoreSessionSnapshotStatistics false;
}

```

**Step 3** Issue the following command to see detailed airlink statistics for a given IMSI session collected with the **StoreSessionSnapshotStatistics** parameter set to *true*. This example uses IMSI session 217151.

#### **show Session UMTS SessionID 217151 Verbose**

```

Session: 217151 (Historical)
RATType: UMTS, IMSI: 001010123451019
DataSessionNumberOfEntries: 1, VoiceSessionNumberOfEntries: 1
ConnectTime: 2011-10-13T03:32:50.975504Z, ConnectCause: HSDPA,
DisconnectTime: 2011-10-13T03:35:30.618951Z,
DisconnectCause: All radiolinks failed
RRState: Cell_DCH, UMTSSessionID: 1084227597, CurrentSnapshotID: 2,
ServingCellHandle: 405, AdmissionControlPriority: 65533
CSDomainActive: true, CSSessionType: Voice_FR
PSDomainActive: true, PSSessionType: HSDPA_64U
DataSession: 217151
    FlowID: 7, APNName: wap.scwl1, SwitchingMode: PassThrough
    UEIPAddress: 10.1.10.247
    PrimaryDNSIPAddress: 0.0.0.0, SecondaryDNSIPAddress: 0.0.0.0,
    ProviderPrimaryDNSIPAddress: 10.1.11.200,
    ProviderSecondaryDNSIPAddress: 10.1.11.200
VoiceSession: 217153
    FlowID: 8
Handover Statistics:
    NumServingCellChanges: 0, NumAsetAdds: 0, NumAsetDeletes: 0,
    NumAsetSwaps: 0
RadioLinks:
    RadioLink: 1
        CellHandle: 405, PSC: 405, RLID: 0, IsActive: false,
        IsServingCell: 1
Snapshots:
    Snapshot CreationCause      StartTime                      EndTime          TerminationCause
    ----- -----
    1  New Session   2011-10-13T03:32:50.991222Z  -               MultiRAB Add
    2  MultiRAB Add 2011-10-13T03:33:45.617883Z  -               Session Deletion

```

## 17.7.2 Viewing PM Statistics

You can view a wide range of PM statistics using Operational Mode **show** commands. The following four examples are frequently used PM statistical **show** commands. This is not an exhaustive list.

### To show PM statistics

**Step 1** From the Operational Mode, issue the **show System UMTS** command to display the current system level statistics:

```

show System UMTS
Current Status:
    TimeOfLastStatsReset: 2012-06-12T02:49:21.789561Z
    TimeOfLastStatsUpdate: 2012-06-13T20:58:01.969398Z
    NumCellsProvisioned: 5
    NumCellsActive: 1
    IuCSStatus: Connected
    IuPSSStatus: Connected
    EmergencyCallActive: false

```

**Step 2** Issue the **show Cell UMTS** command to display statistics for all cells in the system:

```

show Cell UMTS
CellHandle Name          RN     CID     UCID      PSC  MaxTxPwr  ModeInUse   RLs
----- -----
    1  -            1      1        1    400  11.0dBm  UMTSNetmon   0
    2  -            2      2        2    400  11.0dBm  UMTSNetmon   0

```

**Step 3** Issue the **show Session UMTS** command to display available of statistics for the currently active sessions in the system:

**show Session UMTS**

Session	IMSI	D	V	ConnectTime	RRCState	ConnectCause	Cell	CSSessionType	PSSessionType
2453027	001010123451129	1	0	06-12 02:57:16.13	Cell_DCH	HSUPA	6	UNKNOWN	HSPA
2453024	001010123451131	1	0	06-12 02:56:45.42	Cell_DCH	HSUPA	6	UNKNOWN	HSPA
2453023	001010123451130	1	0	06-12 02:56:43.33	Cell_DCH	HSUPA	6	UNKNOWN	HSPA
2453021	001010123451132	1	0	06-12 02:56:10.15	Cell_DCH	HSUPA	6	UNKNOWN	HSPA

**Step 4** Issue the **show Session UMTS history** command to display a table of statistics for the previously active sessions in the system:

**show Session UMTS History**

Session	IMSI	D	V	ConnectTime	RRCState	ConnectCause	Cell	DisconnectTime	DisconnectCause
2462402	001010123451064	0	0	06-13 20:59:28.05	Cell_DCH	Registration	3	06-13 20:59:29.33	Normal Release
2462401	001010123451134	0	0	06-13 20:58:31.42	Cell_DCH	Registration	4	06-13 20:58:32.71	Normal Release
2462400	001010123451136	0	0	06-13 20:57:49.51	Cell_DCH	Registration	4	06-13 20:57:51.15	Normal Release
2462399	001010123451204	0	0	06-13 20:56:25.41	Cell_DCH	Registration	4	06-13 20:56:27.01	Normal Release
2462398	001010123451288	0	0	06-13 20:55:56.61	Cell_DCH	Registration	4	06-13 20:55:58.21	Normal Release

## 17.7.3 Configuring Performance Management Reports

You can configure the system to copy each PM report to up to three remote devices for storage and analysis. Each generated report is given a unique name that includes a timestamp. The system retains 100 Mb of PM data. When the capacity is exceeded, older data is replaced with the latest measurements.

If the remote server is unavailable, the controller will keep trying to upload a file, regardless of the error (such as: unreachable, authentication failure, lack of disk space on the remote server). The system administrator can configure the re-trial behavior, and can specify retry parameters either in terms of the number of attempts, or time (duration).



You can set the number of upload attempts with the *MaxAttemptDuration* parameter for the number of seconds, or the *MaxAttempts* parameter for the number of tries, but not both.

### Note

If the path to the remote directory is not specified, the file transferred to the user's home directory.

To configure the remote storage device and data transfer parameters

**Step 1** From the Configuration Mode, issue the **set System FileManagement <number> ModuleID PerfMgmt UploadTarget** command to configure the remote file transfer. In this example:

- the remote device has the index number 1
- it has the IP address 10.20.10.1
- the user name and password are *admin*
- uses forwarding group 2
- it stores the file in the /a/pmlogfiles directory
- the file transfer uses the SCP protocol
- it will attempt to upload the file three times

```
set System FileManagement 1 Enable true ModuleID PerfMgmt MaxAttempts 3 UploadTarget 1
Host 10.20.10.1 Enable true Username admin Password admin Protocol SCP RemotePath /a/
pmlogfiles
```

**Step 2** Issue the following command to configure the second file transfer target. Note that no remote path is defined. The files will be placed in the user *admin*'s home directory.

```
set system FileManagement 2 Enable true ModuleID PerfMgmt MaxAttempts 3 UploadTarget 2
Host 10.20.10.2 Enable true Username admin Password adminProtocol SCP
```

**Step 3** Issue the **show System FileManagement** command to verify the configuration:

```
show System FileManagement
FileManagement 1 {
    Enable          true;
    ModuleID       PerfMgmt;
    MaxAttempts    3;
    UploadTarget 1 {
        Enable          true;
        Protocol        SCP;
        Username        admin;
        Password        admin;
        Host            10.20.10.1;
        RemotePath      /a/pmlogfiles;
    }
}
FileManagement 2 {
    Enable          true;
    ModuleID       PerfMgmt;
    MaxAttempts    3;
    UploadTarget 2 {
        Enable          true;
        Protocol        SCP;
        Username        admin;
        Password        admin;
        Host            10.20.10.2;
        ForwardingGroupIndex 0;
        RemotePath      "";
    }
}
```

**Step 4** Define the local distinguished name of the controller. This example names it *controller-5*.

```
set FAPService 1 LocalDN ManagedElement controller-5 MEContext Node_5
```

**Step 5** Issue the **show FAPService <ServiceNumber> LocalDN** command to verify the configuration:

```
show FAPService 1 LocalDN ManagedElement
MEContext      Node_5;
ManagedElement scsn-5;
```

**Step 6** Issue the **set FAPService <ServiceNumber> PerfMgmt ReportMgmt SampleSet** command to configure how frequently the report is generated and which statistics to gather. This example samples the *RAB.AttEstabCS* statistic and generates 24 reports, one every hour (3600 seconds) starting October 1, 2011 at 1 a.m. UT. Refer to the 3GPP TS 32.405 standard for definitions of collectible statistics.

```
set FAPService 1 PerfMgmt ReportMgmt Enable true SampleSet 1 Description Report01 Enable
true ReportSamples 24 SampleInterval 3600 TimeReference 2011-10-01T01:00:00Z Statistic 1
Enable true Reference RAB.AttEstabCS
```

**Step 7** Issue the **show FAPService <ServiceNumber> PerfMgmt** command to verify the configuration:

```
show FAPService 1 PerfMgmt
ReportMgmt {
    Enable true;
    SampleSet 1 {
        Enable          true;
        Description     Report01;
        SampleInterval  3600;
        ReportSamples   24;
        TimeReference   2011-10-01T01:00:00Z;
        Statistic 1 {
            Enable          true;
            Reference      RAB.AttEstabCS;
        }
    }
}
```

## 17.7.4 Resetting PM Counters

Reset all system and cell PM counters with the following Operational Mode commands.

To reset system PM counters

**Step 1** From the Operational Mode, issue the **request Statistics Reset** command to reset *cell*, *session*, *system syslog*, or *UE* statistics. In this example, cell 666 statistics.

```
request Statistics cell reset cellhandle 666
status OK
```

**Step 2** Issue the **request Statistics reset all** command to reset all system and cell statistics.

```
request Statistics reset all
status OK
```

**Step 3** Issue the **request Statistics ue reset imsi** command to reset statistics for an individual UE. This example uses UE with IMSI 001010123451351.

```
request Statistics ue reset imsi 001010123451351
```

**Step 4** Issue the **request Statistics session reset sessionid** command to reset statistics for an individual session. This example uses session ID 122047.

```
request Statistics session reset sessionid 122047
```

## 17.7.5 Deleting PM Statistics

Administrators can delete all stored system statistics. Active records will never be deleted.

To delete PM statistics

**Step 1** From the Operational Mode, issue the **request Statistics delete all** command to delete all stored statistics:

```
request Statistics delete all
status OK
```

## 17.7.6 Viewing Real-Time Resource Usage

Use the Operational Mode **show ServicesNode Resource** command to display current controller CPU and memory resource usage data. [Table 37](#) shows CPU and memory usage parameters and their definitions:

**Table 37: USC 8088 Controller Resource Parameters**

Resource	Parameter	Description
<b>CPU</b>	User	Percentage of time CPU is in user-mode.
	Kernel	Percentage of time CPU is in kernel-mode.
	IOWait	Percentage of time CPU is waiting for IO.
	Swap	Percentage of time CPU is swapping.
	Idle	Percentage of time CPU is idle.

**Table 37: USC 8088 Controller Resource Parameters (continued)**

Resource	Parameter	Description
	LoadAvg1	Average CPU load over the last 1 minute in number of processes x 100. CPU load is the number of processes waiting in the run-queue plus the number currently executing.
	LoadAvg5	Average CPU load over the last 5 minutes in number of processes x 100. CPU load is the number of processes waiting in the run-queue plus the number currently executing.
	LoadAvg15	Average CPU load over the last 15 minutes in number of processes x 100. CPU load is the number of processes waiting in the run-queue plus the number currently executing.
<b>Memory</b>	Free	Percent of memory available for use.
	Used	Percent of memory in-use.
	Cache	Percent of memory free, but not re-claimed.
	Total	Total amount of memory, in bytes.

To view real-time resource usage

**Step 1** From the Operational mode, issue the **show ServicesNode Resource** command to view real-time controller resource usage:

```
show ServicesNode Resource
ServicesNode 1025:
CPU:
  User:          37.63%
  Kernel:        22.68%
  IOWait:        0.00%
  Swap:          0.00%
  Idle:          39.67%
  LoadAvg1:      1.63
  LoadAvg5:      1.31
  LoadAvg15:     1.26
Memory:
  Free:          87.48%
  Used:          12.52%
  Cache:          48.65%
  Total:         1689144K
```

## 17.7.7 Tracking Unique User Devices

In order to track system usage, you can show the number of unique user devices that access the system over a period of time ranging from ten minutes to one day. The system counts all unique devices, defined by IMSI, for each circuit-switched, packet-switched, or multi-RAB session request.

When the *UniqueIMSI* parameter value is modified, the change must be committed before querying for another interval.

To track unique user devices

**Step 1** From the Configuration Mode, issue the **set FAPService 1 PerfMgmt Collection** command to set the enable collection of user device visits and configure the interval. This example sets the interval to 1 day (1440 minutes).

