7705 SAR-Hm
7705 SAR-Hmc
Release 25.7.R1

Interface Configuration Guide

3HE 21730 AAAB TQZZA
Edition: 01
July 2025

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

List of tables

List of figures

1 Preface

1.1 How to use this guide

The 7705 SAR-Hm series of routers is made up of the 7705 SAR-Hm and the 7705 SAR-Hmc. Unless specified otherwise, references in this guide to the router, the node, or the system apply to both chassis.

This guide is organized into functional chapters that describe the operation of the routers. It provides conceptual information as well as Command Line Interface (CLI) syntax and command descriptions for provisioning ports, interfaces, and functionality that is specifically related to the 7705 SAR-Hm series.

The 7705 SAR-Hm series shares functionality with the SR OS and the Virtualized Service Router (VSR). This guide is intended to be used in conjunction with guides from the SR software documentation set. Chapters in this guide map to the SR software guides. Shared functionality between the SR OS and the 7705 SAR-Hm series is referenced in each chapter of this guide but described in the relevant SR software guide; users are directed to the appropriate location in the SR guide for information. For ease of use, all references are mapped to section headings in the SR guides. When a high-level section heading from an SR guide is referenced without references to lower-level sections, this indicates that all the functionality described in that section is supported on the 7705 SAR-Hm series. When lower-level section headings are specified, this indicates that only the functionality described in those sections is supported. Lower-level section headings are omitted if those areas of functionality are not supported on the 7705 SAR-Hm series.

Note: This manual generically covers supported Release 25.x.Rx content and may contain some content that will be released in later maintenance loads. Please see the *7705 SAR-Hm and SAR-Hmc 25.x.Rx Software Release Notes*, part number 3HEYYYYYxxxxTQZZA, for information about features supported in each load of the Release 25.x.Rx software.

1.1.1 Software guides in this documentation suite

The software guides that make up the documentation suite for the 7705 SAR-Hm series of routers are as follows:

- *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*
- *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*

Table 1: 7450 ESS, 7750 SR, 7950 XRS, and VSR software guides lists the guides from the SR software documentation suite that are intended to be used with the guides from the 7705 SAR-Hm series.

Table 1: 7450 ESS, 7750 SR, 7950 XRS, and VSR software guides

Guide title	Description
7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide	This guide describes system concepts and provides configuration explanations and examples to configure SR OS boot option file (BOF), file system, and system management functions.

Guide title	Description
7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide	This guide describes system security features, SNMP, and event and accounting logs. It covers basic tasks such as configuring management access filters, passwords, and user profiles.
7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide	This guide describes logical IP routing interfaces and associated attributes such as IP addresses, as well as IP and MAC-based filtering.
7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide	This guide provides an overview of unicast routing concepts and provides configuration examples for Routing Information Protocol (RIP) and Border Gateway Protocol (BGP) routing protocols and for route policies.
7450 ESS, 7750 SR, 7950 XRS, and VSR Multicast Routing Protocols Guide	This guide provides an overview of multicast routing concepts and provides configuration examples for Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), Multipoint LDP, multicast extensions to BGP, and Multicast Connection Admission Control (MCAC).
7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide	This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), and Label Distribution Protocol (LDP).
7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide	This guide provides a general overview of functionality provided by the routers and describes how to configure service parameters such as Service Access Points (SAPs), Service Distribution Points (SDPs), customer information, and user services.
7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide	This guide describes Layer 2 service and Ethernet Virtual Private Network (EVPN) functionality and provides examples to configure and implement Virtual Leased Lines (VLLs), Virtual Private LAN Service (VPLS), Provider Backbone Bridging (PBB), and EVPN.
7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN	This guide describes Layer 3 service functionality and provides examples to configure and implement Internet Enhanced Services (IES) and Virtual Private Routed Network (VPRN) services.
7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide	This guide describes how to configure Quality of Service (QoS) policy management.
7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide	This guide describes how to use the Operations, Administration and Management (OAM) and diagnostics tools.

Guide title	Description
7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide	This guide describes how to provision Input/Output Modules (IOMs), Media Dependent Adapters (MDAs), connectors, and ports.
7450 ESS, 7750 SR, and VSR Multiservice ISA and ESA Guide	This guide describes services provided by integrated service adapters, such as Application Assurance, IPSec, ad insertion (ADI), and Network Address Translation (NAT).
SR OS Log Events Guide	This guide describes log events that apply to the 7705 SAR-Hm series of routers.
7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide	This guide describes the Triple Play Service Delivery Architecture (TPSDA) support and provides examples to configure and implement various protocols and services.
7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide	This guide describes all classic CLI commands and their supported values and parameters.
7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide	This guide describes all clear, show, and tools commands for both classic and MD-CLI and their supported values and parameters.

1.1.2 Technical support

If you purchased a service agreement for your 7705 SAR-Hm series router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased a Nokia service agreement, follow this link to contact a Nokia support representative and to access product manuals and documentation updates:

Product Support Portal

2 Interfaces

This chapter provides overview information about the types of interfaces supported on 7705 SAR-Hm series routers.

Note: For specific information about the topics that are not explicitly described in this guide (in black text in the list below), see the corresponding topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*.

Topics in this chapter include:

- Configuration overview
  - Chassis IOM and MDAs
- Ports
  - Port types
  - Port features
    - Port State and Operational State
- Port Cross-Connect
  - PXC Terminology
  - Overview
  - PXC sub-ports
  - PXC statistics
  - Basic PXC provisioning
  - Health monitoring on the PXC
  - Configuration example
- MTU configuration guidelines
  - Default and maximum MTU values
  - MTU considerations over a cellular port
  - MTU considerations over the WLAN interface
- Serial transport over raw sockets
  - Raw socket configuration
  - Raw socket packet processing
  - Raw socket squelch functionality
- Configuration process overview
- Configuration notes

2.1 Configuration overview

This guide uses the term preprovisioning in the context of preparing or preconfiguring ports and interfaces before enabling them. When the entity is in a **no shutdown** state (administratively enabled), the entity is considered provisioned.

2.1.1 Chassis IOM and MDAs

The 7705 SAR-Hm series routers have a fixed physical configuration that uses an integrated control and switching functional block. The Input/Output module (IOM) and Media Dependent Adapters (MDAs) are also integrated into the chassis.

On the CLI, a port is identified using the format *slot/mda/port*. The slot ID identifies the IOM and is always 1. The MDA identifiers are:

- 1/1 for the cellular MDA and for the GNSS receiver
- 1/2 for the Ethernet MDA
- 1/3 for the serial port MDA
- 1/4 for the WLAN port MDA
- 1/5 for the virtualized integrated ISA MDA, for IPSec, IP tunnel, Network Address Translation (NAT), and Application Assurance (AA) firewall functionality
- 1/6 for the virtualized integrated ISA MDA, for IPSec, IP tunnel, NAT, and AA firewall functionality

On the 7705 SAR-Hm, MDAs 1/1 through 1/4 are automatically provisioned and cannot be deprovisioned. MDAs 1/5 and 1/6 are not automatically provisioned, but can be provisioned and deprovisioned. When they are deprovisioned, the operator must reset the node to ensure the MDAs are completely deprovisioned before being reprovisioned.

On the 7705 SAR-Hmc, MDAs 1/1, 1/2, and 1/3 are automatically provisioned. MDAs 1/5 and 1/6 are not automatically provisioned, but can be provisioned and deprovisioned. When MDAs 1/5 and 1/6 are deprovisioned, the operator must reset the node to ensure the MDAs are completely deprovisioned before being reprovisioned.

Table 2: CLI port Identifiers lists the CLI port identifiers for each port type on the chassis.

Table 2: CLI port Identifiers

Port type	CLI identifier	Variable definition
Cellular	1/1/*port-id*	*port-id* is the port number, 1 or 2
Ethernet	1/2/*port-id*	*port-id* is the port number: • from 1 to 6 on the 7705 SAR-Hm • from 1 to 3 on the 7705 SAR-Hmc
RS-232	1/3/*port-id*	*port-id* is the port number, 1 or 2
WLAN	1/4/*port-id*	*port-id* is the port number, 1 or 4

There are virtual ports in the CLI for the isa-tunnel-v, the isa-bb-v, and the isa-aa-v virtualized MDAs.

The following chassis and card names are used on the CLI:

- integrated control and switching functional block—cpm-sar-hm or cpm-sar-hmc
- IOM—iom-sar-hm or iom-sar-hmc
- cellular MDA 1/1—i2-cellular
- Ethernet MDA in slot 1/2—i6-10/100eth-tx or i3-10/100eth-tx
- serial port MDA in slot 1/3—i2-sdi
- WLAN port MDA in slot 1/4—i1-wlan or blank
- virtualized integrated ISA MDA in slot 1/5—isa-tunnel-v, isa-bb-v, or isa-aa-v
- virtualized integrated ISA MDA in slot 1/6—isa-tunnel-v, isa-bb-v, or isa-aa-v

The following CLI output shows the factory-provisioned settings when the **show card state** command is issued on the 7705 SAR-Hm.

```
*A:Dut-C# show card state
===============================================================================
Card State
===============================================================================
Slot/  Provisioned Type                  Admin Operational   Num   Num Comments
Id         Equipped Type (if different)  State State         Ports MDA
-------------------------------------------------------------------------------
1      iom-sar-hm                        up    up                  6
1/1    i2-cellular                       up    up            2
1/2    i6-10/100eth-tx                   up    up            6
1/3    i2-sdi                            up    up            2
1/4    i1-wlan                           up    up            2
1/5    (not provisioned)                 up    unprovisioned 4
           isa-ms-v
1/6    (not provisioned)                 up    unprovisioned 4
           isa-ms-v
A      cpm-sar-hm                        up    up                      Active
===============================================================================
```

The CLI output for the example above looks similar to the following output when the **config>card 1** and the **info** commands are issued on the 7705 SAR-Hm:

```
*A:Dut-C# configure card 1
*A:Dut-C>config>card# info
----------------------------------------------
        card-type iom-sar-hm
        mda 1
            mda-type i2-cellular
            no shutdown
        exit
        mda 2
            mda-type i6-10/100eth-tx
            no shutdown
        exit
        mda 3
            mda-type i2-sdi
            no shutdown
        exit
        mda 4
            mda-type i1-wlan
            no shutdown
        exit
```

```
        no shutdown
-----------------------------------------
*A:Dut-C>config>card#
```

The following CLI output shows the factory-provisioned settings when the **show card state** command is issued on the 7705 SAR-Hmc.

```
A:Dut-C# show card state
===============================================================================
Card State
===============================================================================
Slot/  Provisioned Type                  Admin Operational   Num   Num Comments
Id         Equipped Type (if different)  State State         Ports MDA
-------------------------------------------------------------------------------
1      iom-sar-hmc                       up    up                  6
1/1    i2-cellular                       up    up            2
1/2    i3-10/100eth-tx                   up    up            3
1/3    i2-sdi                            up    up            2
1/5    (not provisioned)                 up    unprovisioned 2
           isa-ms-v
1/6    (not provisioned)                 up    unprovisioned 2
           isa-ms-v
A      cpm-sar-hmc                       up    up                     Active
===============================================================================
```

The CLI output for the example above looks similar to the following output when the **config>card 1** and the **info** commands are issued on the 7705 SAR-Hmc:

```
A:Dut-C# configure card 1
A:Dut-C>config>card# info
-----------------------------------------
        card-type iom-sar-hmc
        mda 1
            mda-type i2-cellular
            no shutdown
        exit
        mda 2
            mda-type i3-10/100eth-tx
            no shutdown
        exit
        mda 3
            mda-type i2-sdi
            no shutdown
        exit
        no shutdown
-----------------------------------------
*A:kansarhmc1: Dut-A>config>card#
```

2.2 Ports

This section provides information about the types of ports supported on the system.

2.2.1 Port types

The system supports the port types listed below.

- Cellular

  The cellular interface supports dual SIM operation using major carrier frequency bands in North America, EMEA, and APAC. For more information about cellular ports, see Cellular MDA and ports.

- Ethernet

  The system supports Fast Ethernet (10/100Base-T) ports. The Ethernet ports are typically connected to field devices, such as Intelligent Electronic Devices (IEDs), AMI collectors, supervisory modules, weather monitoring devices, cameras, and other hosts.

  In some cases, an Ethernet port may be connected to a 7705 SAR-18, 7705 SAR-8, 7705 SAR-H, or 7705 SAR-Hc node, which will use the system's cellular port as a backup link.

  For more information about Fast Ethernet ports, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*, '"Port types".

- Serial

  RS-232 asynchronous ports are typically used for connecting to remote SCADA equipment. The ports support full-duplex communication and interface speeds of 600 b/s, 1200 b/s, 2400 b/s, 4800 b/s, 9600 b/s, 19 200 b/s, 38 400 b/s, 57 600 b/s, and 115 200 b/s. The serial ports can be configured to support raw socket transport; see Serial transport over raw sockets for more information.

- Alarm

  For information about the alarm port and the number of supported alarm inputs and outputs, see the *SAR-Hm and SAR-Hmc Chassis Installation Guide*.

  For information about configuring alarm inputs, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*.

  Alarm inputs are configured using the **config>system>alarm-contact-input** command and sub-commands. For information, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

  To display the status of the alarm inputs, use the **show>system>alarm-contact-input all** command; see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide* for information.

- WLAN

  The WLAN interface supports the IEEE 802.11 b/g/n WLAN standard. The interface is enabled as a WLAN access point (AP) that remote WLAN stations can connect to. For more information, see Wireless LAN interface. WLAN traffic that is received from WLAN stations connected to the WLAN AP is transported over a Layer 2 service using an Epipe. See the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide* for details about configuring services for the WLAN AP.

2.2.2 Port features

For general information about port features, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*, "Port state and operational state".

2.3 MTU configuration guidelines

Observe the general rules described in "MTU configuration guidelines" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide* when planning service and physical MTU configurations.

2.3.1 Default and maximum MTU values

Table 3: MTU default and maximum values lists the default and maximum MTU values for Fast Ethernet ports, cellular ports, and the WLAN interface.

For information about how to modify the MTU defaults, see "Modifying MTU defaults" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*.

Table 3: MTU default and maximum values

Port type	Mode	Default	Maximum
Fast Ethernet	Access/network	1514 bytes (includes Ethernet header, but excludes Ethernet CRC)	1622 bytes
Cellular interface	Network (PDN router interface)	None Operators must configure this value on the PDN router interface to ensure correct operation of a cellular port.	1486 bytes
WLAN interface	Access	1500 bytes (non-configurable)	1500 bytes (non-configurable)

2.3.2 MTU considerations over a cellular port

The cellular port IP layer MTU is derived from the PDN router interface that is configured for the cellular port. By default, the PDN router interface MTU is not set. To operate the cellular interface without failures, an MTU value that is less than or equal to 1486 bytes must be configured (using the **ip-mtu** command) for the PDN router interface. For information about configuring the PDN router interface, see "PDN router interface command descriptions" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

Mobile networks often require a strict IP layer MTU for the cellular interface that is less than or equal to1486 bytes. Consult with the cellular service provider about the correct IP layer MTU value to set for the associated PDN router interface.