```
set FAPService 1 PerfMgmt Collection Enable true UniqueIMSI 1440
```

**Step 2** Issue the following command to verify the configuration:

```
show FAPService 1 PerfMgmt Collection
Enable                      true;
UniqueIMSI Timer             1440;
```

To view unique user devices

**Step 1** From the Operational Mode, issue the following command to view unique user devices for a configured period. This example uses the default time of 1 day (1440 minutes).

```
show status OpState FAPService 1 UMTS CurrentStatus NumUniqueIMSI
NumUniqueIMSI 14;
```

## 17.7.8 Tracking User Visit Duration

Visit duration is measured between the time of first connection establishment to the time of the last connection teardown. The visit is considered ended after a configurable inactivity threshold time. The number of user registrations without subsequent session requests indicate devices that likely pass through the periphery of the coverage area and are not the intended coverage targets.

Note that the *VisitThresholdTimer* must be larger than the periodic location update timer parameter (*CN CSDomain T3212*). The *T3212* parameter is measured in seconds with a default of one hour (3600 seconds).

To set user visit duration threshold

**Step 1** From the Configuration Mode, issue the **set FAPService 1 PerfMgmt Collection** command to set the user visit duration threshold. This example sets the visit duration threshold to 4 hours (240 minutes).

```
set FAPService 1 PerfMgmt Collection Enable true VisitThresholdTimer 240
```

**Step 2** Issue the following command to validate the configuration:

```
show FAPService 1 PerfMgmt Collection
Enable                      true;
VisitThresholdTimer          240;
```

To view user visit duration

**Step 1** From the Operational Mode, issue the following command to view the number of unique user visits

```
show status OpState cell 6 UMTS VisitDuration HoursHist
HoursHist "[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ]";
```

For the visits shorter than an hour, the visit duration is further broken down into fifteen minute intervals:

```
show status OpState cell 6 UMTS VisitDuration MinutesHist
MinutesHist "[ 0 0 0 0 ]";
```





# 18 System Maintenance

This chapter discusses managing files; backup and restore procedures; and downloading, upgrading, reverting the software image, and replacing a small cell. It contains the following sections:

- [Section 18.1, Managing Files](#) on page 269
- [Section 18.2, Backing Up and Restoring the Database](#) on page 278
- [Section 18.3, Downloading, Upgrading, and Reverting](#) on page 280
- [Section 18.4, Replacing a Small Cell](#) on page 282
- [Section 18.5, Rebooting the System](#) on page 283

Refer to [Section 2.12, Managing the Configuration](#) on page 25 for related information about managing the controller configuration.

## 18.1 Managing Files

The following sections have information about managing files in the controller:

- [Section 18.1.1, Using the file list Command](#) on page 269
- [Section 18.1.2, Using the file show Command](#) on page 270
- [Section 18.1.3, Using the file match Command](#) on page 271
- [Section 18.1.4, Using the file get Command](#) on page 272
- [Section 18.1.5, Using the file put Command](#) on page 272
- [Section 18.1.6, Using the file archive Command](#) on page 273
- [Section 18.1.7, Using the file delete Command](#) on page 273
- [Section 18.1.8, Using the file storage cleanup Command](#) on page 274
- [Section 18.1.9, Rotating Debug Log Files](#) on page 274
- [Section 18.1.10, Configuring a Remote Server for Log Files](#) on page 274
- [Section 18.1.11, UMTS Call Performance Event Report Files](#) on page 275
- [Section 18.1.12, LTE Call Performance Event Report Logs](#) on page 277

### 18.1.1 Using the *file list* Command

Core dumps and error bundles for both the controller and small cells are stored in the controller under the *error\_incidents* directory. Use the **file list <directory\_to\_list>** command from the Operational Mode to display the contents of that directory:

```
file list error_incidents/
```

The file name syntax includes the process name that crashed, the process ID that was running at the time of the crash, and the date and time when the core dump was generated:

```
<SN | RN>-<node id>.<process name>.<pid>.<date YYMMDD>.<time HH_MM_SS>.tgz
```

For example:

SN-1025.addressd.17863.091007.11\_24\_58.tgz

Component log files are stored under the *logfiles* directory. The system maintains a logging history of 10 files with a size limitation of a 50MB for each log file. Issue the **file list logfiles/** command in the Operational Mode to display the contents of a logfiles directory:

```
file list logfiles/
audit.log
confd.log
db_logfile-2014-10-01_222702.log
db_logfile-2014-10-01_225251.log
db_logfile-2014-10-01_230355.log
db_startup.log
debug.log
debug.log.ac-2015.141001.22_52_46
debug_session.log
debug_session.log.ac-2015.141001.22_52_46
devel.log
event.log
event.log.01
messages
wtmp
```

[output truncated]

Use the **file list detail** command to display detailed information about files in the root directory:

```
file list detail
drwx----- 2 4096 Aug 17 22:36 .ssh/
-rw-r--r-- 1 343 Aug 31 21:16 readme
drwxr-xr-x 2 4096 Aug 30 07:11 error_incidents/
-rw-r--r-- 1 2494 Sep 1 11:29 filecopy-2011-09-01_112940
-rw-r--r-- 1 2494 Sep 1 11:29 filecopy-2011-09-01_112942
-rw-r--r-- 1 2415 Sep 1 11:29 filecopy-2011-09-01_112944
```

Refer to [Section 2.9.1, Processing Command Output](#) on page 20 and [Section 2.9.2, Filtering Output with Regular Expressions](#) on page 21 for information about refining command output.

Use the **file list detail <directory\_to\_list/>** command to display detailed information about the files in another directory:

```
file list detail logfiles/
-rw-r--r-- 1 2797079 Aug 29 21:15 audit.log
-rw-r--r-- 1 90910 Aug 27 10:17 confd.log
-rw----- 1 244941 Aug 26 10:13 db_logfile-2011-08-26_070840.log
-rw----- 1 6507 Aug 26 14:53 db_logfile-2011-08-26_101410.log
-rw----- 1 6507 Aug 26 18:44 db_logfile-2011-08-26_145351.log
-rw----- 1 8843 Aug 26 18:48 db_logfile-2011-08-26_184441.log
-rw----- 1 465 Aug 26 19:35 db_logfile-2011-08-26_184840.log
[output truncated]
```

## 18.1.2 Using the *file show* Command

Issue the **file show <file\_to\_show>** command from the Operational Mode to display the contents of a file saved in the controller. Refer to [Section 2.9.1, Processing Command Output](#) on page 20 and [Section 2.9.2, Filtering Output with Regular Expressions](#) on page 21 for information about refining command output.

The following example first uses the **file list** command to display a list of available files, then uses the **file show** command to display the contents of the file *config4.cfg*:

```

file list
.ssh
ac-23-ap396-cstest
ac-23-baseline.cfg
ac-23-config
ac-23-config-new
config4.cfg
ipfactory.txt
logfiles
scw_Rel_1.5.101

file show config4.cfg
Time {
    NTPServer1      10.1.11.200;
    NTPServer2      1.1.1.2;
    LocalTimeZoneName PDT;
    Enable          true;
}
Layer3Forwarding {
    Forwarding 1 {
        Enable          true;
        DestIPAddress   0.0.0.0;
        DestSubnetMask  0.0.0.0;
        LANDevice       1;
        IPIInterface    1;
        ForwardingGroupIndex 0;
    }
    ForwardingGroup 1 {
        Name SCW-CLI-Test-String1;
    }
}
[output truncated]

```

### 18.1.3 Using the *file match* Command

Issue the **file match <string> <filename>** command (where <string> can include wildcards) from the Operational Mode to match a text string in the contents of a specified file. The output displays the contents of any full line that contains that string. The match string is case sensitive.

The following example displays all lines with the string *LAN* in the file *sn\_config.cfg*:

```

file match LAN sn_config.cfg
    LANDevice           1;
LANDevice 1 {
    LANHostConfigManagement {
        LANEthernetInterfaceConfig 1 {
LANDevice 2 {
    LANHostConfigManagement {
        LANEthernetInterfaceConfig 1 {
LANDevice 3 {
    LANHostConfigManagement {
        LANEthernetInterfaceConfig 1 {
            PrimaryLANDevice      1;
            PrimaryLANDevice      1;
            PrimaryLANDevice      3;
            PrimaryLANDevice      1;

```

The following example matches the string *1048576392* in the *debug.log* file in the *logfiles* directory to view the events related to session ID *1048576392*. This command is useful for diagnosing problems related to a given session.

```
file match 1048576392 logfiles/debug.log
```

```

1a 00000001 S 1025 uem      11/09/07 17:09:26.219399 umts_ue_construct: UE:1048576392
1a 00000001 m 1025 uem      11/09/07 17:09:26.219539 umts_ue_t::handle_rrc_msg: UE:1048576392
MsgId:CV ASN_RRC_CONN_REQ Category:4
1a 00000001 m 1025 uem      11/09/07 17:09:26.219562 umts_ue_t::handle_rrcconnreq: UE:1048576392
TMSI:1355 CELL:14 State:4
1a 00000001 M 1025 uem      11/09/07 17:09:26.219568 umts_ue_t::handle_rrcconnreq. UE:1048576392
Rel Ver:3 EstabCause:origSubscribedTrafficCall.
1a 00000001 m 1025 uem      11/09/07 17:09:26.219577 umts_ue_t::change_conn_state: UE:1048576392
Old State:IDLE New State:REQ_RCVD
1a 00000001 m 1025 uem      11/09/07 17:09:26.219586 umts_ue_t::set_ps_session_type UE:1048576392
Type:0->3
1a 00000001 m 1025 uem      11/09/07 17:09:26.219591 umts_ue_t::set_master_session_type
UE:1048576392 Type:0->5

```

The following example matches the string `1048576392` in all files in the `logfiles` directory to view the events related to session ID `1048576392`:

```
file match 1048576392 logfiles/*
```

Refer to [Section 2.9.1, Processing Command Output](#) on page 20 and [Section 2.9.2, Filtering Output with Regular Expressions](#) on page 21 for information about refining command output.

## 18.1.4 Using the `file get` Command

Issue the `file get <source-url> <local_path>` command from the Operational Mode to copy a file from a remote server to the controller. This is typically used to download a software package for an upgrade using Secure Copy Protocol (SCP), File Transfer Protocol (FTP), or Trivial File Transfer Protocol (TFTP).

If you do not specify a password for the remote server, a prompt for the password displays. The password you enter is not echoed to the terminal.

The following example uses SCP to copy the software image from the remote server at IP address `10.1.11.30`:

```
file get scp://user@10.1.11.30/volume/prebuild/packages/rel_2.0.5.12/scw_Rel_2.0.5.12
scw_Rel_2.0.5.12
user@10.1.11.30's password:
```

The following example uses SCP to copy the software image from the remote server at IP address `10.1.11.30` on port `49152`:

```
file get scp://user@10.1.11.30:49152/volume/prebuild/packages/rel_3.1.5.12/
scw_Rel_3.1.5.12 scw_Rel_3.1.5.12
user@10.1.11.30's password:
```

## 18.1.5 Using the `file put` Command

Issue the `file put <local_path> <destination-url>` command from the Operational Mode to copy a file to a remote server using SCP, FTP, or TFTP. If you do not specify a password for the remote server, a prompt for the password displays. The password you enter is not echoed to the terminal.

The following example uses SCP to copy the file `system.debug.log` to a server:

```
file put logfiles/debug.log scp://user@10.1.11.22/a/system.debug.log
user@10.1.11.22's password:
```

The following example uses SCP to copy the file `system.debug.log` to a server on port `49152`:

```
file put logfiles/debug.log scp://user@10.1.11.22:49152/a/system.debug.log
user@10.1.11.22's password:
```

The command prompts you to enter your password on the remote server.

## 18.1.6 Using the *file archive* Command

Issue the **file archive <archive\_name>** command from the Operational Mode to archive a file, list of files, or directory in the controller. You can use wildcards to include multiple files.

By default, the archived file is compressed. Use the *NoCompress* parameter to archive without compression. In either case the archived file must be given a filename with a *.tgz* or *.tar.gz* extension.

The following example first uses the **file list** command to display a list of available files, then uses the **file archive** command to archive the files *hs-insert.txt* and *hs-test.txt* into an archive named *newarchive.tar.gz*, and finally uses the **file list** command again to verify the file has been archived:

```
file list
bc_add_cell_test_config
error_incidents/
filecopy-2011-08-26_195437
filecopy-2011-08-26_195437.tgz
filecopy-2011-08-26_201737
hs-insert.txt
hs-test.txt

file archive newarchive.tar.gz hs*.txt

file list
bc_add_cell_test_config
error_incidents/
filecopy-2011-08-26_195437
filecopy-2011-08-26_195437.tgz
filecopy-2011-08-26_201737
hs-insert.txt
hs-test.txt
newarchive.tar.gz
```

## 18.1.7 Using the *file delete* Command

Issue the **file delete <file\_to\_delete>** command in the Operational Mode to delete the specified file in the controller.

The following example first uses the **file list** command to display a list of available files, then uses the **file delete** to delete the file *filecopy-2011-08-26\_184214*, and finally uses the **file list** command again to verify the file has been deleted:

```
file list
bc_add_cell_test_config
error_incidents/
filecopy-2011-08-26_184214
filecopy-2011-08-26_195437
filecopy-2011-08-26_201737
filecopy-2011-08-26_203909
filecopy-2011-08-26_205837
filecopy-2011-08-26_211307

file delete filecopy-2011-08-26_184214

file list
bc_add_cell_test_config
error_incidents/
filecopy-2011-08-26_195437
```

```
filecopy-2011-08-26_201737
filecopy-2011-08-26_203909
filecopy-2011-08-26_205837
filecopy-2011-08-26_211307
```

### 18.1.8 Using the *file storage cleanup* Command

Issue the **file storage cleanup** command from the Operational Mode to delete temporary files from the controller to increase storage space and improve system performance. A list of temporary files displays with a confirmation prompt. Enter **y** to delete the files. A file confirmation message displays.

```
file storage cleanup
=====
The following files will be deleted
=====

Size      Name
-----
798513   /scw/data/error_data/incidents/SN-1025.110824.10_57_38.tgz
545057   /scw/data/error_data/incidents/SN-1025.110824.11_02_09.tgz
1109963   /scw/data/error_data/incidents/SN-1025.snmpd.1883.110823.21_58_14.tgz
244941   /scw/data/logfiles/db_logfile-2011-08-26_070840.log
  6507   /scw/data/logfiles/db_logfile-2011-08-26_101410.log
  6507   /scw/data/logfiles/db_logfile-2011-08-26_145351.log
  8843   /scw/data/logfiles/db_logfile-2011-08-26_184441.log
  465    /scw/data/logfiles/db_logfile-2011-08-26_184840.log
~~~  
~~~  

Total size = 30067645  

Delete these files? [y/N]  

y  

All files deleted
```

### 18.1.9 Rotating Debug Log Files

The controller supports one current and up to ten previous debug log files. Each log file is identified by a timestamp. When the current log file reaches 50 megabytes, it is automatically closed (rotated) and a new log begins. If there are already ten old log files, the system deletes the oldest log file.

You can manually rotate a log file by entering the **request log rotate subsystem debug** command from the Operational Mode. Optionally, to add a comment to the new log file, first issue the **request log rotate marker** command:

```
request log rotate subsystem debug marker <textstring>
```

### 18.1.10 Configuring a Remote Server for Log Files

Configure the parameters of up to three remote servers to receive error bundle, debug, performance monitoring, and call reporting event management files for archival purposes. To avoid congestion in environments with multiple controllers you can schedule files to upload at random times.

If the path to the remote directory is not specified, the file transferred to the user's home directory. Refer to [Section 4.1.15.2, Configuring Virtual Routing and Forwarding](#) on page 53 for information about remote server configuration when using forwarding groups.



You can set the number of upload attempts with the *MaxAttemptDuration* parameter for the number of seconds, or the *MaxAttempts* parameter for the number of tries, but not both.

**Note**

## To configure a remote server for log files

**Step 1** From the Configuration Mode, issue the **set System FileManagement** command to configure and enable a remote server. In this example:

- it will attempt to send the file for 60 seconds
- it will randomly attempt to send the files after a delay of 4 minutes
- the remote device has the index number 1
- the upload server has the IP address 10.20.10.1
- the user name and password are *admin*
- uses forwarding group 2
- it stores the file in the /a/logfile directory
- the file transfer uses the SCP protocol
- it will attempt to upload the file for one minute (60 seconds).

```
set System FileManagement 1 Enable true ModuleID DebugLog MaxAttemptDuration 60
RandomUploadMaxDelay 4 UploadTarget 1 Host 10.20.10.1 Enable true Username admin Password
admin Protocol SCP RemotePath /a/logfiles
```

**Step 2** Issue the **show System FileManagement** command to display configuration information about the remote file server:

```
show System FileManagement 1
Enable           true;
ModuleID        DebugLog;
MaxAttemptDuration 60;
MaxAttempts     0;
RandomUploadMaxDelay 4;
UploadTarget 1 {
    Enable           true;
    Priority         Primary;
    Protocol         SCP;
    Username         admin;
    Password         admin;
    Host             10.20.10.1;
    ForwardingGroupIndex 2;
    RemotePath       /a/logfiles;
    RemotePermissions rw-r--r--;
    OverwriteMode   Overwrite;
}
```

### 18.1.11 UMTS Call Performance Event Report Files

The controller can create a file containing call report information with call details which provide per-UE information associated with signaling procedures on the small cell solution. It provides procedure information for operations and customer service teams to track user call performance.

These files can be uploaded to a designated host and can be imported to third-party applications for near real-time call performance monitoring. When properly configured, they can provide detailed per-UE information over user-defined granularity periods. Call performance report files are disabled by default, but can be enabled upon demand.

Each call constitutes multiple rows of the call performance report file. The controller retains call report files to a maximum of 1 GB.

The file details:

- the user IMSI
- radio technology
- signaling procedures and results, such as call origination, handovers, and reason for context release

- start/stop timestamps
- associated systems procedures, such as source/target, cells, and MMEs
- KPIs such as peak data rate associated with the procedure.

A call report file is created either at the end of the configured periodic interval or when the size exceeds a configurable size. By default the periodic interval is one minute but can be set to any one minute interval up to 30.

The filename identifies the controller that generated the file, the RAN technology (UMTS or LTE), a sequential serial number, and local timestamp in the following format:

cdr.log.umts.<sequenceNumber>.<eNodeBID>.<hostname>.<date>.<time>. For example:  
cdr.log.umts.1.5.ac-355.140904.18\_45\_15.

Refer to the *Cisco USC 8000 Series Call Performance Event Reporting Guide* for information about CRER events, event attributes and the format of CPER files.

### Configuring UMTS call performance event report logs

**Step 1** From the Configuration Mode, issue the following command to enable CPER file logging on the UMTS subsystem. This example sets the rollover interval to 1 minute and the file rollover size to 1 Mb.

```
set System CallPerformanceEventReport UMTS Enable true RollOverInte rval 1 RollOverSize 1
```

**Step 2** Issue the following command to verify the configuration:

```
show System CallPerformanceEventReport
UMTS {
    Enable      true;
    RollOverInterval 1;
    RollOverSize   1;
}
```

**Step 3** From the Configuration Mode, issue the **set System FileManagement** command to configure and enable a remote server. In this example:

- set the module ID to *UMTSCallPerformanceEventReport*
- it will attempt to send the file for 60 seconds
- it will randomly attempt to send the files after a delay of 4 minutes
- the remote device has the index number 1
- the upload server has the IP address 10.20.10.1
- the user name and password are *admin*
- uses forwarding group 2
- it stores the file in the /a/logfile directory
- the file transfer uses the SCP protocol

```
set System FileManagement 1 Enable true ModuleID UMTSCallPerformanceEventReport
MaxAttemptDuration 60 RandomUploadMaxDelay 4 UploadTarget 1 Host 10.20.10.1 Enable true
Username admin Password admin Protocol SCP RemotePath /a/logfiles
```

**Step 4** Issue the **show System FileManagement** command to display configuration information about the remote file server:

```
show System FileManagement 1
Enable      true;
ModuleID   UMTSCallPerformanceEventReport;
MaxAttemptDuration 60;
MaxAttempts 0;
RandomUploadMaxDelay 4;
UploadTarget 1 {
    Enable      true;
    Priority   Primary;
    Protocol   SCP;
    Username   admin;
    Password   admin;
```

```

Host           10.20.10.1;
ForwardingGroupIndex 2;
RemotePath     /a/logfiles;
RemotePermissions rw-r--r--;
OverwriteMode  Overwrite;
}

```

## 18.1.12 LTE Call Performance Event Report Logs

The controller can create a file containing call report information with call details which provide per-UE information associated with signaling procedures on the small cell solution. It provides procedure information for operations and customer service teams to track user call performance.

These files can be uploaded to a designated host and can be imported to third-party applications for near real-time call performance monitoring. When properly configured, they can provide detailed per-UE information over user-defined granularity periods. Call performance report files are disabled by default, but can be enabled upon demand.

Each call constitutes multiple rows of the call performance report file. The controller retains call report files to a maximum of 1 GB.

The file details:

- the user IMSI
- radio technology
- signaling procedures and results, such as call origination, handovers, and reason for context release
- start/stop timestamps
- associated systems procedures, such as source/target, cells, and MMEs
- KPIs such as peak data rate associated with the procedure.

A call report file is created either at the end of the configured periodic interval or when the size exceeds a configurable size. By default the periodic interval is one minute but can be set to any one minute interval up to 30.

The filename identifies the controller that generated the file, the RAN technology (UMTS or LTE), a sequential serial number, and local timestamp in the following format:

cdr.log.lts.<sequenceNumber>.<eNodeBID>.<hostname>.<date>.<time>. For example:  
cdr.log.lte.1.5.ac-355.140904.18\_45\_15.

Refer to the *Cisco USC 8000 Series Call Performance Event Reporting Guide* for information about CRER events, event attributes and the format of CPER files.

### Configuring LTE call performance event report logs

**Step 1** From the Configuration Mode, issue the following command to enable CPER file logging on the LTE subsystem. This example sets the rollover interval to 1 minute and the file rollover size to 1 Mb.