The SAP MTU settings must also correctly account for the PDN router interface IP layer MTU, as services that are transported over the cellular interface are impacted by this configuration.

For example, if a cellular provider allows an IP layer MTU of 1486 bytes, the following calculations and values must be considered when setting up services over a cellular port.

For BGP and T-LDP protocols, the MTU of protocol packets must be set to 1486 bytes or less. For information about BGP path MTU discovery and LDP path MTU discovery, see the **path-mtu-discovery** command in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

For Layer 3 services over a VPRN service using GRE transport, the SAP MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VPRN service label)}
- SAP MTU = {1486 bytes- (24 bytes) - (4 bytes)}
- SAP MTU = 1458 bytes

For Layer 3 services over a VPRN service using GRE transport with NGE enabled, the SAP MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VPRN service label) - (NGE overhead)}
- SAP MTU = {1486 bytes - (24 bytes) - (4 bytes) - (77 bytes)}
- SAP MTU = 1381 bytes

For Layer 2 services over a VPLS service using GRE transport, the SAP (port) MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VPLS service label)}
- SAP MTU = {1486 bytes - (24 bytes) - (4 bytes)}
- SAP MTU = 1458 bytes

For Layer 2 services over a VPLS service using GRE transport with NGE enabled, the SAP MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VPLS service label) - (NGE overhead)}
- SAP MTU = {1486 bytes - (24 bytes) - (4 bytes) - (77 bytes)}
- SAP MTU = 1381 bytes

For Layer 2 services using an Epipe VLL/VPWS service with a control word, an additional 4 bytes of overhead is required for the control word. Therefore, the following SAP (port) MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VLL service label) - (CTL word)}
- SAP MTU = {1486 bytes - (24 bytes) - (4 bytes) - (4 bytes)}
- SAP MTU = 1454 bytes

For Layer 2 services using an Epipe VLL/VPWS service with a control word and NGE enabled, an additional 4 bytes of overhead is required for the control word and 4 bytes of NGE overhead is added. Therefore, the following SAP (port) MTU must be set as follows:

- SAP MTU = {1486 bytes - (GRE packet overhead) - (VLL service label) - (CTL word) – (NGE overhead)}
- SAP MTU = {1486 bytes - (24 bytes) - (4 bytes) - (4 bytes) - (81 bytes)}
- SAP MTU = 1373 bytes

The SAP MTU of Layer 2 services can be increased to accommodate larger packets that are closer to the Ethernet port maximum MTU value by using GRE SDP fragmentation and reassembly. See "GRE SDP tunnel fragmentation and reassembly" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

2.3.3 MTU considerations over the WLAN interface

The WLAN port MTU value is set to 1500 bytes and cannot be changed. Since cellular ports have a lower MTU with a maximum of 1486 bytes, and WLAN traffic from stations connected to the WLAN AP is carried over an IP/MPLS service that adds additional overhead to traffic traveling over cellular ports, the operator must understand the requirements of the MTU for their applications in order to successfully use the WLAN interface.

For example, when the WLAN interface AP is connected to the Nokia WLAN GW using an Epipe service, there is at most 1454 bytes available to carry a Layer 2 packet for the WLAN AP packet that includes a Layer 2 header of 14 bytes (see MTU considerations over a cellular port for information about the SAP MTU of an Epipe service over a cellular port). In order to successfully send these packets over a cellular port without further modification, the MTU of the IP payload in the WLAN AP Layer 2 packet must be restricted to 1440 bytes.

The MTU of the WLAN interface can be handled in one of two ways:

- by modifying the MTU value on clients that are connecting to the WLAN AP such that they send traffic that conforms to the service MTU of the IP/MPLS transport service, minus the 14 byte Layer 2 overhead
- by configuring GRE SDP fragmentation and reassembly on the node to allow packets that require an MTU greater than that available on the cellular interface to be fragmented and reassembled when carried over the cellular interface

2.4 Serial transport over raw sockets

Serial transport over raw sockets provides the capability of transporting serial data, in the form of characters, over an IP transport service within a Layer 3 IP/MPLS VPRN service. A raw socket allows direct sending and receiving of IP packets without any protocol-specific transport layer formatting. For information about raw socket IP transport services, see "Raw socket IP transport service" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

The feature provides the functionality for a local host to listen to and open raw socket sessions from remote hosts, and for a remote host to initiate and open raw socket sessions to local hosts. The local and remote host functions support TCP or UDP sessions (but not both concurrently) over the IP transport service.

Raw sockets are supported for RS-232 ports on the node.

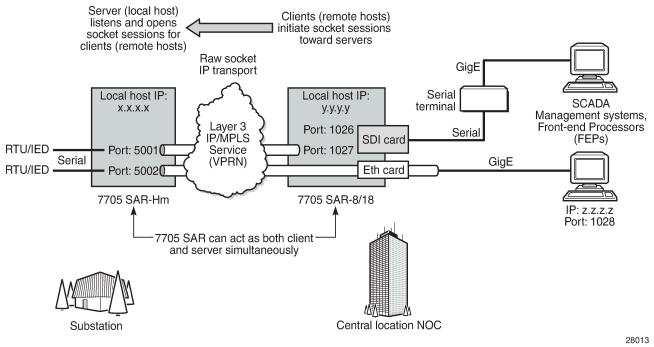
Figure 1: Serial transport over raw socket application shows an example of a raw socket application, where serial data is transferred between RTUs and a utility's SCADA management system using an IP transport service across a Layer 3 VPRN service that includes 7705 SAR-Hm and 7705 SAR-8/7705 SAR-18 nodes.

A raw socket local host (acting as a server) at the 7705 SAR-Hm substation listens to TCP sessions that originate at the 7705 SAR-8 or 7705 SAR-18 central location network operations center (NOC). The 7705 SAR-8 or 7705 SAR-18 at the NOC is connected to two front-end processors (FEPs), one via a serial port and another via an Ethernet port. The serial port on the 7705 SAR-8 or 7705 SAR-18 is configured as a remote host (acting as a client) that initiates TCP/UDP sessions toward the RTU at the 7705 SAR-Hm substation when traffic is received from the FEP over the serial port. These TCP/UDP sessions are transported over the IP/MPLS network using IP transport service over a VPRN service. The serial data transported over the TCP/UDP session and received at the 7705 SAR-Hm is then sent over the serial link toward the RTU. TCP/UDP sessions received from the FEP over the Ethernet port are transported over a VPRN service (that is, there is no need for serial port remote host configuration in this case).

Multiple FEPs can poll a single RTU. If multiple sessions attempt to transmit serial data on the serial port simultaneously, the 7705 SAR-Hm queues packets per session and ensures that all data for one session is sent out before processing another session's data, ensuring that sessions do not overlap one another.

Note: A serial port can be concurrently configured as both a server (local host) and a client (remote host). This is accomplished with the **local-host** command configuration to support the server function and the **remote-host** command configuration to set up client sessions to far-end remote hosts.

Figure 1: Serial transport over raw socket application



2.4.1 Raw socket configuration

A raw socket IP transport interface can be configured for each RS-232 serial port on a node. This allows the serial port to receive TCP connections or UDP session packets from multiple remote hosts, or to create new sessions to remote hosts in order to send and receive serial data to and from those remote hosts.

There are port-level and service-level configuration requirements for a raw socket serial port to send and receive serial data in either server mode, client mode, or both modes.

Raw socket port-level configuration includes defining the end of packet checking parameters (idle time, length, special character) and the inter-session delay for transmitting session data over the serial link.

At the service level, an IP transport subservice is created within a VPRN service to associate the serial port with the VPRN service. TCP/UDP encapsulated serial data is routed within the corresponding Layer 3 VPRN service. The required configuration includes IP transport subservice local host and remote host configuration, TCP timers, and session control.

See Serial raw socket interface configuration commands for information about the required port-level configuration. For information about how the IP transport subservice operates within a VPRN service, as well as information about the required system-level configuration, see "Raw socket IP transport service" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

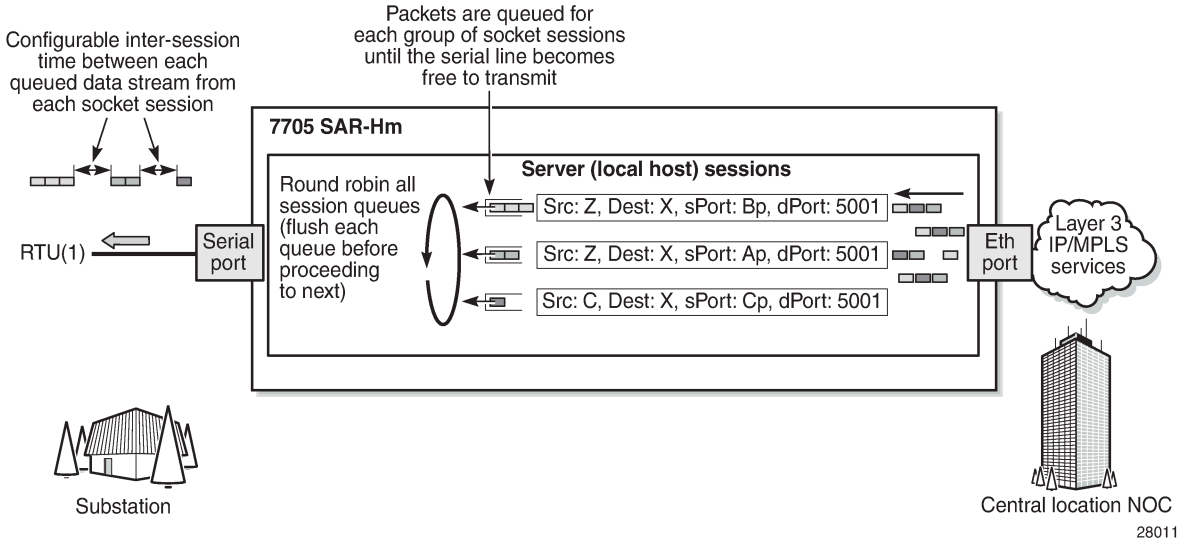
2.4.2 Raw socket packet processing

Figure 2: Raw socket packet processing illustrates how raw socket packets are processed over a serial link.

Session data attempting to access the serial port is queued. One queue is maintained per session. The purpose of the session queue is to prevent two different flows of packets from interleaving out the serial

port and creating unreadable messages. When data is being transmitted over the serial link for a session, any other session's data is queued until the first session has emptied its queue. The next session's data is transmitted over the serial link only after the **inter-session-delay** timer expires. Each session's data is sent out in round-robin fashion.

Figure 2: Raw socket packet processing



2.4.2.1 Raw socket processing for UDP sessions

When the local host receives a UDP packet from a remote host, it queues the packet and sends it over the serial link. The local host remembers the UDP session while there is still data to send from the serial link. If further packets are received for the same session, they are queued behind the already queued packet. After all the queued data has been sent over the serial link, the session is removed from the system. An associated UDP remote host for the serial link must be configured to have serial data sent back to the remote host from the serial port.

When a packet is received from the serial link based on end-of-packet (EOP) requirements, the data is copied and sent in a UDP packet to each configured remote host.

2.4.2.2 Raw socket processing for TCP sessions

An open TCP session from a remote host to a raw socket's local host is kept open until either the remote host terminates the session or the TCP inactivity timer expires. When a TCP session is open, all packets received from the remote host are queued for the raw socket serial link and sent over the serial link until no packets remain in the queue. If multiple sessions are open toward the local host, and each is receiving data, then each session's data is queued and then sent over the serial link in round-robin fashion for each session until no packets remain. When a packet is received over the serial link, it is copied to each open TCP session and transmitted to the remote host.

2.4.3 Raw socket squelch functionality

A condition may occur where the end device connected to the serial port continues to send out a continuous stream of data after the normal response period has expired. This can prevent the far-end remote host or master equipment from receiving data from other end devices in the network. To resolve this condition, the **squelch** command can be used on the raw socket at the port level (it is disabled by default). This stops the socket from receiving any more data from the problematic device.

If the command is enabled, the node will monitor the serial port for a constant character stream. A configurable squelch delay period, using the **squelch-delay** command, is used to determine how long to measure the constant character stream before initiating the squelch function. If the squelch function is initiated, the port is considered locked up and an alarm is raised indicating the lock-up and that the squelching function has been triggered.

The serial port can be forced out of squelch and put back to normal, either manually using the **squelch-reset** command or automatically using the **unsquelch-delay** command. The **unsquelch-delay** command defines the time to wait after squelch is initiated before it is removed.

3 Cellular MDA and ports

3.1 In this chapter

This chapter describes the cellular MDA and cellular ports. Topics include:

- Overview
- Prerequisites and required configurations
- Cellular MDA management
- Cellular port management
- Firmware update
- Obtaining system time from the cellular interface
- Citizens Broadband Radio Service authorization
- Remote access to cellular diagnostics port

For more information about using the cellular MDA and ports for establishing IP/MPLS service, see the following topics in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*:

- PDN router interfaces
- Services over the cellular PDN interface
- Dedicated bearers

3.2 Overview

The cellular MDA supports 5G, 4G LTE, and 3G connectivity, depending on the radio module installed in the node. See the *SAR-Hm and SAR-Hmc Chassis Installation Guide* for information about the types of supported modules.

Each node supports a single cellular MDA. Each cellular MDA supports two cellular ports, one for each SIM that can be configured on the node. Each cellular port has its own PDN router interface. A PDN router interface is a network-facing interface that is used to route traffic to and from the node over a cellular network, providing WAN connectivity over the cellular port.

3.3 Prerequisites and required configurations

Before configuring the cellular MDA and cellular ports, the following prerequisites must be considered.

- Depending on the radio module variant selected, appropriate cellular network coverage is required where the node is to be physically installed.
- The operator must subscribe to a service plan with a wireless service provider. For private cellular networks, the operator must procure a SIM that allows the node to connect to the private cellular

network being deployed. If dual SIM functionality is required, the operator must subscribe to a second service plan with another wireless provider and procure a second SIM.

- The radio firmware shipped with the node is a generic firmware version. Some service providers require a specific radio firmware version to run on the node, depending on the radio variant used on the node and the wireless service provider being connected to; in this case, the firmware on the node must be updated to the correct version. See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for details about updating the radio firmware to the correct version. If dual SIM functionality is enabled, the firmware associated with the second wireless service provider must be updated for the associated SIM.
- The SIM or SIMs must be physically installed before powering up the router and configuring the cellular MDA and cellular ports.
- For a typical GSM profile, and if required by the service plan, the following information must be obtained from the service provider: Access Point Name (APN), username, and password. For dual SIM deployments, obtain the GSM profile information for each SIM.