```
set System CallPerformanceEventReport LTE Enable true RollOverInte rval 1 RollOverSize 1
```

**Step 2** Issue the following command to verify the configuration:

```
show System CallPerformanceEventReport
LTE {
    Enable          true;
    RollOverInterval 1;
    RollOverSize    1;
```

}

**Step 3** From the Configuration Mode, issue the **set System FileManagement** command to configure and enable a remote server. In this example:

- set the module ID to *LTECallPerformanceEventReport*
- it will attempt to send the file for 60 seconds
- it will randomly attempt to send the files after a delay of 4 minutes
- the remote device has the index number 1
- the upload server has the IP address 10.20.10.2
- the user name and password are *admin*
- uses forwarding group 2
- it stores the file in the /a/logfile directory
- the file transfer uses the SCP protocol

```
set System FileManagement 1 Enable true ModuleID LTECallPerformanceEventReport
MaxAttemptDuration 60 RandomUploadMaxDelay 4 UploadTarget 1 Host 10.20.10.1 Enable true
Username admin Password admin Protocol SCP RemotePath /a/logfiles
```

**Step 4** Issue the **show System FileManagement** command to display configuration information about the remote file server:

```
show System FileManagement 1
Enable          true;
ModuleID        DebugLog;
MaxAttemptDuration 60;
MaxAttempts     0;
RandomUploadMaxDelay 4;
UploadTarget 1 {
    Enable          true;
    Priority        Primary;
    Protocol        SCP;
    Username        admin;
    Password        admin;
    Host            10.20.10.2;
    ForwardingGroupIndex 2;
    RemotePath      /a/logfiles;
    RemotePermissions rw-r--r--;
    OverwriteMode   Overwrite;
}
```

## 18.2 Backing Up and Restoring the Database

The controller maintains a database that contains the current system configuration of provisioned and learned elements. This file can be backed up to an external server on a one-time basis or scheduled for periodic backup. The backup does not restore certificates used for IPsec authentication.

The database backup includes data and configurations entered through the CLI (the running configuration) and information learned by the system as it runs. For example, the database backup includes information learned from a

REM scan, such as primary scrambling codes, cell power, and neighborhood topology). It can optionally contain logged events and historical alarms.

Refer to the following sections for the procedures to back up and restore the running configuration. Refer to the following sections for the procedures to back up and restore the running configuration:

- [Section 2.12.5, Saving the Running Configuration](#) on page 28
- [Section 2.12.6, Backing Up the Running Configuration](#) on page 29
- [Section 2.12.7, Loading and Merging a Configuration File](#) on page 29

## 18.2.1 Backing Up the Database

A database backup archives the current system configuration of provisioned and learned elements. The system does not support granular backups of selected elements. Database backups are exported to the controller administrator home directory. A failed backup does not produce a file.

Backup files have a maximum length of 127 characters including any file extension. Only the characters inside the following brackets are permitted: [a-z A-Z 0-9 \_ . -].

To back up the database

**Step 1** From the Operational Mode, issue the **request System Database Backup FileName <filename>** to backup the database to the administrator user home directory.

```
request System Database Backup FileName SCWDB_BACKUP
```

To back up the database and logged events and historical alarms

**Step 1** From the Operational Mode, issue the **request System Database Backup FileName <filename> IncludeLoggingDB** command to backup the database to the administrator user home directory.

```
request System Database Backup FileName SCWDB_BACKUP IncludeLoggingDB
```

## 18.2.2 Restoring the Database

Database restoration triggers a controller reboot. Do not modify the backed up database. The system performs a database validation before the system boots, and will not attempt restoration with an incompatible or modified backup.

The backup database is not merged with the current persistent database. It replaces it and all data in the current database is permanently deleted.

Once a database has been restored, it cannot be reverted to the previous configuration. In the event of a major error in the restoration process, the restore process is aborted and the system continues using the current database and the system generates a *DB\_BACKUP\_FAILED* error message.



**Note** When updating the system software and restoring a database, upgrade the controller software and reboot before restoring the database. Users connected through an SSH session will lose connectivity to the controller. Start a new session by connecting to the new IP address on port 22.

Once the database has successfully been restored, validate that all configured IP addresses are still valid and that authentication certificates are properly configured.

To restore the database

**Step 1** From the Operational Mode, issue the **request system Database Restore FileName <filename>** command to restore the database:

```
request system Database Restore FileName SCWDB_BACKUP
Valid restore file accepted. The SN will now reboot...
```

## 18.3 Downloading, Upgrading, and Reverting

The OS (OS) is a binary file residing in the controller containing the system software images for the controller and the small cells. A small cell retrieves its software image from its master controller. When the controller reboots, all associated client small cells also reboot.

Use the following two commands to copy and install a new image:

- **file get**
- **request system update package**

The controller supports any protocol to copy files from the server and to the small cell. On the remote server, an SSH daemon must be running or the copy operation will fail.

You must use an IP address in the SCP URL string. The system does not support DNS-resolved addresses.

The following Operational Mode commands are used to display, upgrade, and revert the software image:

```
show Version
show Version Revert
show Version Detail
file get scp://user@ipaddress/full/path/to/filename filename
request system update package <filename>
request system revert
```

### 18.3.1 Displaying the Software Image Version

Use the **show Version**, **show Version Revert**, and **show Version Detail** commands in the Operational Mode to display information about the software image running in the controller and the revert image.

The **show Version** command provides brief information about the running image:

```
show Version
Product Image Version Timestamp
-----
SCOS    running  4.0.0   2014-02-21T10:48:51Z
```

The **show Version Revert** command displays the revert software image:

```
show Version Revert
PackageID Version          Builder      BuildTime
-----  -----
PLAT     4.0.0.           david       Fri Feb 21 08:22:12 2014 PST
UMTS     4.0.0.           ortiz       Fri Feb 21 08:50:11 2014 PST
```

The **show Version Detail** command displays the current UMTS and Platform (PLAT) images installed. If there are any small cells connected to the system, this command displays the software version running on the small cells (provisioned and unprovisioned).

#### **show version detail**

NodeID	PackageID	Version	Builder	BuildTime
1025	LTE	4.0.0.188.797	builder	Fri Feb 21 02:45:42 2014 PST
1025	LTE	4.0.0.188.797	builder	Fri Feb 21 02:45:42 2014 PST
1025	UMTS	4.0.0.188.5026	builder	Fri Feb 21 02:41:54 2014 PST
1025	PLAT	4.0.0.188.10827	builder	Fri Feb 21 02:07:32 2014 PST
1025	BOOTB	2.3.2	builder	Wed Apr 3 18:20:10 2013 PDT
1025	BOOTA*	2.3.2	builder	Wed Apr 3 18:20:10 2013 PDT

### 18.3.2 Copying the Software Image and Update

To upgrade the software image, locate the file and its path on a remote server. Include that path in the **file get** command to copy the software package from the remote server to the controller. Then, issue the **request system update package** command to update the image in the controller.

The following safeguards apply when performing software upgrades:

- You cannot upgrade a software version with an older software version.
- To fallback to a previously release, use the **revert** command.
- You cannot upgrade to the same software version that is currently running on a controller.

#### To copy the software image and update the controller

You will need the path and the image name to copy the software image from the remote server to the controller. The image name used in this example is *scw\_Rel\_2.0.0.55*.

**Step 1** Log onto a remote server and issue a command to list the contents of the image directory:

```
[user@osun ~]$ ls /volume/prebuild/packages/rel_2.1.0.55/
scw_Rel_2.1.0.55
```

**Step 2** From the Operational Mode, issue the **file get** command to copy the new software image from the remote server to the controller. This example uses SCP to copy the image from the remote server.

```
file get scp://user@ipaddress/volume/prebuild/packages/rel_2.1.0.55/scw_Rel_2.1.0.55
scw_Rel_2.1.0.55
```

**user@10.1.11.30's password:**

**Step 3** Enter your password.

**Step 4** Issue the **request system update package** command using the name of your image to update the local system package:

```
request system update package scw_Rel_2.1.0.55
status Update successful, now rebooting...
```

Connection to ac-23 closed by remote host.  
Connection to ac-23 closed.

The controller will automatically reboot to load the new software version. The command prompt is inaccessible during this process.

### 18.3.3 Reverting to the Previous Image

You can revert the system to the previously installed image using the **request system revert** command. When the controller performs an update, it records a snapshot of the database and saves it. When a revert is issued, the system is brought back to the exact point before the update. All configuration changes made after the update will be lost.

The controller supports storing two images at one time: the active and immediately previous. Therefore the controller retains only one previous image for rollback.



When the revert command executes, all CLI user sessions terminate and the controller reboots. You can log back in after the boot sequence completes.

#### Note

To revert to the previous software image

**Step 1** From the Operational Mode, issue the **request system revert** command to revert to the previous software image:

```
request system revert
status Update successful, now rebooting...
```

Connection to ac-23 closed by remote host.  
Connection to ac-23 closed.

The controller will automatically reboot to load the new software version. The command prompt is inaccessible during this process.

If no previous image is available to fall back to, the following error message displays:

```
error: System revert failed! Reason: Unable to revert, previous image not found, status:3
[error] [2011-05-20 23:28:27]
```

## 18.4 Replacing a Small Cell

Follow these high-level steps to replace a failed small cell in an active system:

- Disable auto provisioning
- Disable the failed small cell
- Physically replace the small cell
- Update the controller database
- Enable the new small cell
- Verify that the small cell is functioning properly
- (Optional) Re-enable auto provisioning

To replace a small cell

**Step 1** From the Configuration Mode, issue the following command to disable auto provisioning:

```
set FAPService 1 FAPControl UMTS SelfConfig AutoProvisionEnable false
```

**Step 2** Issue the following command to place the small cell out of service. This example uses small cell 55.

```
set RadioNode 55 Enable false
```

**Step 3** Commit the configuration:

```
commit
```

**Step 4** Physically replace the old small cell with the new small cell and wait for it to fully reboot.

**Step 5** From the Operational Mode, issue the `request radionode replace` command to update the small cell record in the controller database.

```
request radionode replace node_id 55 with_node_id 2049
```

**Step 6** The small cell reboots again. After the small cell has rebooted, issue the following command from the Configuration Mode to place the new small cell in service.

```
set RadioNode 55 Enable true
```

**Step 7** Issue the following command from to verify the small cell is in service and functioning properly:

run	show	RadioNode	Radio	RN	Name	Enable	EthernetID	IPAddress	OuterIPAddress	OperState
				55	ap55	true	00:24:48:01:2d:74	10.1.213.244	10.1.213.244	IS-NORMAL

**Step 8** (Optional) From the Configuration Mode, issue the following command to re-enable auto provisioning:

```
set FAPService 1 FAPControl UMTS SelfConfig AutoProvisionEnable true
```

## 18.5 Rebooting the System

You can reboot the controller either with no affects to the configuration data, database, or the cell manager configuration, or in a clean mode that resets one of these configurations to the factory default.

### To reboot the system

**Step 1** From the Operational Mode, issue the following command to reboot the system:

```
request system reboot
```

### To reboot the system in a clean mode

**Step 1** From the Operational Mode, issue the following command to reboot the system in a clean mode:

```
request system reboot clean
```

Possible completions:

configuration	- Removes configuration and replaces it with factory configuration
data	- Removes all persistent data (configuration, logfiles, core files, etc)
db	- Removes the cellmgr.ini file
none	- Removes nothing

**Step 2** Enter a clean mode option and press *Enter*.



# 19 Troubleshooting

This chapter contains the following troubleshooting procedures and small cell LED behavioral definitions:

- [Section 19.1, USC 8088 Controller Diagnostics](#) on page 285
- [Section 19.2, Creating a Bundle of Error Log Files](#) on page 288
- [Section 19.3, Small Cell LED Management](#) on page 289
- [Section 19.4, Small Cell LED Boot Sequence](#) on page 290
- [Section 19.5, Locating Small Cell](#) on page 291
- [Section 19.6, Follow an IMSI](#) on page 292
- [Section 19.7, Small Cell Link Test](#) on page 292
- [Section 19.8, Service Affecting Actions](#) on page 293

The small cell has one top-panel LED to indicate power and status. The LED displays in three colors in three different patterns for informational and troubleshooting purposes.

## 19.1 USC 8088 Controller Diagnostics

Network operators and administrators rely primarily on the eRMS management system and on the controller CLI to manage small cell solution systems and to perform standard procedures, including provisioning, monitoring, and troubleshooting. System administrators on eRMS and on the CLI have complete access to all the configurable parameters and tasks in the small cell solution system.

Occasionally, there may be a need for a support technician without *admin* level privileges to perform diagnostic procedures on a controller. For example, a controller that becomes temporarily unresponsive or unreachable through the regular CLI and eRMS interfaces.

To address such uncommon situations, the controller has a Recovery Command Interface (RCI) with a *field\_recovery* user. The *field\_recovery* user has limited access to a fixed set of debug and recovery commands. While ensuring the security of the controller, these commands provide tools for the *field-recovery* user to restore to service a unit experiencing system failure to avoid prolonged system outages. Once logged in, the recovery user has access to the RCI that provides system recovery related functions.

Access to the RCI and *field\_recovery* user is available through either:

- the console port (if the user has defined a password and the *EnableFieldRecoveryConsoleAccess* parameter is set to *true*)  
*or*
- SSH (if only the password is defined).

## 19.1.1 Field Recovery User Overview

The *field\_recovery* user account is disabled by default. To enable the *field\_recovery* user, first define the password, then enable the *field\_recovery* user account. Refer to [Section 19.1.2.1, Enabling the Field Recovery User](#) on page 286 for instructions.

The *field\_recovery* user account has a timer that logs off after five minutes of inactivity. The *admin* user can disable and re-enable console access for the *field\_recovery* and *admin* users.




---

The *field\_recovery* user account is deleted upon a factory reset and console access is removed when the CLI *clean data* or *clean config* options are selected.

---

**Caution**

The *field\_recovery* account persists across system reboot, software upgrade, and revert. The *field\_recovery* user does not display when a **show System AdminAAA User** command is issued from the Configuration Mode.

Upon *field\_recovery* login to the system, the user is presented the following options, selected by entering the number and pressing **Enter**:

SCW Recovery CLI:

- 1 Exit
  - 2 Reboot
  - 3 Revert
  - 4 Ping
  - 5 Generate Error Bundle
  - 6 System Status
- recovery:

After selecting one of the above numbers, the *field\_recovery* user is presented a very limited set of commands and options. For example, selecting the *Revert* option presents a series of validations and displays the software version to revert to (if present). The *System Status* option displays high-level system status information.

## 19.1.2 Configuring the Field Recovery User

---

**Note:** User names and passwords are case-sensitive.

---

### 19.1.2.1 Enabling the Field Recovery User

This procedure assumes that you are logged in as an administrator to the CLI interface of a functioning system.

To enable the *field recovery* user

**Step 1** From the Operational Mode, issue the **set system password username** command to enable the *field recovery* user:

```
set system password username field_recovery
Enter new password to enable account: <NewPassword>
Re-enter new password: <NewPassword>
```

### 19.1.2.2 Disabling the Field Recovery User

Disable a *field recovery* user account by deleting its password. Delete the password by first entering the existing password, then pressing **Enter** when prompted for a new password. By pressing **Enter** you are creating an empty password.

## To disable the field recovery user

**Step 1** From the Operational Mode, issue the set system password username command to disable the field recovery user:

```
set system password username field_recovery
field_recovery account is enabled.
Enter current password: <Password>
Enter new password (empty password disables account): <Enter>
Disable field_recovery account? [yes,no]: yes
```

### 19.1.2.3 Changing the Field Recovery User Password

Change the *field\_recovery* user password with the following procedure:

#### To change a field recovery user password

**Step 1** From the Operational Mode, issue the set system password username command to change the password:

```
set system password username field_recovery
field_recovery account is enabled.
Enter current password: <Password>
Enter new password (empty password disables account): <NewPassword>
Re-enter new password: <NewPassword>
```

### 19.1.3 Configuring Console Access for the Field Recovery User

Connect your laptop to the controller console port with an RS-232 console cable. The console port has the following settings:

- Baud rate: 115,200 bps
- Data bits: 8
- Stop bits: 1
- Parity: none
- Flow control: none

Use the following commands from the configuration mode to configure field recovery console access to the controller:

#### To enable console access for the field recovery user:

```
set System EnableFieldRecoveryConsoleAccess TRUE
```

#### To disable console access for the field recovery user:

```
set System EnableFieldRecoveryConsoleAccess FALSE
```

### 19.1.4 Configuring Console Access for the Administrative User

#### To disable console access for the administrative user:

```
set System CLI EnableAdminConsoleAccess FALSE
```

#### To re-enable console access for the administrative user:

```
set System CLI EnableAdminConsoleAccess TRUE
```

## 19.1.5 Resetting the USC 8088 Controller to the Factory Default

In some instances it is necessary to reset a controller to its factory default settings. Resetting the controller to its factory default settings can improve the chances of returning a failed unit to operational state.

Resetting the controller to the default settings deletes the current system configuration, database, and all passwords. If you want to return the system configuration and database settings after the system reset, back up the database to an external location prior to resetting the system.

Resetting the system defaults does not affect the current OS software version. It retains the current software version regardless of the software version originally shipped with the controller.

### To reset a controllers to the factory defaults

Connect to the console port. This example uses a console port with the IP address 10.10.10.1. You are then presented with a login prompt.

```
telnet 10.10.10.1
login:
```

**Step 2** Enter the login name *factory\_reset*. The system will reset to factory default settings and reboot within ten seconds unless the command is aborted.

```
factory_reset
Resetting system to factory settings in 10 seconds.
All system data will be removed and the system will be rebooted.
Enter CNTRL-C to abort.
```

## 19.2 Creating a Bundle of Error Log Files

It is often convenient in troubleshooting to bundle a number of related error log files for off-controller processing and evaluation. The following procedure shows how to create a bundle of log files.

**Step 1** From the Configuration Mode, issue the **save <filename.cfg>** command to save the current running configuration. This example names the file 2012-07-20.cfg.

```
save config-2012-07-20.cfg
```

**Step 2** From the Operational Mode, issue the **file list** command to verify the file has been created:

```
file list
config-2012-07-20.cfg
error_incidents/
filecopy-2012-07-16_211235
filecopy-2012-07-17_185518
filecopy-2012-07-17_205307
```

**Step 3** Issue the **request set-debug <component> <level>** command to change the system level logging levels. The *level* parameter has the following attributes: Flow: captures everything; max and minor: bare minimum; off: turns logging off. This example changes the sc level to *minor*.

```
request set-debug sc level minor
```

**Step 4** Issue the **request umts debug <component> <level>** command to change logging level for UMTS.

```
request umts debug ranap level 3
```

**Step 5** Issue the **request log rotate subsystem debug marker <filename>** command to create a new log file. This example creates the file named *newlog.log*

```
request log rotate subsystem debug marker newlog.log
```

**Step 6** Perform the activity or test to collect the logs for.

**Step 7** Issue the **request log bundle** command to create a log file. This creates a tar file in the **error\_incidents** directory containing all the files located in the **logfiles** folder.

```
request log bundle
```

**Step 8** Issue the **file list error\_incidents/** command to list all log files in the directory.

```
file list error_incidents/
SN-1025.120709.10_44_35.tgz
SN-1025.120709.10_58_18.tgz
SN-1025.120709.11_04_46.tgz
SN-1025.120709.11_34_16.tgz
SN-1025.120709.11_37_57.tgz
```

## 19.3 Small Cell LED Management

The LED display is active by default, but can be deactivated in light-sensitive environments as needed. Even when the display is disabled, the LED will be lighted during the following conditions:

- while the small cell is booting
- if the small cell or cell is in fault state
- if there is an active emergency call
- if the locate small cell feature is active
- if the follow IMSI feature is active

Table 38 shows the default LED behavior of the small cell:

**Table 38: Small Cell LED Behavior**

LED	Status	Flash Rate
Green: slow flashing	Administratively disabled	Approximately ½ second on, 1½ sec. off
Green: fast flashing	Booting	Approximately 1.4 second on/off cycle
Green: solid	Operational	
Red: solid	Fault	
Red: fast flashing	One or more emergency calls active	Approximately 1 second on/off cycle
Blue: fast flashing	Locate small cell enabled	Approximately 1 second on/off cycle
Blue: solid	Follow IMSI enabled	
Off	Powered off or LED disabled	

To disable the LED display

**Step 1** From the Configuration Mode, issue the **set System RadioNode LED DefaultMode Dark** command to disable the LED display:

```
set System RadioNode LED DefaultMode Dark
```

**Step 2** Issue the **show System RadioNode LED** command to verify the configuration:

```
show System RadioNode LED
DefaultMode Dark;
```

To re-enable the LED display

**Step 1** From the Configuration Mode, issue the `set System RadioNode LED DefaultMode Standard` command to re-enable the LED display:

```
set System RadioNode LED DefaultMode Standard
```

**Step 2** Issue the `show System RadioNode LED` command to verify the configuration:

```
show System RadioNode LED
DefaultMode Standard;
```

## 19.4 Small Cell LED Boot Sequence

The small cell state machine is sequential and progresses in the following order:

State 0 -> State 1 -> State 2 -> State 3 -> State 4 -> State 5

A normal boot sequence transitions through all these states sequentially and the LED state transitions accordingly. If the small cell fails to transition to the next state, the system restarts the boot sequence, starting with State 0. You can determine the progress during the booting stages by observing the LED color transitions. On failure, the last LED state will display the state that encountered the failure. [Table 39](#) shows the small cell boot sequence and corresponding LED behavior:

**Table 39: Small Cell LED Boot Sequence**

State	LED Color	Description	Possible Failures and Actions
0. Power On/ Reset	Flashing green	This is the initial state on startup.  The small cell bootup is controlled by firmware in this state.  It will go through a lamp test in this state. A lamp test involves cycling through all LED colors.	This state should be very short lived and should transition to the next state immediately.  A small cell should not stay in this state indefinitely.  Note: Flashing Green is also used to indicate a small cell that has been administratively disabled. This can be determined from the CLI.
1. DHCP	Solid red	The small cell starts by sending out a DHCP Request.  The small cell moves to the next state (State 2) upon receiving a DHCP response and an IP Address.	No DHCP Response, IP Address not allocated.  Check cabling, DHCP Server configuration.
2. Join	Solid blue	The small cell has an IP Address and sends a UDP Join request to the Serving controller.  The small cell moves to the next state (State 3) upon getting a JOIN GRANT from the controller.	No IP reachability to the controller.  Check IP network between small cell and controller for routing issues.

**Table 39: Small Cell LED Boot Sequence (continued)**

State	LED Color	Description	Possible Failures and Actions
3. TFTP	Flashing blue	The small cell proceeds next to download the operating system image from the controller.  The small cell moves to the next state (State 4) after the image has been downloaded.	Failure to download TFTP image.  Check firewall between small cell and controller.
4. Operating System Booting	Flashing green	The small cell loads the operating system and starts the default platform applications.  The small cell moves to the next state (State 5) when it establishes connectivity with the service node.	Failure to start the operating system.  This normally points to a software/build issue. Please contact Cisco support.
5. Running	Solid green	The operating system is running. The small cell continues the startup sequence, but is now controlled by the controller.	The operating system is up and running on the small cell.  Any subsequent state transitions can now be tracked from events and logs on the controller.

## 19.5 Locating Small Cell

For troubleshooting purposes, you can identify the location of a specified small cell by issuing the **request radionode led locate node\_id** command from the Operational Mode to trigger a fast blue LED flashing pattern. This command will be executed even when the small cell is administratively Out Of Service (OOS) or LEDs are globally disabled.

The command remains active until the system is manually returned to the default mode or the controller reboots. The **request radionode led locate node\_id** command overrides an active **request radionode led follow imsi** setting, but is overridden by the emergency call indication.

### To locate a small cell

**Step 1** From the Operational Mode, issue the **request radionode led locate node\_id <Number>** command to activate the small cell LED with a fast flashing blue pattern. This example activates the LED of small cell 714.