When the prerequisites have been met, the following configurations are required.

- A cellular port interface must be configured for each installed SIM.
- The required SIMs must be configured under the cellular MDA.

The following CLI syntax shows an example of the required cellular MDA and cellular port parameters:

```
*A:Dut# configure card 1 mda 1 cellular sim 1
*A:Dut>config>card>mda>cellular>sim# pin
Enter PIN: xxxx
Re-enter PIN: xxxx
*A:Dut>config>>card>mda>cellular>sim# exit
*A:Dut# configure port 1/1/1 cellular pdn
*A:Dut>config>port>cellular>pdn# pdn-profile 1
*A:Dut>config>port>cellular>pdn# exit
*A:Dut#
```

- A cellular system PDN profile must be created and the corresponding APN, GSM parameters (such as username, password, and authentication), and protocol must be configured for each installed SIM. For an example of the CLI syntax required for the PDN profile configuration, see PDN profile.
- A PDN router interface must be created for each cellular port to enable services over the cellular port; for information, see "PDN router interfaces" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

3.4 Cellular MDA management

Cellular MDA management activities include the following:

- setting SIM control parameters such as specifying the active SIM and the preferred SIM to use after a node reset
- specifying the SIM PIN value needed to operate each SIM if SIM security is enabled
- specifying failover criteria on each SIM to determine when to automatically switch to the backup SIM when the system is operating in dual SIM mode
- configuring optional recovery criteria for cellular ports or BGP sessions that are operationally down, and an associated interval when it is desirable to perform a node reset because of a potential cellular lockup as a result of a modem failure

- configuring the maximum transmit power on the 7705 SAR-Hmc for applications that require changes to maximum transmit power. See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for information about applications that require a change to the maximum transmit power.

3.4.1 SIM installation and configuration

Up to two valid SIMs must be procured before configuring the cellular MDA or cellular ports. The SIMs must be inserted into the proper SIM slots before the node is powered up. SIMs cannot be installed when the node is powered on. To run the Automatic Discovery Protocol (ADP-Hm) on the node, a SIM must be inserted into slot 1; otherwise, ADP-Hm will not function. For more information about ADP-Hm, see "Basic system configuration" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

For information about dual SIM operation, see Dual SIM deployment.

3.4.1.1 SIM security and security commands

A SIM that is installed on the node can be secured using a personal identification number (PIN). The PIN is a 4- to 8-digit code that is used to control access to information stored on the SIM. The PIN is stored on the SIM and is used to lock the SIM, unlock the SIM, or change the PIN value.

To secure a node, the PIN needs to be set and the SIM must be locked using the PIN. When locked, the SIM cannot be used to access the cellular network unless the PIN is present in the configuration file of the node operating the SIM. If the locked SIM is inserted into another node that does not have the correct PIN configured for the SIM, the SIM will not allow access to the cellular network. If the number of attempts made to access the cellular network using an incorrect PIN exceeds the number of attempts allowed by the SIM, then the SIM will become blocked and will not allow any further attempts to gain access the cellular network.

When a SIM is procured from a carrier, the PIN is either not set or sometimes set to a default value such as 0000 or 1111. When a locked SIM is first installed in the node, the operator must enter the default PIN in the node system configuration twice. When stored in the system configuration, the PIN provides access to the locked SIM, both to read information from the SIM and to grant access to the cellular network.

The PIN can be stored in the system configuration in encrypted form to keep the PIN value secret.

Caution:

- Avoid entering an invalid PIN in the system configuration. If an invalid PIN is saved to the system configuration file, the system will attempt to enter that PIN on the SIM each time the system reboots. This will eventually exhaust the number of available PIN retries for the SIM and make the SIM inoperative until it is unblocked with the personal unblocking key (PUK).
- In addition, if multiple attempts are made to either lock or unlock the SIM using an incorrect PIN, the SIM becomes blocked. In both cases, the SIM must be unblocked using the PUK.

The number of allowed attempts to access a SIM depends on the SIM. The "PIN retries left" field under the SIM Card heading in the **show>port** CLI output indicates the number of attempts left before the SIM is blocked and must be unblocked to establish cellular connections.

If the SIM becomes blocked, the operator must enter the personal unblocking key (PUK) in the CLI to unblock the SIM and reset the PIN. The PUK is stored on the SIM and must be acquired from the service provider or administrator.

Many carriers provide unlocked SIMs. If an unlocked SIM is installed in a node, the operator does not need to know the PIN or configure the PIN in order for a cellular port to become operational. For example, during the ADP-Hm process, setting the PIN before attempting to connect to the network is not required.

The default PIN can be changed on the SIM using the **tools>perform>mda>cellular>sim>change-pin** command. If the default PIN is changed on the SIM, the system configuration must be updated with the new PIN value using the **config>card>mda>cellular>sim>pin** command.

The commands described below are available for SIM security. All of the SIM security commands are in the **tools>perform>mda>cellular>sim** context.

Note: The SIM specified in the **tools>perform>mda>cellular>sim** commands must be the currently active SIM. If the SIM is not the currently active SIM, the commands fail.

- **lock-sim**—this command locks the SIM and enables the PIN verification function on the SIM. A locked SIM verifies the PIN stored in the system configuration for operation. To lock the SIM, the operator must enter the current PIN.
- **unlock-sim**—this command unlocks the SIM and disables the PIN verification function on the SIM. To unlock the SIM, the operator must enter the current PIN.
- **unblock-sim**—this command unblocks a SIM that is currently blocked because too many attempts were made to access the SIM with an incorrect PIN. To unblock the SIM, the operator must enter the PUK for the SIM and then enter a new PIN twice. The lock/unlock state of the SIM does not change when it becomes unblocked.
- **change-pin**—this command allows the operator to change the PIN value on the SIM. The operator must enter the existing PIN and then enter the new PIN twice correctly to change the PIN. The command is shown in the output below.

```
A:Dut-A# tools perform mda 1/1 cellular sim 1 change-pin
Enter current PIN:
Enter new PIN:
Re-enter new PIN:
```

WARNING:

- When an operator successfully locks a SIM, unblocks a SIM, or changes a SIM PIN, the system updates the PIN value in the system configuration. However, the system does not automatically save the system configuration containing the new PIN. The operator must perform an **admin>save** command immediately after changing the PIN in order to save the new PIN in the system configuration file and avoid potential service interruptions such as the node becoming unreachable.
- If the SIM becomes blocked when setting the PIN remotely using in-band management over a cellular port, the node will be unreachable. Physical access to the node will be required to unblock the SIM.

Note: Changes can only be made to the currently active SIM. If changes to the backup SIM in a dual SIM deployment are required, then a SIM switchover must be performed in order to modify the backup. Before switching over to the backup SIM, the operator must ensure that it is operational and not locked. The operator should configure the **down-recovery-interval** command and ensure that one of the SIMs is operational in order to reduce the risk of the node becoming unreachable.

3.4.1.2 Cellular band selection

In some deployments, it may be necessary to control which spectrum the cellular interface uses when it is searching for a cellular network to connect to. This can be achieved by configuring a list of cellular bands for each SIM using the command **configure>card>mda>cellular>sim>band-list**. See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for information about the platforms that support cellular band selection.

The operator creates the band list by specifying the bands that are supported on the MDA. For node variants that support LTE on the ceullular MDA, a total of four bands can be configured in the list: up to three LTE bands and one 3G band.

In a dual SIM deployment, a band list can be configured on one or both SIMs.

A SIM switchover causes the MDA to reset. If a band list is configured on the newly active SIM, the reset enables this band list. If the newly active SIM is not configured with a band list, the node uses the bands that are supported by the firmware.

If the list contains bands that are not supported by the firmware for a specific carrier, the node will use only the bands that are supported by the firmware. For example, if the firmware supports bands B2, B5, B7, B13, and B66 but the **band-list** is configured with bands B2, B42, B48, and B71, the node will only allow B2 to be configured on the MDA because it is the only band on the list that is supported by the firmware.

If none of the bands on the list are supported by the firmware, the node considers the band list to be misconfigured and ignores it. The node reverts to enabling all the bands supported by the firmware. Enabling all the supported bands ensures that the node can connect to the network if further actions are required to manage the node.

Note: When a band list changes, the PDN interface goes down and attempts to reattach to the network. This may result in a brief data outage.

The output from the **show mda 1/1** command provides information about the operational bands in use and whether the band list was applied or ignored. The command output also displays whether 3G is enabled or disabled.

3.4.1.3 RSSI threshold alarm

The Received Signal Strength Indicator (RSSI) of the cellular interface can be monitored to detect weak signals on the interface. Monitoring signal strength can be useful for determining the stability of the carrier or private cellular network and whether to log (generate) an RSSI threshold alarm log event or generate an alarm log event and switch carriers, either manually or by automatically switching SIMs in a dual SIM deployment.

The **rssi-threshold** command is used to set the level at which the received signal is considered weak enough to trigger an alarm log event. If the RSSI falls below the configured threshold, a tmnxCellularRssiAlarm log event is generated. As well, if the threshold is configured as a failover criterion, a SIM switchover occurs in a dual SIM deployment.

Note: When a band list changes, the PDN interface goes down and attempts to reattach to the network. This may result in a brief data outage.

The node polls the radio signal strength approximately once per second. If the RSSI falls below the configured **rssi-threshold**, a timer starts. If the RSSI stays below the threshold for the time specified with the **rssi-alarm-wait-time** command, the tmnxCellularRssiAlarm log event is generated. This

log event is generated only once even if the RSSI remains below the threshold indefinitely. After the tmnxCellularRssiAlarm log event is generated, if the RSSI level rises to the configured **rssi-threshold** value or higher and remains at that level for the duration of the **rssi-alarm-wait-time**, the tmnxCellularRssiAlarmClear log event is generated. The operator can monitor the logging frequency to determine whether to manually switch carriers.

The RSSI threshold can be set as a failover criterion in a dual SIM deployment. When the **rssi-threshold** option is set in the **failover-criteria** command, if the RSSI signal level falls below the configured RSSI threshold for the configured **failure-duration** time, the node performs an automatic switchover from the currently active SIM to the other SIM. See Criteria for automatic failover for information about using RSSI as a failover criterion for dual SIMs.

3.4.2 Down-recovery timer and criteria

A down-recovery timer can be set so that if the cellular MDA fails to establish cellular service or if BGP cannot be established on any interface configured in the system, the node will reboot. The **down-recovery-interval** is configured at the cellular MDA level and is not specific to a particular SIM. The timer can be set when there is a single SIM or two SIMs installed in the node.

The operator can specify the criteria that will cause the node to reboot by configuring the **down-recovery-criteria** command. The **down-recovery-criteria** can be set to **port** or **bgp**. When set to **port**, all cellular ports configured on the system are monitored during the down-recovery interval. When set to **bgp**, all BGP sessions configured on the node are monitored during the down-recovery interval. Both options can be specified concurrently, and the node will use either the cellular port state or BGP session state to declare the operational state of the node as down.

When set, the **down-recovery-interval** specifies the length of time that the configured **down-recovery-criteria** are monitored from the moment when either the ports or the BGP sessions are declared operationally down. If the interval is exceeded without any port or BGP sessions going operationally up, the node reboots so that the preferred SIM can try to connect to a cellular network again. As soon as any port or BGP sessions is operationally up, the down-recovery timer stops.

The **down-recovery-interval** is measured in minutes, with a range of 1 to 240 minutes. Sixty seconds before the timer expires, the node will issue a log event stating that the node will reboot in 60 seconds if the down-recovery condition (based on the configured criteria) is not resolved. This 60-second warning interval can be used for further debugging and diagnostics before the node resets.

3.4.3 Dual SIM deployment

The node supports dual SIM deployment for users who require a redundancy option using two wireless carriers.

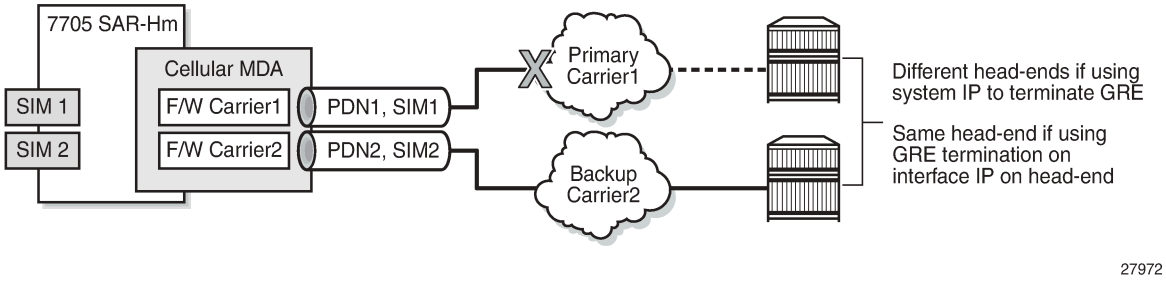
With dual SIM deployment, two SIMs are installed in the node, one from each carrier. Only one SIM is active at a time to establish a cellular service WAN connection. The operator choses which SIM is primary and which is secondary or manually selects which SIM to keep active.

Configurable criteria give the operator some control over when it is appropriate for the system to perform a SIM switchover. For example, the BGP operational state associated with the cellular port can be used as a criterion for determining when a SIM switchover should occur. If the BGP operational state is down for a specified interval, a SIM switchover occurs. See Criteria for automatic failover for more information.

Caution:
A SIM switchover is service-affecting. Operators should perform a SIM switchover only when necessary, as overly frequent switchovers will impact service operation.

Figure 3: Dual SIM operation shows dual SIM operation on a 7705 SAR-Hm.

Figure 3: Dual SIM operation



For information about IP/MPLS services when dual SIM functionality is enabled, see the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

3.4.3.1 Enabling dual SIM operation

To enable dual SIM operation on the node, operators must perform the following tasks.

- Procure two SIMs, each for a different cellular network.
- If ADP-Hm is required, insert the SIM needed to operate with ADP-Hm into SIM slot 1. For more information about ADP-Hm, see "Basic system configuration" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.
- Ensure that each SIM is associated with a unique packet data network (PDN) by configuring a PDN profile and a PDN router interface that will be assigned a unique IP address during the PDN attach process. The PDN profiles and PDN router interfaces must be configured beforehand.
- Choose whether the SIMs will be switched manually or use automatic failover. If automatic failover is chosen, the operator must determine the criteria for failover. See Criteria for automatic failover for information.

3.4.3.2 Active SIM selection

After the two SIMs are installed in the node, the operator chooses which SIM will be active by configuring the **active-sim** command under the cellular MDA. This command can be configured either with a specific SIM (**1** or **2**) or with the **auto** parameter. The default is **1**. The configuration of this command determines whether the SIMs are switched manually or use automatic failover.

3.4.3.2.1 Manual selection

The operator can manually select the active SIM by configuring a specific SIM as active, either **1** or **2**. This configuration makes the selected SIM permanently active.