```
request radionode led locate node_id 714
```

### To disable the locate small cell function

**Step 1** From the Operational Mode, issue the **request radionode led normal** command to disable the locate small cell functionality and return all small cells to the default mode defined in [Section 19.5, Locating Small Cell](#) on page 291.

```
request radionode led normal
```

## 19.6 Follow an IMSI

For troubleshooting purposes, you can follow a given user device as it traverses the coverage area to identify the serving small cell by issuing the **request radionode led follow imsi** command from the Operational Mode. This command lights the serving small cell LED solid blue. This command will be executed even when the small cell is administratively OOS or LEDs are globally disabled.

The command remains active until the system is manually returned to the default mode or the controller reboots. The **request radionode led follow imsi** command overrides an active **request radionode led locate node\_id** setting, but is overridden by the emergency call indication.

To follow a defined IMSI

**Step 1** From the Operational Mode, issue the **request radionode led follow imsi <imsi>** command to identify the serving small cell for a defined IMSI. The serving small cell will display a solid blue LED. This example uses IMSI 123456789101001.

```
request radionode led follow imsi 123456789101001
```

To disable the follow IMSI function

**Step 1** From the Operational Mode, issue the **request radionode led normal** command to disable the follow IMSI functionality and return all small cells to the default mode defined in [Section 19.5, Locating Small Cell](#) on page 291.

```
request radionode led normal
```

## 19.7 Small Cell Link Test

To verify system installation, test the IP connectivity of the controller link to all small cells in the cluster. The small cell link test utility performs this test and benchmarks the network performance of the system. The utility uses loopback capability and support for RFC2544-like methodology to measure controller-to-small cell link parameters and to troubleshoot one or more small cells.

The test measures throughput, latency, packet loss, and jitter for frame sizes of 64, 512, and 1280 bytes. If packets are dropped at a given speed, the test is repeated at a reduced rate. The rate is reduced again if there are further packet drops for a total of five test iterations before the results are reported.

The system stores the last results of 8 tests before the replacing the oldest test with newer ones. Test results do not persist across reboots.

By default the test measures all controller to small cell links in the system. The test can also target any combination of the following parameters:

- **description:** Test description
- **duration:** Duration in seconds for which test frames are sent
- **mode:** Test mode
- **rate:** Rate in Mbps at which test frames are sent
- **rn-id:** ID of the small cell to be tested
- **rn-name:** Name of the small cell to be tested
- **size:** Size in bytes for the test frames

## To initiate a controller to all small cell link test

**Step 1** From the Operational mode, issue the **request test ip rn-link start** command to initiate the link test:

```
request test ip rn-link start
RNLink Test 1 started
```

**Step 2** Issue the **show Diagnostics IP RNLink** command to view the link test results:

```
show Diagnostics IP RNLink
RNLinkTest: 1
  Status: Success, StartTime: 2012-07-07T18:18:43.416802Z,
  EndTime: 2012-07-07T18:19:13.448203Z
  RNLinkResultsNumberOfEntries: 1
    RNLinkResult: 1, RadioNodeID: 399
      RadioNodeResultStatus: Success, RadioNodeTestDuration: 10
      Size  Rate  TotalFrames  TotalBytes  Throughput (Mbps)  Latency (msecs)  Jitter (msecs)  Packet-loss (%)  OutOfOrderFrames
      -----  -----
      1370  15     14369     19685530          15            1.851864        0.059463       0.000000           25
      64    2      40975     2622400           2            1.715705        0.013891       0.000000          857
      512   12     30769     15753728          12            1.776797        0.029749       0.000000          194
    RNLinkResult: 2, RadioNodeID: 3
      RadioNodeResultStatus: Success, RadioNodeTestDuration: 10
      Size  Rate  TotalFrames  TotalBytes  Throughput (Mbps)  Latency (msecs)  Jitter (msecs)  Packet-loss (%)  OutOfOrderFrames
      -----  -----
      1370  15     14369     19685530          15            1.931428        0.067033       0.000000           18
      64    2      40984     2622976           2            1.762415        0.012858       0.000000          826
      512   12     30768     15753216          12            1.817011        0.060731       0.000000          208
```

## To initiate a targeted link test

**Step 1** From the Operational Mode, issue the following command to initiate a targeted link test. This example tests small cell 922 for 60 seconds at 15 Mbps with frames of 1388 bytes.

```
request test ip rn-link start rn-id 922 duration 60 rate 15 size 1388
RNLink Test 2 started
```

**Step 2** Issue the following command to view the results of the link test:

```
show Diagnostics IP RNLink
RNLinkTest: 1
  Status: Success, StartTime: 2012-07-10T21:31:37.633866Z, EndTime: 2012-07-10T21:35:37.673136Z
  RNLinkResultsNumberOfEntries: 1
    RNLinkResult: 1, RadioNodeID: 922
      RadioNodeResultStatus: Success, RadioNodeTestDuration: 60
      Size  Rate  TotalFrames  TotalBytes  Throughput (Mbps)  Latency (msecs)  Jitter (msecs)  Packet-loss (%)  OutOfOrderFrames
      -----  -----
      1370  15     82145     112538650         14            2.285998        0.090374       4.946132           112
      1370  13     74628     102240360         12            2.237671        0.072346       0.000000            97
      64    2      245895    15737280          2            2.030750        0.087594       0.000000          4018
      512   12     184616    94523392         12            1.910230        0.035920       0.000000          760
```

## 19.8 Service Affecting Actions

The actions and events in this section result in service outages in the Cisco small cell system.

### 19.8.1 USC 8088 Controller Reboots

The following events and actions reboot the controller resulting in a system-wide loss of service:

- The following commands from the Operational Mode:
  - **request system reboot**
  - **request system update package**
  - **request system revert**
  - **request system Database Restore**

- Critical OVER\_TEMPERATURE event
- Crash of a critical process
- Three or more non-critical process crashes in 15 seconds

## 19.8.2 Small Cell Reboots

A controller reboot automatically reboots all of its small cells. The following actions and events cause a small cell reboot resulting in loss of service for its cell:

- The Operational Mode `request system reboot node` command
- Software mismatch
- IP connectivity goes down
- The small cell loses power
- Crash of a critical process
- Three or more non-critical process crashes in 15 seconds
- Critical OVER\_TEMPERATURE event

## 19.8.3 Non-Rebooting Events and Actions

The following events and actions take the cell out of service but do not cause a controller or small cell reboot:

- Loss of IP connectivity to the security gateway
- Changing a parameter in the security gateway connection
- Changing the connection to the core network from one security gateway server to another
- REM scans that change the settings of active cells
- Changing any cell parameter other than *Name* and *Description*
- Administratively disabling the controller, small cell, radio, or cell
- The Operational Mode `request umts self-config neighborlist-create` command

## 19.8.4 Actions Requiring a Reboot

- Changing the security mode for the controller to small cell connection requires a small cell reboot to take effect.



# A Operational States

---

## Operational States

There are four primary attributes that affect the operational state of a managed object:

- **Operability:** whether or not the resource is currently working and providing service
- **Usage:** whether or not the resource is actively in use at a specific instant
- **Administration:** permission to use, or prohibition against, using the resource imposed through the configuration
- **Internal Status:** additional information collected from other subsystems as to the health and status of the managed object, such as conditions and faults

The objects in the system have one of three operational states:

- **Primary state:** Describes the operability of the object:
  - In-Service (IS): The object is currently providing service.
  - MAINT: The system is in maintenance mode.
  - Out-Of-Service (OOS): The object is not currently providing service.
- **Secondary state:** Provides additional information about the primary state, such as usage, administration, and internal status attributes to provide insight as to why the object is either IS or OOS.

If the object is IS, possible secondary state values are:

- ACTIVE: There is at least one resource actively being used by the object.
- BUSY: Not in current use.
- DEGRADED: A minor fault is active that is preventing the object from operating normally.
- EMERGENCY: There is currently an active emergency call on the cell.
- IDLE: Currently the object is not using any resources.
- LOCKED: Locked for accepting new resource requests. For example, it is trying to naturally drop all calls before taking the entity OOS.
- NETMON: The resource is currently operating in network monitor mode.
- NORMAL: The object is operating normally.
- RFMGMNT: The system is in service and a REM scan is active.
- STANDBY: The object is in standby-mode.

If the object is in MAINT, possible secondary state values are:

- RFMGMNT: The system in maintenance mode and a REM scan is active.

If the object is OOS, possible secondary state values are:

- AUTHENTICATING: The object is currently being authenticated.
- CFGMISMATCH: The object is present and configured but the actual hardware does not match the configured hardware. For example, a band 4 radio is present but it is configured as band 1.
- DEPROVISIONING: The object is currently being deprovisioned.

- DIAG: The object is currently running diagnostics.
- DISABLED: The object has been administratively inhibited from being used.
- FAULT: A fault is present on the object.
- INDETERMINATE: Unknown (the cause typically hasn't been determined yet).
- INHERITED: The parent object is not in service. For example, a cell would be inherited if the small cell was OOS.
- INIT: The object is initializing.
- NOTPRESENT: A configured resource is not present.
- PROVISIONING: The object is currently being provisioned.
- SYNCING: The object is currently synchronizing with a peer.
- SWMISMATCH: A configured object is currently running an incorrect version of the software.
- UNPROVISIONED: An object has been detected that has not been provisioned for service.

As an example, the **show RadioNode** command from the Operational Mode displays the *OperState* field. The output below shows that the primary state of small cells 1, 2, and 4 **IS** (In Service) and the secondary state is **NORMAL**. Small cells 6 and 7 have a primary state of **OOS** (Out of Service), the secondary state is **SYNCING** (still provisioning). Small cells 8 and 0 have a primary state **IS**, the secondary state is **DEGRADED**.

**show RadioNode**

RN	Name	Enable	EthernetID	IPAddress	OuterIPAddress	OperState
1	ap-820	true	00:24:48:01:2a:eb	172.17.0.107	172.17.0.107	IS-NORMAL
2	ap-830	true	00:24:48:01:2a:e1	172.17.0.108	172.17.0.108	IS-NORMAL
4	ap-816	true	00:24:48:01:2a:f2	172.17.0.106	172.17.0.106	IS-NORMAL
6	ap-839	true	00:24:48:01:2a:e9	172.17.0.101	172.17.0.101	OOS-SYNCING
7	ap-818	true	00:24:48:01:2a:f4	172.17.0.111	172.17.0.111	OOS-SYNCING
8	ap-822	true	00:24:48:01:2a:b2	172.17.0.112	172.17.0.121	IS-DEGRADED
9	ap-823	true	00:24:48:01:2a:b8	172.17.0.115	172.17.0.122	IS-DEGRADED



## B Miscellaneous Show Commands

The following Operational Mode show commands are convenient for displaying information about the state of the system, but are not discussed in detail elsewhere in this manual. The commands are listed alphabetically, and give sample return values. Refer to the *Cisco 8000 Series OS Data Model Reference Guide* for information about these commands and their parameters.

- [show configuration](#) on page 298
- [show Core](#) on page 299
- [show FAPService 1 CellConfig UMTS RAN FDDFAP PagingRetryCount](#) on page 299
- [show IP ARP](#) on page 300
- [show IP Route](#) on page 300
- [show IP Route Configured](#) on page 300
- [show IP Route Configured Detail](#) on page 300
- [show RadioNode](#) on page 301
- [show RadioNode Radio](#) on page 301
- [show RFMgmt UMTS](#) on page 301
- [show ServicesNode](#) on page 303
- [show Session](#) on page 303
- [show Session Detail UEIPAddress](#) on page 303
- [show Session Detail UENATIPAddress](#) on page 304
- [show Session UMTS Detail SessionID](#) on page 304
- [show Session UMTS Summary](#) on page 305
- [show status](#) on page 305
- [show System File Target](#) on page 305
- [show System File Transfer History](#) on page 306
- [show System UMTS Detail](#) on page 306
- [show UE Location](#) on page 306

## B.1 Sample Show Commands

### B.1.1 show configuration

Use the **show configuration** command to view details of the current configuration. Note that entering this command without a parameter returns all system information. Enter one of the following parameters to filter the information for a more useful return:

- Cell: Table containing the configured system cell list
- DeviceInfo: General device information
- FAPService: Femto Access Point (FAP) service object
- LANDevice: Port number as labeled on device faceplate
- Layer3Forwarding: Forwarding configuration
- Layer3Routing: Routing configuration
- ManagementDevice: Management device port number
- ManagementServer: Parameters relating to the CPE's association with an ACS
- PacketCapture: Packet capture
- QueueManagement: Queuing and classifications (ACLs)
- RadioNode: Parameters relating to small cells
- ServicesNode: Parameters relating to controllers
- System: Parameters relating to the entire system
- Time: System time and NTP related parameters
- details: Show details
- displaylevel: Depth to show

For example:

```
show configuration Layer3Forwarding
Forwarding 1 {
    Enable          true;
    DestIPAddress  0.0.0.0;
    DestSubnetMask 0.0.0.0;
    LANDevice       1;
    IPInterface     1;
}
Forwarding 2 {
    Enable          true;
    DestIPAddress  172.17.0.0;
    DestSubnetMask 255.255.255.0;
    GatewayIPAddress 172.16.0.2;
    LANDevice       2;
    IPInterface     1;
}

show configuration PacketCapture
Enable false;
Mode All;
MaximumFileSize 16;
Filter {
    PeerAPort      40005;
    Protocol       17;
}
```

```
show configuration Time
NTPServer1      10.1.11.200;
NTPServer2      0.0.0.0;
Enable          true;
```

## B.1.2 show Core

Use the **show Core** command to view the connectivity status between the controller and the provider core network:

```
show Core

IPSec:
  SecGWServer 1: Local 172.17.0.8 <-> Remote 172.17.0.1 (Established)
    SN Internal IPAddress: 172.19.0.24

Control:
  Protocol: Iuh
  Iuh gateway (Connected):
    Peering: Local 172.19.0.24:29169 <-> Remote 192.168.10.3:29169
```

## B.1.3 show FAPService 1 CellConfig UMTS RAN FDDFAP PagingRetryCount

Use the **show FAPService 1 CellConfig UMTS RAN FDDFAP PagingRetryCount** command to view the number of times they system will re-send CN originated paging Type 1 messages.

```
show FAPService 1 CellConfig UMTS RAN FDDFAP PagingRetryCount
PagingRetryCount 2;
```

## B.1.4 show FAPService 1 CellConfig UMTS RAN FDDFAP PowerRampSetup

Use the **show FAPService 1 CellConfig UMTS RAN FDDFAP PowerRampSetup** command to view the PRACH preamble power ramp setup parameters:

```
show FAPService 1 CellConfig UMTS RAN FDDFAP PowerControl
ConstantValue      -10;
PowerRampSetup     1;
PreambleRetransMax 10;
MMax               4;
NB01Min            0;
NB01Max            20;
OLPCEnable         true;
MinSIRTargetUL    30;
MaxSIRTargetUL    90;
InitialSIRTargetUL 50;
```

## B.1.5 show FAPService 1 FAPControl UMTS HomeNodeB

Use the **show FAPService 1 FAPControl UMTS HomeNodeB** command to view information about the Home NodeB registration:

```
show FAPService 1 FAPControl UMTS HomeNodeB
```

```
RegistrationTimeout    1;
UERegistrationTimeout 1;
UEIdleTimeout         3600;
```

## B.1.6 show IP ARP

Use the **show IP ARP** command to view information about the Address Resolution Protocol (ARP) table:

```
show IP ARP
Address          HWtype  HWaddress           Flags Mask      Iface
172.17.0.198    ether    00:24:48:00:00:2d  C          ge-2
172.17.0.167    ether    00:24:48:01:2a:3f  C          ge-2
172.17.0.162    ether    00:24:48:01:2a:26  C          ge-2
10.1.15.2       ether    00:22:bd:94:45:53  C          ge-1
10.1.15.5       ether    00:22:bd:94:45:53  C          ge-1
10.1.11.26      ether    00:22:bd:94:45:53  C          ge-1
172.17.0.168    ether    00:24:48:01:2a:0a  C          ge-2
172.17.0.175    ether    00:24:48:01:2a:1f  C          ge-2
172.17.0.164    ether    00:24:48:01:2a:46  C          ge-2
172.17.0.169    ether    00:24:48:01:2a:1c  C          ge-2
172.17.0.161    ether    00:24:48:00:00:47  C          ge-2
```

## B.1.7 show IP Route

Use the **show IP Route** command to view basic information about the configured static routes:

```
show IP Route
RIB 1, 4 destinations
10.0.0.0/8
  *[Connect/1] 2013-02-05T17:02:33Z
    > via LANDevice 1, IPIInterface 1
127.0.0.0/16
  *[Connect/1] 2013-02-05T17:02:17Z
    >
127.1.0.0/16
  *[Connect/1] 2013-02-05T17:02:17Z
    >
172.30.30.0/24
  *[Connect/1] 2013-02-05T17:02:37Z
    > via LANDevice 2, IPIInterface 1
```

## B.1.8 show IP Route Configured

Use the **show IP Route Configured** command to view information about the configured static routes to the default gateway:

DestIPAddress	GatewayIPAddress	DestSubnetMask	LANDevice	IPIInterface	Enable
0.0.0.0	0.0.0.0	0.0.0.0	1	1	true
172.17.0.0	172.16.0.2	255.255.255.0	2	1	true

## B.1.9 show IP Route Configured Detail

Use the **show IP Route Configured Detail** command to view detailed information about the static route to the default gateway:

```
show IP Route Configured Detail
Forwarding 1:
  DestIPAddress: 0.0.0.0, DestSubnetMask: 0.0.0.0
  GatewayIPAddress: 0.0.0.0, LANDevice: 4, IPIInterface: 1,
  ForwardingGroupIndex: 0
```

Forwarding 2:

```
DestIPAddress: 172.17.0.0, DestSubnetMask: 255.255.255.0
GatewayIPAddress: 172.16.0.2, LANDevice: 2, IPInterface: 1, ForwardingGroupIndex: 0
```

## B.1.10 show RadioNode

Use the **show RadioNode** command from the Operational Mode to display the number, name, MAC address, IP addresses, and operational state of each small cell in the system:

<b>show RadioNode</b>		RN	Name	Enable	EthernetID	IPAddress	OuterIPAddress	OperState
1	ap-820	true	00:24:48:01:2a:eb	172.17.0.107	172.17.0.107	IS-NORMAL		
2	ap-830	true	00:24:48:01:2a:e1	172.17.0.108	172.17.0.108	IS-NORMAL		
4	ap-816	true	00:24:48:01:2a:f2	172.17.0.106	172.17.0.106	IS-NORMAL		

## B.1.11 show RadioNode Radio

Use the **show RadioNode Radio** command to display information about the parameters of all radios in the system:

<b>show RadioNode Radio</b>					
RN	Radio	Enable	Band	ActualBand	OperState
1	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
2	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
3	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
4	1	true	umts-band-IV	not-available	OOS-NOTPRESENT
5	1	true	umts-band-IV	not-available	OOS-NOTPRESENT
7	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
8	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
9	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
10	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
11	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
12	1	true	umts-band-IV	umts-band-IV	IS-NORMAL
13	1	true	umts-band-IV	not-available	OOS-NOTPRESENT
14	1	true	umts-band-IV	umts-band-IV	IS-NORMAL

## B.1.12 show RFMgmt UMTS

Use the **show RFMgmt UMTS** command with its parameters to display aspects of the current RF management state. Top level parameters for this command are:

- **Configuration:** Show configuration
- **DetectedCells:** Show detected cells
- **MeasurementOfGSMCell:** Show internal cells that detected GSM cells
- **MeasurementOfUMTSCell:** Show internal cells that detected UMTS cells
- **NeighborCells:** Show neighbor cells

<b>show RFMgmt UMTS MeasurementOfGSMCell</b>								
Detecting	CellID	Detecting	CID	BSIC	CI	ARFCN	BandID	RSSI
	131072001		1	25	5176	128	GSM 850	-80
	131072001		1	27	32004	129	GSM 850	-69

131072004	4	25	5176	128	GSM	850	-75
131072004	4	27	32004	129	GSM	850	-68

**show RFMgmt UMTS Configuration**

Global Configuration:

.....

FAPService REM Configuration:

=====

WCDMAFDD:

Scan Periodically	false
Periodic Interval	86400
Periodic Time	1970-01-04T00:00:00Z
DL UARFCN List	-
Periodic TxPwr Refresh	false
Periodic TxPwr Refresh Interval	86400

GSM:

Periodic Interval	86400
REM Band List	-
ARFCN List	-

FAPService REM Scans:

=====

GSM	REM Scan	true
UMTS Ext IntraFreq	REM Scan	true
UMTS Ext InterFreq	REM Scan	true
UMTS Int IntraFreq	REM Scan	true

FAPService Locks:

=====

RF	Lock	false
Neighbor List	Lock	false
PSC	Lock	false
Max FAP Tx Power	Lock	false

[output truncated]

**show RFMgmt UMTS DetectedCells**

List Of Cells Detected By Internal Cell With Cell Handle 1, CID 1, And Cell ID 65536001:

-----

Detected INTERNAL UMTS Cells:

CID	Cell Handle	Cell ID	PSC	DL UARFCN	CPICH	RSCP*
2	2	65536002	2	1962	-	-74
3	3	65536003	3	1962	-	-93

\* Measured When Detected Internal UMTS Cell Was Transmitting At FAPService Maximum MaxFAPTxPower

Detected EXTERNAL UMTS Cells:

CID	Cell Handle	Cell ID	PSC	DL UARFCN	PCPICH TxPower	CPICH	RSCP
-----	-----	-----	---	-----	-----	-----	-----

Detected GSM Cells:

Cell Handle	ARFCN	Frequency Band	BSIC	CI	RSSI
-----	-----	-----	---	-----	-----

List Of Cells Detected By Internal Cell With Cell Handle 2, CID 2, And Cell ID 65536002:

Detected INTERNAL UMTS Cells:

=====

CID	Cell Handle	Cell ID	PSC	DL	UARFCN	CPICH	RSCP*
1	1	65536001	1	1962		-79	
3	3	65536003	3	1962		-84	

\* Measured When Detected Internal UMTS Cell Was Transmitting At FAPService Maximum MaxFAPTxPower

Detected EXTERNAL UMTS Cells:

=====

CID	Cell Handle	Cell ID	PSC	DL	UARFCN	PCPICH TX Power	CPICH	RSCP

Detected GSM Cells:

=====

Cell Handle	ARFCN	Frequency	Band	BSIC	CI	RSSI

[output truncated]

## B.1.13 show ServicesNode

Use the **show ServicesNode** command to view the controllers in the system:

show ServicesNode		
SN	ArriveTime	OperState
1025	2011-09-27T23:57:35Z	IS-NORMAL

## B.1.14 show Session

Use the **show Session** command to display all active UE sessions:

show Session							
Session	IMSI	D	V	ConnectTime	Type		
926107	001010123451204	0	1	01-11 18:39:39.98	UMTS		
926106	001010123451065	1	0	01-11 18:39:39.64	UMTS		
926104	001010123451342	0	1	01-11 18:39:32.30	UMTS		
926101	001010123451285	0	1	01-11 18:39:29.11	UMTS		
926098	001010123451134	0	0	01-11 18:39:20.79	UMTS		
925973	001010123451133	1	0	01-11 18:35:50.88	UMTS		
925897	001010123451388	0	1	01-11 18:33:26.53	UMTS		
925894	001010123451385	0	1	01-11 18:33:22.05	UMTS		

## B.1.15 show Session Detail UEIPAddress

Use the **show Session Detail UEIPAddress** command to display information about all voice and data connections for given IP address of a connected device. This command is useful for locating the IMSI of the device, which can then be used for access control and in debugging procedures.

**show Session Detail UEIPAddress 10.1.80.174**

Session: 173384