The active SIM can be manually switched by changing the **active-sim** setting from **1** to **2** or from **2** to **1**.

Caution:
Changing the active SIM from 1 to 2 or from 2 to 1 is service-affecting. The recovery time after making this change can range from a few seconds to up to a few minutes.

When the system powers up or reboots, it uses the **active-sim** setting to determine which SIM is the active SIM. If the operator configures the **active-sim** as **1** but there is no physical SIM in the associated SIM slot, the cellular port remains operationally down. The operator must either install the SIM in the appropriate slot or change the configuration in order to bring the service up.

3.4.3.2.2 Automatic failover

An automatic failover occurs when activity switches from one SIM to the other.

Automatic failover is enabled in a dual SIM deployment when the **active-sim** command is set to **auto**. In this case, the operator must select the SIM to use as the primary SIM by setting the **preferred-sim** value. The node uses the **preferred-sim** setting to determine which SIM to use for a cellular port after a system reset.

If the operator changes the **active-sim** value from **auto** to **1** or from **auto** to **2** and the active SIM is the same as the new configuration, there is no change to service of the active SIM.

Caution:
Changing the **active-sim** setting so that the newly active SIM is different from the currently active SIM is service-affecting. The recovery time after making this change could range from a few seconds to up to a few minutes.

If the operator changes the active SIM from **1** to **auto** or from **2** to **auto**, there is no service outage. The system keeps the currently active SIM up and does not perform any switchover.

When **active-sim** is set to **auto**, the operator can use the **tools>perform>mda>cellular>force-sim-switch** command to manually force a SIM switch.

The **auto** parameter can be set if there is only one SIM installed in the system; however, the system keeps the currently active SIM up and does not perform any switchover.

3.4.3.3 Criteria for automatic failover

When the **active-sim** command is set to **auto**, the operator can configure the parameters that will cause an automatic failover to occur. The parameters that serve as criteria for automatic failover are:

- the cellular port operational state
- the operational state of all BGP sessions configured on the node
- the RSSI value

These parameters are configured per SIM and can be different for each SIM. As well, any combination of parameters can be configured for each SIM.

An automatic failover occurs when the conditions are met for any of the configured parameters on the currently active SIM.

Note: Automatic failover between SIMs can continue indefinitely until either the recovery timer expires, which will reboot the entire system and bring up a cellular port based on the preferred

SIM, or the operator manually intervenes to halt automatic failover by configuring a specific SIM as the active SIM.

Note: When the operational state of BGP sessions is the failover criterion for a specified SIM and established BGP sessions are operationally up on a WLAN or Ethernet interface, the node will not perform a SIM switchover until all BGP sessions are down. When BGP is required to monitor the state of the cellular interface, ensure that only the cellular interface can establish BGP sessions. When BGP sessions are required over WLAN or Ethernet, use the operational state of the port as the failover criterion in order to ensure automatic SIM failover.

3.4.3.3.1 Cellular port operational state

The cellular port operational state can be specified as a failover criterion for the currently active SIM. The operational state of cellular port 1/1/1 is used as the failover criterion for SIM 1 and the operational state of cellular port 1/1/2 is used as the failover criterion for SIM 2.

When the cellular port operational state criterion is specified, the system monitors the operational state of the PDN. If the PDN is operationally down for a specified **failure-duration**, the system performs a SIM failover and attempts to establish cellular service using the other SIM. See Failure duration for more information.

3.4.3.3.2 BGP sessions operational state

When the BGP operational state criterion is specified, the system monitors the operational state of all BGP sessions configured on the node. If all the BGP sessions are operationally down for a specified **failure-duration**, the system performs a SIM failover and attempts to establish cellular service using the other SIM. See Failure duration for more information.

3.4.3.3.3 RSSI threshold value

When the RSSI threshold criterion is specified, the system monitors the RSSI signal level of the SIM. If the RSSI level falls below the value set with the **rssi-threshold** command for a specified **failure-duration**, the system performs a SIM failover and attempts to establish cellular service using the other SIM. See Failure duration for more information.

3.4.3.3.4 Failure duration

When the **active-sim** command is set to **auto** and at least one failure criterion is configured, the system uses the length of time configured for the **failure-duration** to determine when to perform an automatic failover from one SIM to the other.

The **failure-duration** value is configured per SIM but it applies to all failure criteria. It is not possible to configure one failure duration value for one criterion and another failure duration value for another criterion.

The default value is 5 minutes. The valid range is from 1 minute to 60 minutes.

Note: It is recommended that the **failure-duration** be set to a high value so that the system does not perform frequent switches between SIMs.

3.5 Cellular port management

A cellular port enables a specific cellular service for an associated SIM. Each cellular port is managed separately per SIM and per PDN.

Cellular port 1/1/1 is associated with SIM 1 and cellular port 1/1/2 is associated with SIM 2.

A cellular port can be shut down by using the **port>shutdown** command. When a cellular port is shut down, the cellular service for that port is disabled. To enable cellular service for the port, use the **port>no shutdown** command. See Common configuration commands for more information about the **shutdown** command.

WARNING:
Use caution when executing the **port>shutdown** command on a cellular port. Shutting down a cellular port when it is the only means of communication to a remote node over a wireless network may cause permanent loss of connectivity to the node.

3.5.1 Cellular port and its PDN

The node provides a single PDN connection for each cellular port. A cellular port must have an associated PDN router interface in order to allow routed traffic and services over the PDN connection and over the cellular network. For more information about the PDN router interface, see "PDN router interfaces" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

The node supports the configuration of an access point name (APN) as part of a PDN profile in order to establish the PDN connection. In many cases, the default PDN profile is sufficient to establish a connection. For example, often the only configuration that is necessary to establish a connection is to enable the port using the **config>port** *port-id* **no shutdown** command. However, some carriers may require the user to configure a specific APN before allowing a connection to be established. In those cases, the user must configure a PDN profile and configure the cellular port to use that PDN profile. See PDN profile for more information.

3.5.1.1 PDN profile

The node uses PDN profiles to establish PDN connections over a cellular port. When the default PDN profile is not sufficient to establish connections, a PDN profile must be created. Manually created PDN profiles contain additional cellular network access configuration items that are not stored on the SIM but that are required in order to establish a PDN connection. PDN profiles can be created, modified, and deleted.

A PDN profile is referenced using a PDN profile ID. When a PDN profile is created at the system level and then configured on a cellular port, it cannot be modified or deleted until it is removed from the cellular port.

PDN profiles are necessary so that CLI or SNMP changes can be made to cellular ports without first having to shut down the ports. For example, when changing the APN information for a cellular port, another PDN profile can be configured with the changed information and assigned to the cellular port. This change will cause the cellular port to connect to the cellular network using the new PDN profile information immediately.

The following items can be configured as part of a PDN profile:

- APN—the Access Point Name provided by the service provider to use for the cellular service

- authentication—the type of authentication to use for establishing the connection, either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP)
- description—a description for the PDN profile
- password—a password for the PAP or CHAP authentication
- protocol—the protocol for the associated PDN interface, either IPv4 or IPv6
- username—a username for the PAP or CHAP authentication

The following CLI syntax shows an example of how to configure a PDN profile.

```
*A:Dut# config>system>cellular# pdn-profile 1
*A:Dut>config>system>cellular>pdn-prof# apn apn1
*A:Dut>config>system>cellular>pdn-prof# authentication pap
*A:Dut>config>system>cellular>pdn-prof# description "PDNprofile1"
*A:Dut>config>system>cellular>pdn-prof# no password
*A:Dut>config>system>cellular>pdn-prof# protocol ipv6
*A:Dut>config>system>cellular>pdn-prof# username waldowaldo
*A:Dut>config>system>cellular>pdn-prof# exit
*A:Dut>config>system>cellular# exit
*A:Du>config>system# exit
*A:Dut>config# exit
*A:Dut#
```

For more information, see Cellular PDN profile configuration commands .

3.5.1.1.1 Default PDN profile

Table 4: Default PDN profile values lists the settings for the default PDN profile. The default PDN profile is always used when installing a new SIM and running the ADP-Hm process. It can also be used to establish cellular connections that do not require PDN profile configurations. The default PDN profile cannot be modified by the user.

Table 4: Default PDN profile values

Profile parameter	Value
APN	Blank
Authentication	None
Username	Blank
Password	Blank
Protocol	IPv4

3.5.1.1.2 Assigning a PDN profile to a cellular port

To assign a PDN profile to a cellular port, configure the PDN profile under the **config>port>cellular>pdn** CLI context.

The following CLI syntax shows an example of how to assign a PDN profile to a cellular port.

```
*A:Dut# configure port 1/1/1 cellular pdn
*A:Dut>config>port>cellular>pdn# pdn-profile 1
*A:Dut>config>port>cellular>pdn# exit
*A:Dut#
```

For more information, see Cellular MDA and cellular port configuration commands .

3.6 Firmware update

The **update-firmware** command is available to update firmware on the node. The command is used to preload the correct firmware associated with each SIM's wireless service provider onto the cellular modem for those node variants that require firmware updates to operate in that service provider network.

For some node variants, the firmware is updated for each SIM. For other node variants, the firmware is updated for the radio and the SIMs use the same version. There are two forms of the **update-firmware** command to address both cases:

- **tools>perform>mda 1/1>cellular>update-firmware** *firmware-file* **sim 1** | **2**

  This form of the command is used for node variants that require the firmware to be updated for each SIM. In a dual SIM deployment, the command must be run twice, once for each SIM. For example, a node could have an ATT SIM installed in SIM slot 1 and a VZW SIM installed in SIM slot 2. The command is used to ensure that ATT-supported firmware is loaded for SIM 1 operation and that VZW-supported firmware is loaded for SIM 2 operation. Depending on which SIM is active based on the **active-sim** command, the corresponding radio firmware for that carrier SIM is used by the radio. If an automatic failover occurs, the associated firmware for the new SIM is used by the radio to establish service using the new SIM.

- **tools>perform>mda 1/1>cellular update-firmware** *firmware-file*

  This form of the command is used for node variants that do not support firmware updates per SIM. When executed, the command updates the firmware for the radio, and in a dual SIM deployment, both SIMs use the same version of the firmware.

For more information about using the command, see the update-firmware command description in the Interface command reference chapter.

By default, the firmware that is shipped with the node is used for both SIM 1 and SIM 2 when either SIM is active and no other firmware is specified for that SIM. See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for information about the node variants that require firmware updates to operate in a particular service provider network and for information about the firmware that must be used when operating on wireless carriers that require specific firmware.

3.7 Obtaining system time from the cellular interface

The cellular interface can obtain the system time when the **config>port>cellular>sync-system-time** command is enabled. When the command is enabled and the corresponding PDN interface goes up, system time is retrieved and set on the system.

Note: If NTP or SNTP is configured when the **sync-system-time** command is enabled, there is no time source precedence and either process can update the system time at its own discretion.

Do not enable NTP or SNTP when the **sync-system-time** command is enabled unless NTP (or SNTP) and the cellular interface are using the same time source.

The cellular interface and the GNSS receiver can be configured concurrently to obtain the system time. When the **sync-system-time** command is enabled concurrently on the cellular interface and on the GNSS receiver, the GNSS receiver takes priority when it establishes a lock.

When the **sync-system-time** command is enabled, the system time cannot be set manually.

The **sync-system-time** command works in conjunction with the following commands:

- **config>system>time>dst-zone**
- **config>system>time>prefer-local-time**
- **config>system>time>zone**

For information about the **dst-zone**, **prefer-local-time**, and **zone** commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

3.8 Citizens Broadband Radio Service authorization

The cellular interface on the 7705 SAR-Hmc NA variant (3HE12472AA), the 7705 SAR-Hmc NA variant 2 (3HE12473AA), the 7705 SAR-Hmc World variant (3HE12478AA), and the 7705 SAR-Hmc 5G variant (3HE12479AA) supports the Citizens Broadband Radio Service (CBRS) B48/n48 spectrum. When operating in the CBRS spectrum, the 7705 SAR-Hmc is classified as either an end-user device (EUD) or a Citizens Broadband Service Radio Device (CBSD), depending on the maximum effective isotropic radiated power (EIRP) of the device.

Table 5: Maximum EIRP and PSD lists the maximum EIRP levels for each device type, as defined by FCC 47 CFR Part 96.41 – General radio requirements.

Note: The operator must calculate the maximum EIRP or Power Spectral Density (PSD) in order to choose the correct device, either EUD, Category A CBSD, or Category B CBSD.

Table 5: Maximum EIRP and PSD

Device	Maximum EIRP (dBm/10 MHz)	Maximum PSD (dBm/MHz)
EUD	23	n/a
Category A CBSD	30	20
Category B CBSD	47	37

See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for information about operating the node as an EUD.

To operate the node as a CBSD, the maximum EIRP that identifies the node as a Category A or Category B device must be determined and planned beforehand. The CBSD maximum EIRP of the 7705 SAR-Hmc is calculated using the **antenna-gain** and **max-tx-power** values configured in the CLI and must be within the range expected for the category of the CBSD and within the range that is expected by the Spectrum Access System (SAS). Operators can use these parameters to adjust the maximum EIRP to meet the CBSD category requirements expected for a particular site location.

The maximum transmit conducted power that the 7705 SAR-Hmc can operate is 23 dBm. If a detached antenna is used, the antenna gain can be equally increased to compensate for cable losses. The EIRP calculations are:

EIRP = PSD + 10log (channel width)

or

EIRP = Tx conducted power + antenna gain - cable losses

For all CBSDs, before a network operator can enable the node as a CBSD, a Certified Professional Installer (CPI) must register each device with the SAS by populating the SAS with the following information:

- geographic location
- antenna height above ground level (AGL), in meters
- CBSD class, either Category A or B
- requested authorization status, either priority access license (PAL) or general authorized access (GAA)
- FCC ID
  - for the 7705 SAR-Hmc NA variant (3HE12472AA): AS57705SARHMC-1
  - for the 7705 SAR-Hmc NA variant 2 (3HE12473AA): AS57705SARHMC-2B
  - for the 7705 SAR-Hmc World variant (3HE12478AA): AS57705SARHMC-3
  - for the 7705 SAR-Hmc 5G variant (3HE12479AA): AS5770SARHMC-4
- call sign (for PALs only)
- user contact information
- air interference technology
- serial number
- sensing capability, if supported

Note: Observe the following height restriction for Category A CBSDs, as defined by FCC 47 CFR Part 96.43 — Additional requirements for category A CBSDs:
"Category A CBSDs shall not be deployed or operated outdoors with antennas exceeding 6 meters height above average terrain. CBSDs deployed or operated outdoors with antennas exceeding 6 meters height above average terrain will be classified as, and subject to, the operational requirements of Category B CBSDs."

Note: Observe the following installation requirements as defined by FCC 47 CFR Part 96.45 – Additional requirements for category B CBSDs:

- "(a) Category B CBSDs must be professionally installed."
- "(c) Category B CBSDs are limited to outdoor operations."

For Category B CBSDs, the SAS must be populated with more information for each site, as follows:

- antenna gain
- antenna beamwidth
- antenna azimuth
- antenna downtilt angle

For all CBSDs, before an operator can communicate with the SAS or Domain Proxy (DP) over a secure TLS connection, the node must be configured with X.509 certificates for the node and the SAS/DP. The operator must acquire an INSTA Certificate Manager (ICM) account and request CBSD certificates from the ICM. The CBSD certificate and Certificate Authority (CA) certificates in the certificate chain must be requested and downloaded from the ICM portal. The SAS/DP CA certificates must be retrieved from the SAS provider or DP. See Authentication procedure for TLS connection to the SAS/DP for details about configuring the CBSD and SAS/DP certificates on the CBSD.

The CBSD must complete the following network communication procedural steps to receive a grant and be authorized by the SAS to allow regular SR OS traffic on the cellular port:

- establish a secure TLS session with the SAS
- complete the CBSD registration procedures with the SAS/DP
- complete the CBSD grant procedure and CBSD heartbeat procedure with the SAS/DP

After the operator has successfully registered the node information with the SAS and acquired and configured the CBSD and SAS/DP certificates, the node must be enabled to communicate with the SAS over the cellular port that is installed with a SIM that can connect to the CBRS spectrum.

The cellular port cannot be enabled until all the CBSD parameters have been configured on the cellular port in the **config>port>cellular>cbsd-authorization** CLI context and the CBSD authorization procedure is enabled on the cellular port with the **config>port>cellular>cbsd-authorization>no shutdown** command. When the CBSD authorization parameters are configured and the authorization procedure is enabled, the cellular port can be enabled with the **config>port>1/1/1|2>no shutdown** command.

After the **cbsd-authorization** parameters are configured, when the CBSD authorization procedure is enabled using the **no shutdown** command and the PDN router interface is enabled, the system creates a dynamic filter that allows only SAS control traffic. See SAS CBSD registration with Network Group Encryption enabled for information about permitted traffic.

When CBSD authorization is enabled on the cellular port and the cellular port is enabled, the CBSD authorization procedure begins. The CBSD first establishes an HTTPS (HTTP over TLS) session between itself and the SAS. The CBSD signaling procedure is sent over the HTTPS session and is used to authorize the CBSD. When the CBSD authorization procedure is successful, regular SR OS traffic can use the CBRS spectrum.

The CBSD grant procedure and the CBSD heartbeat procedure must be completed successfully before regular router traffic is allowed on the cellular port. When the SAS authorizes the node to transmit, the dynamic filter is removed from the active PDN router interface and all CPM management and SR OS session traffic is enabled. The NSP NFM-P can discover and manage the node, BGP sessions can be established to head-end nodes, and GRE-MPLS-based services can be established.

3.8.1 Authentication procedure for TLS connection to the SAS/DP

When acting as a CBSD, the 7705 SAR-Hmc must complete TLS authentication to communicate with the SAS/DP server. The 7705 SAR-Hmc supports TLS 1.2. For more information about TLS, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

A secure TLS connection to a SAS/DP requires X.509 certificates configured on the CBSD. The operator must acquire an ICM account to request and download device-level CBSD certificates. For each CBSD that requires a certificate, the operator can upload the FCC ID and serial number to the ICM portal, submit the request for the certificates, and download the certificate .pem files.

In addition, the operator must download the following CA certificate files from the ICM portal:

- the INSTA root CA certificate (included with the device-level CBSD certificate)
- the INSTA manufacturer CA for the CBSD (included with the device-level CBSD certificate)
- the INSTA root CA's CRL file URL
- the INSTA manufacturer CA's CRL file URL
- the SAS/DP root CA certificate (contact the SAS/DP provider for this certificate)
- the SAS/DP intermediary certificate (contact the SAS/DP provider for this certificate)
- the SAS/DP root CA's CRL file URL (contact the SAS/DP provider for this CRL file URL)
- the SAS/DP intermediary CA's CRL file URL (contact the SAS/DP provider for this CRL file URL)

The operator must FTP the CA certificate files listed above into the temporary directory on the CBSD and then use the **admin>certificate>import** CLI command to import each CA certificate.

The following examples show the **admin>certificate>import** command for each CA certificate:

```
*A:SARHmc# admin certificate import type cert format pem input
cf3:/newcerts/WInnForum_RSA_Root_CA.pem output WInnForum_RSA_Root_CA.cer

*A:SARHmc# admin certificate import type cert format pem input
cf3:/newcerts/WInnForum_RSA_CBSD_Mfr_CA.pem output WInnForum_RSA_CBSD_Mfr_CA.cer

*A:SARHmc# admin certificate import type cert format pem input
cf3:/newcerts/RSA_Root_CA_CA0001.pem output RSA_Root_CA_CA0001.cer

*A:SARHmc# admin certificate import type cert format pem input
cf3:/newcerts/RSA_SAS_Provider_CA_0002.pem output RSA_SAS_Provider_CA_0002.cer
```

The operator must FTP each CRL file for each CA certificate into the temporary directory on the CBSD and then import them using the **admin>certificate>import** CLI command for each file.

The following examples show the **admin>certificate>import** command for each CRL file:

```
*A:SARHmc# admin certificate import type crl input
cf3:/newcerts/InstaCBRSRootCAv2.crl output InstaCBRSRootCAv2.crl format pem

*A:SARHmc# admin certificate import type crl input
cf3:/newcerts/InstaCBSDMfrCA0004.crl output InstaCBSDMfrCA0004.crl format pem

*A:SARHmc# admin certificate import type crl input
cf3:/newcerts/InstaCBRSRootCA_SAS.crl output InstaCBRSRootCA_SAS.crl format pem

*A:SARHmc# admin certificate import type crl input
cf3:/newcerts/InstaSASCA0002.der_CA_0002.crl output InstaSASCA0002.crl format pem
```

The CA periodically updates the CRL file, which must also be updated on the CBSD. The CBSD can be configured to automatically update the CRL for a CA with the **auto-crl-update** CLI command under the **ca-profile** context.

The following example shows a sample **auto-crl-update** configuration:

```
config
 system
        file-transmission-profile "http" create
            redirection 5
            router "management"
        exit
        security
            pki
```

```
                ca-profile "GTS_CA_1C3" create
                    cert-file "GTS_CA_1C3.cert"
                    crl-file "GTS_CA_1C3.crl"
                    auto-crl-update create
                        crl-urls
                            url-entry 1 create
                                file-transmission-profile "http"
                                url "http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl"
                            exit
                        exit
                        no shutdown
                    exit
                    no shutdown
                exit
            exit
        exit
```

For each CA certificate, a CA profile must be configured using the **config>system>security>pki>ca-profile** command. The CA certificate and CRL file are assigned to the CA profile with the **cert-file** and **crl-file** commands. The example below shows a sample CA profile configuration. The operator can use the **show>certificate>profile** CLI command to confirm that each **ca-profile** is operationally up.

The device-level CBSD certificate and key file must be imported into the CBSD. The operator must download the PKSC12 certificate file from the ICM portal, FTP the file into the temporary directory on the CBSD and then use the **admin>certificate>import** CLI command to import the certificate file and key file.

The following example shows the **admin>certificate>import** command for the CBSD certificate and key file:

```
*A:SARHmc# admin certificate import type cert input cf3:/newcerts/CBSD_NS213062783.p12 output
CBSD_NS213062783.cer format pkcs12 password PASSWORD

*A:SARHmc# admin certificate import type key input cf3:/newcerts/ CBSD_NS213062783.p12 output
CBSD_NS213062783.key format pkcs12 password PASSWORD
```

The configuration of CBSD authorization on the cellular interface includes a TLS client profile configuration. The TLS client profile uses the imported CBSD certificate and key file, the CA certificate profiles, and the SAS/DP root trust anchor to authenticate a TLS session between the CBSD and SAS/DP. The TLS client profile is configured using the **config>system>security>tls>client-tls- profile** CLI command on each CBSD.

The following example shows a sample configuration of CA profiles and the TLS client profile:

```
config
    system
        security
            pki
                ca-profile "WInnForumRootCA" create
                    cert-file "WInnForum_RSA_Root_CA.cer.cer"
                    crl-file "WInnForum_RSA_Root_CA.crl"
                    no shutdown
                exit
                ca-profile "WInnForumCBSDMfrCA" create
                    cert-file "WInnForum_RSA_CBSD_Mfr_CA.cer"
                    crl-file "WInnForum_RSA_CBSD_Mfr_CA.crl"
                    no shutdown
                exit
                ca-profile "RSARootCA0001" create
                    cert-file "RSA_Root_CA0001.cer"
                    crl-file "InstaCBRSRootCA.crl"
                    no shutdown
```

```
            exit
            ca-profile "RSASASProviderCA0002" create
                cert-file "RSA_SAS_Provider_CA_0002.cer"
                crl-file "InstaSASCA0002.crl"
                no shutdown
            exit
        tls
            cert-profile "cbsd_cert_profile" create
                entry 1 create
                    cert "CBSD_NS213062783.cer"
                    key " CBSD_NS213062783.key"
                    send-chain
                        ca-profile "WInnForumCBSDMfrCA"
                        ca-profile "WInnForumRootCA"
                    exit
                exit
                no shutdown
            exit
            trust-anchor-profile "sas_trust_anchor_profile" create
                trust-anchor "RSA_Root_CA0001"
            exit
            client-cipher-list "sas_client_cipher_list" create
                cipher 1 name tls-rsa-with-aes128-gcm-sha256
                cipher 2 name tls-rsa-with-aes256-gcm-sha384
            exit
            client-tls-profile "sas_client_tls_profile" create
                cert-profile "cbsd_cert_profile"
                cipher-list "sas_client_cipher_list"
                trust-anchor-profile "sas_trust_anchor_profile"
                no shutdown
            exit
```

The main components of the TLS configuration for the TLS client profile include:

- the **cert-profile** of the CBSD that specifies the certificate file, key file, and CA certificate chain
- the **trust-anchor-profile** that specifies the SAS/DP root CA trust anchor to the TLS session
- the **client-cipher-list** supported by the CBSD (the CBSD supports the following two ciphers, **tls-rsa-with-aes128-gcm-sha256**, and **tls-rsa-with-aes256-gcm-sha384**)
- the **client-tls-profile** details, which include the **cert-profile**, **cipher-list** and **trust-anchor-profile**

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* for more information about the CLI commands discussed above.

For mutual authentication, the CBSD authenticates the SAS/DP server and the SAS/DP server authenticates the CBSD. During the TLS message exchange, the CBSD authenticates the SAS server using the procedures in RFC 2818, *HTTP Over TLS*. Server certificate validation is performed according to RFC 5280, *Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile*. If the CBSD cannot authenticate the server, the TLS connection establishment procedure is aborted. The CBSD reattempts the TLS connection every 60 s.

The CBSD sends its client certificate to the SAS server, where the SAS performs the client authentication based on RFC 5280. If the SAS server fails to authenticate the CBSD, the TLS connection is terminated.

If a TLS connection is established with the SAS/DP, the registration process begins.

3.8.2 SAS CBSD registration with Network Group Encryption enabled

When router interface Network Group Encryption (NGE) is configured on a PDN router interface that is enabled for CBSD authorization, an exception filter must be configured to ensure that SAS control packets are permitted. The filter must allow the following:

- outbound and inbound clear text traffic to and from the primary SAS. The server IP address must be known.
- outbound and inbound clear text traffic to and from the secondary SAS server, if configured. The server IP address must be known.
- outbound and inbound clear text DNS queries and responses using the DNS server information learned in the PCO. The IP address returned from the DNS query must be known and statically configured for the primary and secondary SAS server addresses.
- outbound and inbound clear text SSH sessions

3.8.3 SAS discovery of the CBSD

In order for the SAS to discover the 7705 SAR-Hmc as a CBSD, the SAS administrator provides the CBSD operator with a URL to the primary SAS server and, optionally, a URL to a secondary SAS server. The URL is used in the **sas-server-primary** and **sas-server-secondary** CLI commands.

When the CBSD attaches to the wireless network, the DNS server IP address is used to resolve the SAS server URL. The CBSD attempts to establish an HTTPS session with the primary SAS server and, optionally, the secondary SAS server. If the attempt to establish a session with the primary SAS server fails, the node attempts a session with the secondary server if it is configured. If that attempt fails, the 7705 SAR-Hmc will wait 60 s before reattempting an HTTPS session with the primary server.

3.8.4 CBSD registration request parameters

After the CBSD is discovered by the SAS server and authentication is complete, the CBSD creates a secure session with the SAS and begins the registration procedure by sending a registration request.

The registration request includes the following parameters:

- configured CBSD user ID
- FCC ID:
  - for the 7705 SAR-Hmc NA variant (3HE12472AAAB): AS57705SARHMC-1
  - for the 7705 SAR-Hmc NA variant 2 (3HE12473AAAA): AS57705SARHMC-2B
  - for the 7705 SAR-Hmc World variant (3HE12478AA): AS57705SARHMC-3
  - for the 7705 SAR-Hmc 5G variant (3HE12479AA): AS5770SARHMC-4

  For all nodes, the FCC ID is used for CBRS B48 CBSD categories A and B.
- CBSD serial number
- configured CBSD category A or B

  The CBSD category supplied in the registration request and the category configured in the CLI must match.

- air interface — set to E-UTRA, as defined in the *Wireless Innovation Forum Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): WInnForum Recognized CBRS Air Interfaces and Measurements*, Document WINNF-17-SSC-0002

If the CBSD had any existing grants with the SAS before sending the registration request, they are deleted.

The SAS sends the CBSD a registration response that contains the following parameters:

- CBSD ID
- response — an indication of whether the registration request is approved

The CBSD ID is stored by the CBSD and used for all subsequent procedures with the SAS.

If the registration request fails for any reason, the CBSD retries the request every 60 seconds.

3.8.5 CBSD grant request parameters

Before it can initiate the grant procedure, the CBSD must be registered with the SAS.

The CBSD determines the operational parameters that will be used in the grant request and initiates the grant procedure by sending a grant request.

When the grant request is successful and the CBSD receives a valid heartbeat response, the CBSD is authorized to transmit using the parameters specified in the request.

The 7705 SAR-Hmc supports the following parameters in a grant request:

- CBSD ID
- operational parameters:
  - maximum EIRP — the CBSD maximum EIRP, determined by calculating the sum of the **antenna-gain** and **max-tx-power** values configured in the CLI. This total must be within the range expected by the SAS for the CBSD category.
  - operational frequency range — this information is retrieved from the cellular interface when the CBSD attaches to the network

The SAS sends the CBSD a grant response that contains the following parameters:

- CBSD ID
- grant ID
- grant expire time
- heartbeat interval
- response — an indication of whether the grant request is approved

If the grant ID is included in the grant response, the grant request succeeded. As soon as the grant request succeeds, the CBSD uses the heartbeat interval parameter to start the heartbeat procedure. The heartbeat is needed for the grant to be authorized.