```

RATType: UMTS, IMSI: 001010123451269
NumberOfActiveDataSessions: 1, NumberOfActiveVoiceSessions: 0
DataSessionNumberOfEntries: 1, VoiceSessionNumberOfEntries: 0
ConnectTime: 2011-09-21T14:52:38.550501Z
RRCSState: Cell_PCH, UMTSSessionID: 1048579917, CurrentSnapshotID: 24, ServingCellHandle: 14
CSDomainActive: false, CSSessionType: UNKNOWN
PSDomainActive: true, PSSessionType: HSUPA
DataSession: 173385
    FlowID: 483, APNName: 11apn1, SwitchingMode: PassThrough
    UEIPAddress: 10.1.80.174
    PrimaryDNSIPAddress: 0.0.0.0, SecondaryDNSIPAddress: 0.0.0.0, ProviderPrimaryDNSIPAddress: 10.1.11.200,
    ProviderSecondaryDNSIPAddress: 10.1.11.200
RLC DTCH stats:
    RadioBearer: 5
        RLCMode: AM, RBType: DTCH, IsActive: true
Handover Statistics:
    NumServingCellChanges: 3, NumAsetAdds: 7, NumAsetDeletes: 2, NumAsetSwaps: 0
RadioLinks:
    RadioLink: 1
        CellHandle: 14, PSC: 206, RLID: 0, IsActive: false, IsServingCell: 1

```

## B.1.16 show Session Detail UENATIPAddress

Use the **show Session Detail UENATIPAddress** command to display information about all voice and data connections for each IMSI in a given NATted IP address of a connected device. This command is useful for locating the IMSI of the device, which can then be used for access control and in debugging procedures.

### **show Session Detail UENATIPAddress 172.20.0.108**

```

Session: 173384
RATType: UMTS, IMSI: 001010123451355
NumberOfActiveDataSessions: 1, NumberOfActiveVoiceSessions: 0
DataSessionNumberOfEntries: 1, VoiceSessionNumberOfEntries: 0
ConnectTime: 2011-09-21T14:55:18.550501Z
RRCSState: Cell_DCH, UMTSSessionID: 1048579935, CurrentSnapshotID: 12, ServingCellHandle: 4
CSDomainActive: false, CSSessionType: UNKNOWN
PSDomainActive: true, PSSessionType: HSUPA
DataSession: 173385
    FlowID: 483, APNName: apn3, SwitchingMode: NAPT
    UEIPAddress: 10.1.80.155, UENATIPAddress: 172.20.0.108
    PrimaryDNSIPAddress: 0.0.0.0, SecondaryDNSIPAddress: 0.0.0.0, ProviderPrimaryDNSIPAddress: 10.1.11.200,
    ProviderSecondaryDNSIPAddress: 10.1.11.200
RLC DTCH stats:
    RadioBearer: 5
        RLCMode: AM, RBType: DTCH, IsActive: true
Handover Statistics:
    NumServingCellChanges: 3, NumAsetAdds: 7, NumAsetDeletes: 2, NumAsetSwaps: 0
RadioLinks:
    RadioLink: 1
        CellHandle: 4, PSC: 201, RLID: 0, IsActive: false, IsServingCell: 1

```

## B.1.17 show Session UMTS Detail SessionID

Use the **show Session UMTS Detail SessionID** command to display detailed information about a specific UE session:

### **show Session UMTS Detail SessionID 2453027**

```

Session: 2453027
RATType: UMTS, IMSI: 001010123451129
NumberOfActiveDataSessions: 1, NumberOfActiveVoiceSessions: 0
DataSessionNumberOfEntries: 1, VoiceSessionNumberOfEntries: 0
ConnectTime: 2012-06-12T02:57:16.136493Z
RRCSState: Cell_DCH, UMTSSessionID: 1048576025, CurrentSnapshotID: 1,
ServingCellHandle: 6
CSDomainActive: false, CSSessionType: UNKNOWN
PSDomainActive: true, PSSessionType: HSPA
DataSession: 2453028
    FlowID: 4, SwitchingMode: PassThrough
    UEIPAddress: 10.1.15.225
    PrimaryDNSIPAddress: 0.0.0.0, SecondaryDNSIPAddress: 0.0.0.0,
    ProviderPrimaryDNSIPAddress: 10.1.11.200,
    ProviderSecondaryDNSIPAddress: 10.1.11.200
RLC DTCH stats:
    RadioBearer: 5
        RLCMode: AM, RBType: DTCH, IsActive: true
Handover Statistics:
    NumServingCellChanges: 0, NumAsetAdds: 215, NumAsetDeletes: 215,
    NumAsetSwaps: 0

```

```
RadioLinks:
  RadioLink: 1
    CellHandle: 6, PSC: 507, RLID: 2, IsActive: true, IsServingCell: 1
  RadioLink: 2
    CellHandle: 5, PSC: 4, RLID: 1, IsActive: false, IsServingCell: 0
```

## B.1.18 show Session UMTS Summary

Use the **show Session UMTS Summary** command to view specific information about a session. It can be filtered by cell, user session, IP address, or NATted IP address. You can also view the session history.

### **show Session UMTS Summary**

```
Total sessions (active 8, peak 28)

CS sessions (active 3, peak 15):
  EmergencyCall: active 0, peak 0
  Voice: active 2, peak 14
  VideoTelephony: active 0, peak 0
  SMS: active 0, peak 0
  Registration: active 1, peak 4

PS sessions (active 5, peak 14):
  R99Data: active 1, peak 1
  HSDPA: active 2, peak 2
  HSUPA: active 2, peak 12
  Registration: active 0, peak 4
```

## B.1.19 show status

Use the **show status** command to view the current system status. Note that entering this command without a parameter returns the status of all objects in the system. This can be extremely detailed. The following parameters filter the output. Most of these have one or more parameters below them for additional filtering.

- OpState: Read only view of configuration and run time state
- Statistics: Statistics management operations
- airlink: Air link operations
- core: Core level commands
- debug: show debug settings
- displaylevel: Depth to show
- process-details: show process-details
- processes: show process list
- system: System operations
- umts: UMTS operations

## B.1.20 show System File Target

Use the **show System File Target** command to display the status of file upload targets:

### **show System File Target**

ModuleID	Host	Priority	Enable	MaxAttemptDuration	MaxAttempts	FailedAttempts
DebugLog	10.1.11.17	Primary	true	0	10	22

## B.1.21 show System File Transfer History

Use the **show System File Transfer History** command to view all files transferred since the last reboot:

<b>show System File Transfer History</b>					
TransID	ModuleID	Status	RequestCompleteTime	FailedAttempts	LastError
1024	DebugLog	Complete	2011-09-28T13:32:39Z	0	-
1025	DebugLog	Complete	2011-09-28T14:55:19Z	0	-
1026	DebugLog	Complete	2011-09-28T15:11:06Z	0	-
1027	DebugLog	Complete	2011-09-28T15:17:35Z	0	-
1028	DebugLog	Complete	2011-09-28T15:25:07Z	0	-
1029	DebugLog	Complete	2011-09-28T15:29:40Z	0	-
1030	DebugLog	Complete	2011-09-28T16:03:44Z	0	-
1031	DebugLog	Complete	2011-09-28T16:56:00Z	0	-
1032	DebugLog	Complete	2011-09-28T17:13:03Z	0	-
1033	DebugLog	Complete	2011-09-28T18:07:16Z	0	-
1034	DebugLog	Complete	2011-09-28T18:41:14Z	0	-
1035	DebugLog	Complete	2011-09-28T19:09:32Z	0	-
1036	DebugLog	Complete	2011-09-28T20:03:37Z	0	-
1037	DebugLog	Complete	2011-09-28T20:19:14Z	0	-
1038	DebugLog	Complete	2011-09-28T20:53:12Z	0	-

## B.1.22 show System UMTS Detail

Use the **show System UMTS Detail** command to display detailed information about UMTS sessions:

<b>show System UMTS Detail</b>
Current Status:
TimeOfLastStatsReset: 2011-09-19T16:10:37.72018Z
TimeOfLastStatsUpdate: 2011-09-20T13:54:00.664837Z
NumCellsProvisioned: 1
NumCellsActive: 0
IuCSStatus: Connected
IuPSSStatus: Connected
EmergencyCallActive: false
Current Sessions:
EmergencyCall: 0 R99Data: 0
Voice: 0 HSDPA: 0
VideoTelephony: 0 HSUPA: 0
SMS: 0 Registration: 0
Registration: 0 NumPSSessions: 0
NumCSSessions: 0
NAS:
LocationUpdatingRequest: 21
LocationUpdatingReject: 0
[output truncated]

## B.1.23 show UE Location

Use the **show UE Location** command to display location information for a specified UE:

<b>show UE Location IMSI 001010123451341</b>					
UEID	IMSI	IMEI	LastUpdate	LastSessionID	LastServingCell
8	001010123451341	-	09-29 23:07:25.70	406142	12