The CBSD uses the grant expire time parameter to determine when the grant expires. The 7705 SAR-Hmc stores this value and sets a timer equal to the expiry time minus 1 h minus the current time. When this timer expires, there is 1 h left before the grant expires and the 7705 SAR-Hmc sets the grantRenew flag to attempt a grant renewal. If the grant is not renewed, the grant request process is restarted.

If the SAS determines an error in the grant request and does not include a grant ID parameter in its response, the grant request failed. The 7705 SAR-Hmc retries the request every 60 s.

3.8.6 CBSD heartbeat parameters

Upon receiving a successful grant response, the CBSD sends a heartbeat request at every heartbeat interval to indicate to the SAS server that the spectrum is required.

The 7705 SAR-Hmc supports the following parameters in the heartbeat request:

- CBSD ID
- grant ID
- grant renew — the node sets this parameter to TRUE when 1 h remains before either the grant timer expires or the heartbeat interval is longer than 30 min and two heartbeat requests can be sent before the grant timer expires. If either of these conditions cannot be met, this parameter is not included in the heartbeat request.
- operation state — the node sets this parameter to GRANTED when a heartbeat response has not yet been received for the grant and to AUTHORIZED when a successful heartbeat response has been received.

The SAS sends a heartbeat response that contains the following parameters:

- CBSD ID
- grant ID
- transmit expire time — the time that the CBSD must stop transmitting plus 60 s
- grant expire time — the time the grant expires. When included in the grant response, the 7705 SAR-Hmc uses this value as the new grant expire time.
- heartbeat interval — the maximum interval, in seconds, between two consecutive heartbeat requests. This value is used to set the heartbeat timer. If the value is changed by the SAS, the node uses the new value for this parameter.
- response — an indication of whether the heartbeat request is approved

If the transmit timer expires before the CBSD receives a heartbeat response, the CBSD stops transmitting for the grant within 60 s of the timer expiry.

A heartbeat request is sent at every heartbeat interval. The heartbeat interval timer is set when the CBSD receives a grant response or a heartbeat response that includes a defined heartbeat interval. If no heartbeat interval is defined, the CBSD uses the default value of 30 s.

The 7705 SAR-Hmc disables the dynamic filter on the PDN router interface when the heartbeat response is the first successful response it receives after sending a grant request. Disabling the filter allows the router interface to operate normally and for any enabled SR OS features to operate.

If the heartbeat response includes a suspended grant message, the CBSD is no longer authorized to use the spectrum. The 7705 SAR-Hmc re-enables the dynamic filter on the PDN router interface to disable SR OS features and allow only SAS control messages over the interface.

3.8.7 CBSD grant relinquishment

The CBSD sends a request to relinquish a grant when:

- the heartbeat response includes a terminated grant message
- the heartbeat response includes an unsync-op-param message

- changes in any radio parameters are detected
- the CBSD holds a grant and the user issues the **cbsd-authorization shutdown** command

When a relinquish request is sent, the 7705 SAR-Hmc re-enables the dynamic filter on the PDN router interface to stop the SR OS traffic and allow only SAS control messages over the interface.

After receiving a relinquishment response or after 30 s, whichever comes first, the CBSD initiates a new grant request to reauthorize with the SAS.

3.8.8 CBSD deregistration

The 7705 SAR-Hmc deregisters from the SAS if one of the following occurs:

- the **cbsd-authorization shutdown** command is issued in the CLI
- the SAS returns a DEREGISTER code in its response
- the CBSD goes operationally down
- the band changes to one that is not a CBRS band
- the channel changes
- the maximum power value changes

If the CBSD deregisters from the SAS for any reason other than issuing the **shutdown** command in the CLI, the CBSD restarts the authentication procedure as described in Authentication procedure for TLS connection to the SAS/DP.

3.8.9 Interactions with other bands

Some deployments require the 7705 SAR-Hmc to use CBRS B48/n48 and another band to operate. For example, in private cellular networks, CBRS B48 can be used with B8 (privately owned and controlled) using a single SIM, or Verizon may offer carrier services along with CBRS B48 using a single Verizon SIM.

The 7705 SAR-Hmc checks the radio parameters periodically, and if the band is not CBRS B48/n48, it will relinquish the grant because it is no longer using the CBRS B48/n48 spectrum. However, the node will attempt to maintain the registration with the SAS even while on the non-CBRS band.

If the 7705 SAR-Hmc reconnects to CBRS B48/n48 and it is still registered with the SAS, it will enable the dynamic filter on the PDN router interface to stop SR OS traffic. The 7705 SAR-Hmc will initiate a grant request to re-establish the grant and its ability to use the CBRS B48/n48 band. If the node was deregistered while on the other band, it will attempt the CBSD authorization process from the beginning, starting with the registration procedure.

3.9 Remote access to cellular diagnostics port

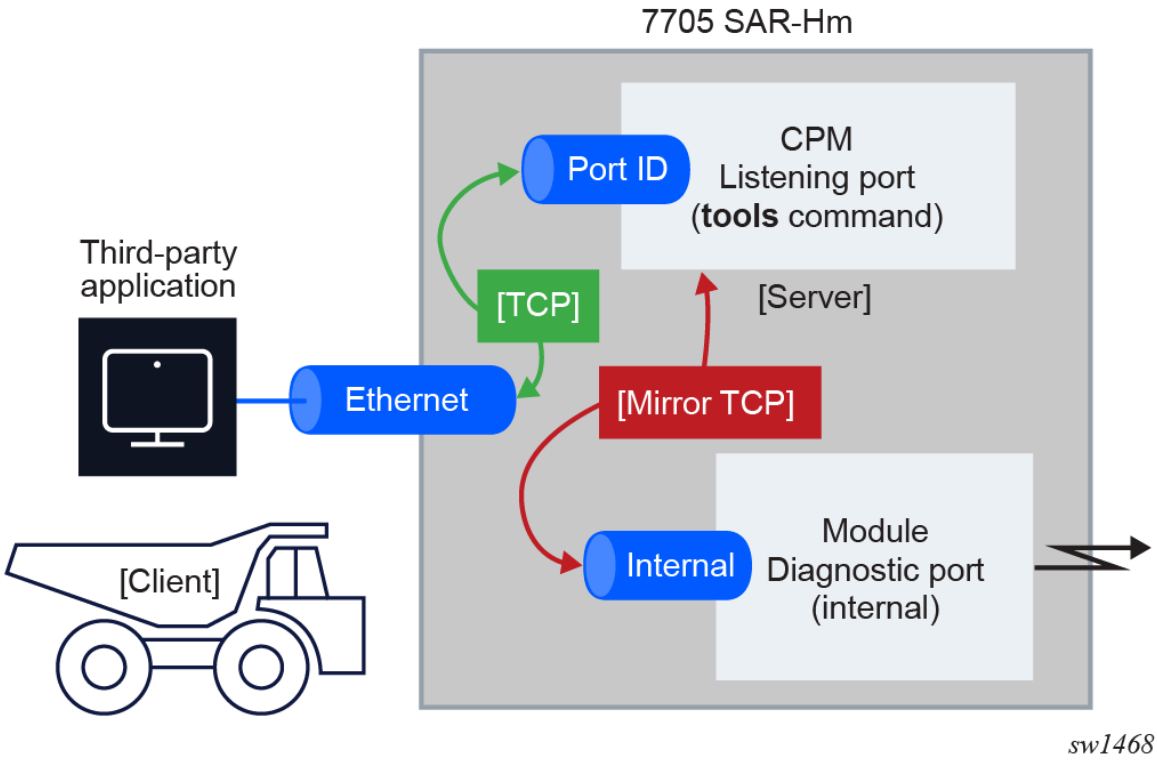
Some variants of the 7705 SAR-Hm series of routers allow the user to stream detailed diagnostic information from the internal cellular MDA diagnostic port on the radio. See the relevant *7705 SAR-Hm and SAR-Hmc Software Release Notes* for the list of variants that support this functionality.

Remote access to the cellular diagnostics port is enabled by executing the **tools>perform>cellular>diag-port-access>listening-port** *port-number***>start** command.The configured listening port remains active until it is disabled with the **tools>perform>cellular>diag-port-access>stop** command.

When enabled, the 7705 SAR-Hm series of routers act as a server for third-party applications to connect directly to the cellular modem to stream binary diagnostic information from the cellular radio in real time. The node acts as a TCP server and listens to connections on the listening port. Only one connection to the listening port is allowed at a time. The TCP connection can be established over any of the node Ethernet ports and the connection IP address (source IP address of the server) can be either the system IP address or the IP address of a base routing interface configured on the Ethernet port.

Figure 4: Remote access to the cellular diagnostics port shows the general mechanism for streaming cellular module diagnostic information to a third-party application that can interpret and display the information.

Figure 4: Remote access to the cellular diagnostics port



The status of the remote cellular diagnostics port on the 7705 SAR-Hm can be displayed on the CLI with the **tools>dump>cellular>diag-port-access>status** command.

4 GNSS receiver

4.1 In this chapter

This chapter provides information about the GNSS receiver. Topics include:

- Overview
- GNSS configuration
- Obtaining system time from the GNSS receiver

4.2 Overview

The GNSS receiver is used for streaming location information from the node (for example, for vehicle position information) or for querying GNSS information on the node.

4.3 GNSS configuration

GNSS services are enabled in the CLI under the cellular MDA (**mda 1/1**). Use the CLI for the following:

- enabling or disabling GNSS
- configuring the GNSS satellite constellation
- configuring NMEA parameters
- displaying GNSS location information and satellite information

4.3.1 Enabling or disabling GNSS

GNSS services are enabled using the **config>card>mda>gnss no shutdown** command. When GNSS services are enabled, the GNSS receiver begins acquiring GPS and/or GLONASS satellite signals and determines the position of the system. The GPS LED on the chassis blinks green during this process. The GPS LED is lit solid green when the GNSS receiver has determined the position of the node. The GPS LED is unlit when the GNSS receiver is disabled.

When NMEA services are also enabled, NMEA sentences are streamed according to the parameters associated with that service. See Configuring NMEA parameters for information.

GNSS services are disabled using the **shutdown** command. When GNSS services are disabled, the GNSS receiver is disabled and satellite information is reset. The GPS LED is unlit when the GNSS receiver is disabled.

GNSS services are disabled by default.

The GNSS receiver generates a logging event when it starts to acquire a position fix and when it has acquired a position fix.

4.3.2 Configuring the GNSS satellite constellation

The constellation of the GNSS receiver can be set to either GPS (**gps**) or GPS and GLONASS (**gps-glonass**). The constellation can be modified only when the GNSS service is shut down. The default constellation setting is **gps**.

4.3.3 Configuring NMEA parameters

The node can be configured to send position, velocity, and time information at regular intervals to servers that can process the data. When the data is formatted as an ASCII string according to National Marine Electronics Association (NMEA) standards, it is called an NMEA sentence. The node uses an IP transport service to send NMEA sentences to remote hosts. For information about enabling IP transport for NMEA sentences, see "GNSS NMEA data IP transport service" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

NMEA data streaming is enabled on the node when the IP transport *ipt-id* parameter is configured as **gnss** and the **nmea no shutdown** command is issued.

The following NMEA parameters must be configured on the node when streaming is enabled:

- sentence-type
- sentence-interval

The NMEA defines a number of sentence types for streaming. The node supports the following sentence types:

- GGA — this sentence is for time, position, and fix-related data for a GNSS receiver
- RMC — this sentence is for time, date, position, course, and speed data provided by the GNSS receiver
- VTG — this sentence is for vector track and speed relative to the ground
- GNS — this sentence is for time, position, and fix-related data for single or combined constellations for a GNSS receiver.

For information about the sentence types, see NMEA 0183, *Standard For Interfacing Marine Electronic Devices*.

The sentence interval specifies the frequency with which NMEA sentences are sent from the GNSS receiver. The interval can be set from 1 s to 3600 s. Different sentence types can be enabled concurrently so that multiple sentences can be streamed per sentence interval.

4.3.4 Displaying GNSS location and satellite information

The following GNSS location information can be displayed in the CLI:

- latitude of the last position fix
- longitude of the last position fix
- time at which the last position fix was taken
- altitude at which the last position fix was taken
- heading and speed of the system

If a GNSS fix is acquired and then subsequently lost by the node, the last known GNSS fix data continues to be displayed in the CLI. When a GNSS fix is reacquired, the GNSS data will then update to match the new fix.

The last GNSS fix data is not preserved after a **power-cycle**, **admin reboot**, **clear mda 1/1**, or **shutdown** command is issued for GNSS.

The following satellite information can be displayed in the CLI for up to 30 satellites:

- the satellite NMEA identifier—for GPS, the range is from 1 to 32; for GLONASS, the range is from 65 to 96
- the elevation of the satellite relative to the node, from 0° to 90°
- the azimuth relative to the node position, from 0° to 360°
- the signal-to-noise ratio (SNR), from 0 to 99 dB

4.4 Obtaining system time from the GNSS receiver

The GNSS receiver can obtain the system time when the **config>card>mda>gnss>sync-system-time** command is enabled. When the command is enabled and the GNSS receiver establishes a lock, system time is retrieved and set on the system.

Note: If NTP or SNTP is configured when the **sync-system-time** command is enabled, there is no time source precedence and either process can update the system time at its own discretion. Do not enable NTP or SNTP when the **sync-system-time** command is enabled unless NTP (or SNTP) and the GNSS receiver are using the same time source.

The cellular interface and the GNSS receiver can be configured concurrently to obtain the system time. When the **sync-system-time** command is enabled concurrently on the cellular interface and on the GNSS receiver, the GNSS receiver takes priority when it establishes a lock.

When the **sync-system-time** command is enabled, the system time cannot be set manually.

The **sync-system-time** command works in conjunction with the following commands:

- **config>system>time>dst-zone**
- **config>system>time>prefer-local-time**
- **config>system>time>zone**

For information about the **dst-zone**, **prefer-local-time**, and **zone** commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

5 Wireless LAN interface

5.1 In this chapter

This chapter provides information about the wireless LAN (WLAN) interface. Topics include:

- Overview
- WLAN radio MDA configuration
- WLAN port configuration
- WLAN MDA operating as both AP and station
- WLAN security
- Router and Layer 3 interfaces for WLAN ports
- WLAN interface status
- WLAN statistics

5.2 Overview

The node provides IEEE 802.11 b/g/n WLAN interface support.

The WLAN interface can be configured as an access point (AP) that clients can connect to or as a station that can connect to another AP. The interface can perform both functions concurrently.

There are two areas of configuration for the WLAN interface:

- the MDA-level configuration, which includes parameters such as channel, frequency band, and country
- the port-level configuration, which includes elements such as the network service set identifier (SSID), security parameters, WLAN access point parameters, and WLAN station parameters

There can be multiple APs per WLAN MDA, but only one station. The station can connect to one network from a list of possible candidates.

The WLAN ports on the node share the same WLAN MDA-level configuration. Each port has parameters that are configurable per network SSID.

5.3 WLAN radio MDA configuration

The following parameters must be configured for the WLAN MDA:

- country
- frequency band
- channel
- bandwidth

- administrative status
- beacon interval

The **country** parameter is required to bring the radio up. The **country** must be configured before any other MDA-level configuration can proceed and before the WLAN radio can be enabled with the **no shutdown** command. The **country** parameter is configured by entering one of the following country names in the CLI: Australia, Belgium, Bolivia, Brazil, Canada, Chile, Colombia, France, Germany, India, Iran, Italy, Japan, Malaysia, Mexico, New Zealand, Peru, Russia, Singapore, South Africa, United States, or Venezuela.

The **frequency-band** can be configured as either 2.4 GHz or 5 GHz. The default is 2.4 GHz. If the configured **country** changes, the frequency band resets to the default value.

The **channel** can be configured either as **auto** or as a specific channel identifier. The channel ID supported by the node depends on the configured **country**. See the Appendix for channel ID and country mappings. The default **channel** setting is **auto**. If the configured **country** changes, the channel resets to the default value.

A network SSID can only be configured when the **country** parameter is configured.

The **bandwidth** can be configured as either 20 MHz or 40 MHz, depending on the configured **country**. See the Appendix for bandwidth and country mapping. The default bandwidth is 20 MHz. If the configured country or frequency band changes, the bandwidth resets to the default value.

The WLAN station port uses the configured **frequency-band** to scan for an SSID that it can connect to.

The WLAN AP broadcasts a beacon packet in order to synchronize the wireless network. The frequency with which the packet is sent can be configured using the **beacon-interval** command.

The WLAN radio can be turned off using the **shutdown** command in the **config>card>mda>wlan-radio** context. When the WLAN radio is turned off, any configured WLAN ports become operationally down if they were not already shut down. When the **no shutdown** command is issued in this context, the radio is turned on and configured WLAN ports can begin operating; however, the **no shutdown** command cannot be issued until the **country** parameter is configured.

The WLAN radio can be put into reset mode using the **shutdown** command in the **config>card>mda** context. Any configured WLAN ports become operationally down when the WLAN radio is in reset mode. When the **no shutdown** command is issued in this context, the radio comes out of reset and configured WLAN ports can begin operating.

5.4 WLAN port configuration

The WLAN port identifiers for the WLAN MDA are fixed and represent either the APs or the station, as follows:

- port 1/4/1 is always AP 1
- port 1/4/2 is always AP 2
- port 1/4/3 is always AP 3
- port 1/4/4 is always station 1

All three APs can be operationally up concurrently when the station is not configured. Only one AP can be operationally up when the station is configured.

Each WLAN port operates either as an access port or as a network port as configured by the **mode** command in the **config>port>wlan** context. By default, when the port is an AP, its mode is **access**, and when the port is a station, its mode is **network**.

When a WLAN AP port is acting as an access port, it provides access-level connectivity to the Nokia WLAN gateway (GW) for subscriber and WLAN access and for WLAN mobility management. For more information, see "Transporting WLAN Access Point Traffic over Services" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*. When acting as a network port, a WLAN AP provides network-level connectivity to transport services to other connected WLAN stations in order to extend services over the AP. For more information, see "Services over the WLAN station port" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

Each WLAN port can be configured with security parameters for the WLAN network (see WLAN security).

Each WLAN AP port is configured with a unique network SSID and with AP-specific parameters, including dot1x parameters, DHCP relay, and access point control parameters. Layer 3 interfaces can be configured on a WLAN AP port.

The WLAN station port is configured with a list of network SSIDs it can connect to if the network is available. It is also configured with station-specific parameters, including network authentication and a password.

A router interface can be configured on any WLAN port. When a router interface is configured on a port, the port ID cannot be used as a SAP.

WLAN ports support IPv4.

5.4.1 Network SSID

The SSID defines the name of the WLAN network.

The WLAN AP ports use this name to allow WLAN clients to connect to their offered WLAN network.

The WLAN station port uses the network SSIDs to connect to remote APs. The WLAN station port supports up to 10 network SSIDs; however, the station can connect to only one network at a time. The 7705 SAR-Hm scans for available networks in priority order until it finds one that matches a configured network SSID and then it connects to that network. If multiple networks are available, the 7705 SAR-Hm connects to the network with the lowest SSID.

Operators must configure security parameters for each configured network SSID.

The SSID can be changed only when the WLAN port has been shut down.

5.4.2 AP-specific parameters

Operators can configure the following on a WLAN AP port:

- dot1x parameters, depending on the type of security configured
- DHCP relay (enabled or disable)
- broadcast of the SSID, using the **broadcast-ssid** command
- the maximum number of clients that can connect to the AP, using the **client-limit** command
- the length of time the port waits before releasing and disconnecting a client when the client has not transmitted or received any data, using the **client-timeout** command

The DHCP relay setting can be modified without shutting down a WLAN AP port. All other AP parameters can only be modified when the WLAN port is shut down.

When a WLAN port is configured as an AP, the CLI parameters in the **config>port>wlan>network>wlan-security>station** context are not available.

5.4.3 Station-specific parameters

When the WLAN port is operating as a station, the AP that the station connects to can be configured with its own set of security parameters when WLAN security is required. Operators can configure the following on a WLAN station port in order to connect to an AP that requires WLAN security:

- the type of authentication to be used by the WLAN station when the **wlan-security** parameter is set to **wpa2-enterprise**
- the password that the station will use when the network authentication method requires a password
- the name that the station will use when the network authentication method requires a username

For more information about WLAN Security, see WLAN security.

5.5 WLAN MDA operating as both AP and station

The 7705 SAR-Hm WLAN interface can operate both as a station and as an AP at the same time. This is possible when one of the WLAN AP ports is configured and the station port is also configured.

When the **configure>card>mda>wlan-radio>channel** command is set either to **auto** or to a specific channel, the station will scan and look for an SSID that it can connect to. The WLAN APs that are configured on the node will go down until the station connects to a channel. When the station connects to the SSID using the channel provided, the WLAN APs will also use the same channel.

When the WLAN MDA is operating concurrently as an AP and as a station and the configured frequency band of the WLAN radio MDA changes for example, from 2.4 GHz to 5 GHz or from 5 GHz to 2.4 GHz, a **clear mda 1/4** command must be issued to ensure the station connects to a remote AP.

Note: When the WLAN MDA is operating concurrently as an AP and as a station, the following restrictions apply:

- the 40 MHz bandwidth is not supported
- channels 149 to 165 are not supported

5.6 WLAN security

The WLAN ports support the following security options:

- open
- WPA2-PSK
- WPA2-Enterprise

When no WLAN security is required, a WLAN port is configured with **no wlan-security** and WLAN port security is open.

When WLAN security is required, a WLAN port can be configured with WPA2-PSK or WPA2-Enterprise security. When configuring either of these security types, the encryption must be set to either TKIP or AES using the **wpa-encryption** command. AES is the default.

When a WLAN port is configured for WPA2-PSK security, operators must use the **wpa-passphrase** command to configure a pre-shared secret passphrase that is used by clients to connect to the AP.

When the WLAN AP port is configured for WPA2-Enterprise security, operators must configure a RADIUS policy under the **config>system>security>dot1x** context in the CLI. For information about configuring a RADIUS policy in this context, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The dot1x RADIUS policy ID used to configure the RADIUS policy is then configured on the WLAN AP port using the **config>port>wlan>access-point>dot1x>radius-plcy** command.

The **retry** and **timeout** commands in the **config>system>security>dot1x> radius-plcy** context are ignored by the WLAN AP port. Instead, the retry count is set to 3 and the timeout value is set to 5 s so that the node will try each server four times before moving on to the next server if multiple servers are configured.

When the WLAN station port is configured with WPA2-Enterprise security, operators must configure the authentication type as one of EAP-TTLS, EAP-FAST, or EAP-PEAP using the **config>port>wlan>network>wlan-security>station>authentication** command. If the port is configured with WPA2-PSK security, the authentication type defaults to **none** and cannot be changed.

When the WLAN AP port is configured for WPA2-Enterprise security, connected clients are required to periodically reauthenticate themselves to the WLAN network. The interval is configured using the **re-auth-period** command.

Table 6: WLAN client authentication types lists the authentication methods that the node supports.

Table 6: WLAN client authentication types

Authentication type	Description	User password	User certificate	Server certificate
EAP-TTLS	The EAP-Tunneled Transport Layer Security (TTLS) authentication type establishes a tunnel in which the username and password are verified. A user and server certificate are optional. The username, password, and certificates are programmed on the client device.	Yes	Optional	Optional
EAP-FAST	The EAP-Flexible Authentication via Secure Tunneling (FAST) authentication type uses Protected Access Credentials (PAC) to establish a tunnel and the selected tunnel type to verify username and password credentials. PACs are handled behind the scenes, transparently to the user. Automatic PAC provisioning can require a user certificate and the validation of a server certificate depending on the tunnel type. The username, password, and certificates are programmed on the client device.	Yes	Optional	Optional
EAP-PEAP	The EAP-Protected Extensible Authentication Protocol (PEAP) authentication type establishes a tunnel and based on the tunnel type, uses a user certificate and/or a username and password. Validating a server certificate is optional. The username, password, and certificates are programmed on the client device.	Optional	Optional	Optional

Security parameters can only be modified when the WLAN port is shut down.

5.7 Router and Layer 3 interfaces for WLAN ports

The WLAN ports can be configured with a router interface or a Layer 3 interface in order to enable transport of network-level services, including VPRN services.

When a WLAN port is configured with a router interface, the port ID cannot be used as a SAP and the port can only operate in network mode.

When a WLAN port is configured with a Layer 3 interface, it can only operate in access mode.

5.7.1 WLAN AP port interfaces

When operating as an AP, the WLAN port can be configured with a Layer 3 interface within a VPRN or IES or with a router interface in the base router context.

Configuring a Layer 3 interface allows the WLAN AP to be added as a SAP in a VPRN or IES.

Configuring a router interface enables the AP to allow other nodes that are acting as WLAN stations to connect to it in order to route network traffic for other Layer 2 and Layer 3 services, using GRE-MPLS transport. A router interface configured on the WLAN AP port supports IPv4.

The WLAN AP port supports the following commands in the **config>router>interface** context:

- **address**
- **dhcp**
- **egress-ingress-stats**
- **cmd**
- **hold-time**
- **ip-mtu**
- **shutdown**

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* for command descriptions.

5.7.2 WLAN station port interface

When operating as a station, the WLAN port can be configured with a router interface. The IP address of the interface can be manually configured or it can be learned dynamically when DHCP client functionality is enabled on the interface. For information about DHCP client support, see "Router configuration" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

5.8 WLAN interface status

Table 7: WLAN interface status describes the operational states that apply to the WLAN interface.

Table 7: WLAN interface status

Status	Description
AdminDown	The WLAN port is administratively disabled
RfAdminDown	The WLAN radio is administratively disabled
RfChScanInProgress	The WLAN radio is scanning frequencies for ACS (Auto-Channel Select)
NoRadiusPlcy	WPA2-Enterprise security is enabled but no RADIUS policy is configured. This status applies only to the WLAN AP port.
Dot1xDisabled	WPA2-Enterprise security is enabled and dot1x authentication is disabled at the system level. This status applies only to the WLAN AP port.
RadiusPlcyDisabled	WP2-Enterprise security is enabled but the configured RADIUS policy is administratively disabled. This status applies only to the WLAN AP port.
NoAuthRadiusSvr	WPA2-Enterprise security is enabled but the configured RADIUS policy contains no authorization servers. This status applies only to the WLAN AP port.
NoRadiusNasIp	WPA2-Enterprise security is enabled but no NAS IP address is found. The NAS IP address is the address specified in the RADIUS policy. This status applies only to the WLAN AP port.

5.9 WLAN statistics

Statistics items can be displayed on the CLI for the WLAN port and for each WLAN instance. The node also collects access point and client-specific data transfer and operational statistics.

5.9.1 WLAN port statistics

On the WLAN port, the CLI displays a summary of the total port traffic into and out of the WLAN radio.

5.9.2 WLAN AP statistics and information

The node collects statistics and information that summarize the use of the WLAN AP, as listed below:

- port-level traffic statistics (packets and bytes)
- RADIUS information
- AP-level operational statistics:
  - number of clients currently connected

- total number of client attachments
- total number of client detachments
- total number of successful client authentications
- total number of failed client authentications

5.9.3 WLAN station statistics and status information

Summary traffic and operational statistics are collected for each SSID configured for the WLAN station port, specifically, the number of successful connections, the number of packets that were transmitted and received and the number of bytes that were transmitted and received. In addition, the CLI displays the MAC address (BSSID) of the AP that the station is connected to as well as information about handshake failures and connections that are detached.

When the WLAN port is acting as a station, the RSSI received by the WLAN station interface is displayed for the SSID that the station is connected to. It is also possible to use the CLI to display the time when the WLAN station connected to an AP and the duration of the connection.

6 Configuring physical ports

This chapter provides information about configuring physical ports with the CLI on the node.

Topics in this chapter include:

- Configuring Ethernet port parameters
- Configuring cellular port parameters
- Configuring serial port parameters
- Configuring RS-232 raw socket serial port parameters

6.1 Configuring Ethernet port parameters

See "Configuring Ethernet port parameters" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide* for information.

6.2 Configuring cellular port parameters

The **pdn-profile** parameter must be configured for the cellular port.

The PDN profile defines the specific APN that the node can connect to. Configure the **pdn-profile** under the appropriate cellular port. If a PDN profile is not specified, the default profile is used; this default PDN profile cannot be changed.

For more information, see Cellular PDN profile configuration commands and Cellular MDA and cellular port configuration commands .

6.3 Configuring serial port parameters

Use the following CLI syntax to configure parameters on an RS-232 serial port.

CLI Syntax:

```
config# port port-id
    no shutdown
    serial
        rs232
            character-length {6 | 7 | 8}
            control-lead
                input
                    dtr-dsr high
                    rts-dcd high
                exit
                output
                    dcd-rts high
                    cts-alb high
                    ri-rdl high
                exit
```

```
                monitor
                    dtr-dsr off
                    rts-dcd off
                exit
            hold-time {[up hold-time-up] [down hold-time-down]}
            no loopback
            parity {odd | even | mark | space}
            speed {600 | 1200 | 2400 | 4800 |
9600 | 19200 | 38400 | 57600 | 115200}
            stop-bits {1|2}
            exit
        exit
    exit
```

The following CLI syntax shows an example of configuring an RS-232 serial port.

Example:

```
config# port 1/3/2
config>port# no shutdown
config>port# description "RS-232 Serial”
config>port# serial
config>port>serial# rs232
config>port>serial>rs232# character-length 8
config>port>serial>rs232# control-lead
config>port>serial>rs232>control-lead# input
config>port>serial>rs232>control-lead>input# dtr-dsr high
config>port>serial>rs232>control-lead>input# rts-dcd high
config>port>serial>rs232>control-lead>input# exit
config>port>serial>rs232>control-lead# output
config>port>serial>rs232>control-lead>output# dcd-rts high
config>port>serial>rs232>control-lead>output# cts-alb high
config>port>serial>rs232>control-lead>output# ri-rdl high
config>port>serial>rs232>control-lead>output# exit
config>port>serial>rs232>control-lead# monitor
config>port>serial>rs232>control-lead>monitor# dtr-dsr off
config>port>serial>rs232>control-lead>monitor# rts-dcd off
config>port>serial>rs232>control-lead>monitor# exit
config>port>serial>rs232>control-lead# exit
config>port>serial>rs232# hold-time up 100
config>port>serial>rs232# no loopback
config>port>serial>rs232# parity odd
config>port>serial>rs232# speed 9600
config>port>serial>rs232# stop-bits 1
config>port>serial>rs232# exit
config>port>serial# exit
config>port# exit
```

Use the **admin>display-config detail** command to display the serial RS-232 port configuration information.

```
*A:Dut>admin# display-config detail
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
  .....
port 1/3/2
        description "RS-232 Serial"
        serial
            rs232
                speed 9600
                control-lead
                    input
```

```
                        dtr-dsr high
                        rts-dcd high
                    exit
                    output
                        dcd-rts high
                        cts-alb high
                        ri-rdl high
                    exit
                    monitor
                        dtr-dsr off
                        rts-dcd off
                    exit
                exit
                character-length 8
                parity odd
                stop-bits 1
                hold-time up 100 down 100
                    exit
                exit
            exit
        exit
    exit
  .....
#--------------------------------------------------
```

6.4 Configuring RS-232 raw socket serial port parameters

Use the following CLI syntax to configure an RS-232 raw socket serial port.

CLI Syntax:

```
config# port port-id
    serial
        rs232
            socket
                description description-string
                rx
                    eop
                        length bytes
                        idle-timeout milliseconds
                        [no] special-char value
                        exit
                    no squelch-delay
                    no unsquelch-delay
                    exit
                tx
                    inter-session-delay ms
                    exit
            exit
        exit
```

The following CLI syntax shows an example of configuring an RS-232 raw socket serial port.

Example:

```
config# port 1/3/2
config>port# description "RS-232 Serial"
config>port# serial
config>port>serial# rs232
config>port>serial>rs232# socket
config>port>serial>rs232>socket# rx
config>port>serial>rs232>socket>rx# eop
```

```
config>port>serial>rs232>socket>rx>eop# idle-timeout 50
config>port>serial>rs232>socket>rx>eop# length 1500
config>port>serial>rs232>socket>rx>eop# no special-char
config>port>serial>rs232>socket>rx>eop# exit
config>port>serial>rs232>socket>rx# no squelch-delay
config>port>serial>rs232>socket>rx# no unsquelch-delay
config>port>serial>rs232>socket>rx# exit
config>port>serial>rs232>socket# tx
config>port>serial>rs232>socket>tx# inter-session-delay 10
config>port>serial>rs232>socket>tx# exit
config>port>serial>rs232>socket# exit
config>port>serial>rs232# exit
config>port>serial# exit
config>port# exit
```

Use the **admin>display-config detail** command to display the raw socket port configuration information.

```
*A:Dut>admin# display-config detail
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
  .....
port 1/3/2
        description "RS-232 Serial"
        serial
            rs232
                socket
                    rx
                        eop
                            length 1500
                            idle-timeout 50
                            no special-char
                        exit
                        no squelch-delay
                        no unsquelch-delay
                    exit
                    tx
                        inter-session-delay 10
                    exit
                exit
            exit
        exit
    exit
  .....
#--------------------------------------------------
```

7 Interface command reference

This chapter describes the following:

- Configuration commands
- Show, clear, and tools commands

7.1 Configuration commands

Note: The commands described in this section apply specifically to the 7705 SAR-Hm series nodes. All other applicable commands supported on the nodes are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* and the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*.

7.1.1 Configuration command hierarchies

- Ethernet commands
- Ethernet access and network commands
- Cellular MDA and cellular port configuration commands
- Cellular PDN profile configuration commands
- GNSS receiver configuration commands
- Serial interface configuration commands
- Serial raw socket interface configuration commands
- WLAN MDA radio configuration commands
- WLAN port configuration commands

7.1.1.1 Ethernet commands

The following commands are supported on 7705 SAR-Hm series nodes. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* for the command descriptions.

Note: Not all commands that are visible in the CLI, and described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* and the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*, are supported on 7705 SAR-Hm series nodes. Only the commands that are listed below are supported.

```
config
    - [no] port {port-id}
        - ethernet
            - autonegotiate [limited]
```

```
            - no autonegotiate
            - dot1q-etype value
            - no dot1q-etype
            - down-on-internal-error [tx-disable]
            - no down-on-internal-error
            - duplex {full | half}
            - egress-scheduler-override [create]
            - no egress-scheduler-override
                - levelpriority-level rate pir-rate [cir cir-rate]
                - levelpriority-level percent-rate pir-percent [percent-cir cir-percent]
                - no level priority-level
                - max-rate rate
                - max-rate percent percent-rate
                - no max-rate
            - egress-scheduler-policy port-scheduler-policy-name
            - no egress-scheduler-policy
            - encap-type {dot1q | null}
            - no encap-type
            - hold-time {[up hold-time up] [down hold-time down] [seconds | centiseconds]}
            - no hold-time
            - mac ieee-address
            - no mac
            - min-frame-length byte-length
            - mode {access | network | hybrid}
            - no mode
            - mtu mtu-bytes
            - no mtu
            - speed {10 | 100}
```

7.1.1.2 Ethernet access and network commands

```
config>port>ethernet
    - access
        - bandwidth bandwidth
        - no bandwidth
        - booking-factor factor
        - no booking-factor
        - egress
        - ingress
    - network
        - accounting-policy policy-id
        - no accounting-policy
        - [no] collect-stats
        - egress
        - queue-policy name
        - no queue-policy
```

7.1.1.3 Cellular MDA and cellular port configuration commands

```
config
    - card 1
        - mda 1
            - cellular
                - active-sim {1 | 2 | auto}
                - b125-max-tx-power power-level
                - no b125-max-tx-power
                - down-recovery-interval interval
                - no down-recovery-interval
```

```
                - down-recovery-criteria criterion [criterion...(up to two)]
                - no down-recovery-criteria
                - max-tx-power maximum-tx-power
                - preferred-sim {1 | 2}
                - no preferred-sim
                - sim sim-card-number
                    - band-list band-num [band-num...(up to 4 max)]
                    - no band-list
                    - description description-string
                    - no description
                    - failover-criteria
                        - [no] bgp-neighbor-state
                        - failure-duration minutes
                        - [no] port-oper-state
                        - [no] rssi-threshold
                    - pin
                    - pin pin-value [hash | hash2]
                    - no pin
                    - rssi-alarm-wait-time wait-time
                    - rssi-threshold rx-power
                    - no rssi-threshold
```

```
config
    - port port-id
        - description description-string
        - no description
        - cellular
            - cbsd-authorization
                - antenna-gain gain
                - no antenna-gain
                - category {a | b}
                - client-tls-profile tls-profile-name
                - no client-tls-profile
                - sas-server-primary url-string
                - no sas-server-primary
                - sas-server-secondary url-string
                - no sas-server-secondary
                - [no] shutdown
                - userid userid-string
                - no userid
            - pdn
                - pdn-profile pdn-profile-id
                - no pdn-profile
            - [no] sync-system-time
        - [no] shutdown
```

7.1.1.4 Cellular PDN profile configuration commands

```
config
    - system
        - cellular
            - pdn-profile  pdn-profile-number [create]
            - no pdn-profile
                - apn apn-name
                - no apn
                - authentication {pap | chap}
                - no authentication
                - description description-string
                - no description
                - password password [hash | hash2 | custom]
```

```
                - no password
                - protocol  {ipv4 | ipv6}
                - username user-name
                - no username
```

7.1.1.5 GNSS receiver configuration commands

```
config
    - card 1
        - mda 1
            - gnss
                - constellation {gps | gps-glonass}
                - nmea
                    - sentence-types sentence-type [sentence-type...(up to 4 max)]
                    - sentence-interval interval
                    - [no] shutdown
                - [no] shutdown
                - [no] sync-system-time
```

7.1.1.6 Serial interface configuration commands

```
config
    - [no] port port-id
        - serial
            -  rs232
                - character-length  {6 | 7 | 8}
                - control-lead  {input | output}
                    - input
                        - dtr-dsr  {high | low}
                        - rts-dcd  {high | low}
                    - monitor
                        - dtr-dsr  {on | off}
                        - rts-dcd  {on | off}
                    - output
                        - cts-alb  {high | low}
                        - dcd-rts {high | low}
                        - ri-rdl  {high | low}
                - hold-time {[up hold-time-up] [down hold-time-down]}
                - no hold-time
                - loopback bidir-e
                - no loopback
                - parity  {odd | even | mark | space}
                - no parity
                - [no] shutdown
                - speed {600 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 |
57600 | 115200}
                - stop-bits {1 | 2}
```

7.1.1.7 Serial raw socket interface configuration commands

Note: To enable the serial transport over raw socket functionality on 7705 SAR-Hm series nodes, configure an RS-232 raw socket serial port and create an IP transport subservice within a VPRN service. For information about how to configure an IP transport subservice within a VPRN, see

the "Serial raw socket IP transport configuration commands hierarchy" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

```
config
    - [no] port port-id
        - serial
            - [no] rs232
                - socket
                    - rx
                        - eop
                            - idle-timeout milliseconds
                            - length bytes
                            - special-char  value
                            - no special-char
                        - squelch-delay  seconds
                        - no squelch-delay
                        - squelch-reset
                        - unsquelch-delay  seconds
                        - no unsquelch-delay
                    - tx
                        - inter-session-delay  milliseconds
```

7.1.1.8 WLAN MDA radio configuration commands

```
config
    - card 1
        - mda 4
            - [no] shutdown
            - wlan-radio
                - bandwidth {20MHz | 40MHz}
                - beacon-interval milliseconds
                - channel {auto | channel-id}
                - [no] country country-string
                - frequency-band {2400 | 5000}
                - [no] shutdown
```

7.1.1.9 WLAN port configuration commands

```
config
    - port
        - description description-string
        - no description
        - [no] shutdown
        - wlan
            - access-point
                - [no] broadcast-ssid
                - client-limit clients
                - client-timeout seconds
                - dhcp
                    - [no] shutdown
                - dot1x
                    - radius-plcy  policy-name
                    - no radius-plcy
                    - re-auth-period seconds
            - mode {access | network}
            - network network-id ssid ssid-name [create]
            - no network
```

```
                - wlan-security [type {wpa2-psk | wpa2-enterprise}]
                - no wlan-security
                    - station
                        - authentication {eap-ttls | eap-fast | eap-peap}
                        - no authentication
                        - password password-string [hash | hash2]
                        - no password
                        - username username-string
                        - no username
                    - wpa-encryption [tkip | aes]
                    - no wpa-encryption
                    - wpa-passphrase ascii-passphrase [hash | hash2]
                    - no wpa-passphrase
```

7.1.2 Configuration command descriptions

The commands described in this section apply specifically to 7705 SAR-Hm series nodes. All other applicable commands supported on the nodes are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* and the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*.

- Common configuration commands
- Cellular MDA and cellular port configuration commands
- Cellular PDN profile configuration commands
- Ethernet configuration commands
- GNSS receiver configuration commands
- Serial interface configuration commands
- Raw socket configuration commands
- WLAN MDA radio configuration commands
- WLAN port configuration commands

7.1.2.1 Common configuration commands

description

Syntax

description *description-string*

no description

Context

config>card>mda>cellular>sim

config>port

config>system>cellular>pdn-profile

Description

This command creates a text description for a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the description string from the context.

Default

n/a

Parameters

description-string

a description character string. Allowed values are any string up to 80 or 160 characters long (depending on the command), composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, or spaces), the entire string must be enclosed within double quotes.

shutdown

Syntax

[**no**] **shutdown**

Context

config>port

config>port>serial>rs232

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.

The **no** form of this command administratively enables an entity.

Default

no shutdown

7.1.2.2 Cellular MDA and cellular port configuration commands

port

Syntax

port *port-id*

Context

config

Description

This command configures an identifier for a cellular port on the node. Up to two cellular ports can be configured and each cellular port is associated with a SIM. Cellular port 1/1/1 is associated with SIM 1 and cellular port 1/1/2 is associated with SIM 2. The relationship between the ports and the SIMs cannot be changed.

Default

1/1/1

Parameters

port-id

the cellular port identifier

Values 1/1/1 or 1/1/2, in the format *slot/mda/port*

active-sim

Syntax

active-sim {**1** | **2** | **auto**}

Context

config>card>mda>cellular

Description

This command assigns a SIM to be the active SIM.

When the system powers up or reboots, it uses the **active-sim** setting to determine which SIM is the active SIM. Selecting **1** or **2** makes the selected SIM permanently active. The active SIM can be manually switched by changing the **active-sim** setting from **1** to **2** or from **2** to **1**.

Caution:
Changing the active SIM from **1** to **2** or from **2** to **1** is considered a manual switchover and is service-affecting. The recovery time after making the change can range from a few seconds to up to a few minutes. Ensure that there is service on the other SIM before changing the active SIM.

If a SIM is specified but is not physically installed in the associated SIM slot, the cellular port remains operationally down. The operator must either install the SIM in the appropriate slot or change the configuration to bring up the service.

Selecting **auto** enables automatic failover in a dual SIM deployment. An automatic failover occurs when activity switches from one SIM to the other. The settings configured for the **failover-criteria** command determine when an automatic failover will occur.

When the **auto** parameter is set in a dual SIM deployment, the node must be configured with a preferred SIM. The **preferred-sim** command specifies whether SIM 1 or SIM 2 is used for a cellular port after a system reset.

If the **active-sim** value is changed from **auto** to **1** or from **auto** to **2** and the active SIM is the same as the new configuration, there is no change to service of the active SIM.

Caution:
Changing the **active-sim** setting so that the newly active SIM is different from the currently active SIM is service-affecting. The recovery time after making this change could range from a few seconds to up to a few minutes.

If the **active-sim** value is changed from **1** to **auto** or from **2** to **auto**, there is no service outage. The system keeps the currently active SIM up and does not perform any switchover.

When **active-sim** is set to **auto**, operators can use the **tools>perform>mda>cellular>force-sim-switch** command to manually force a SIM switch.

The **auto** parameter can be set even if there is only one SIM installed in the system. In this case, the system keeps the currently active SIM up and does not perform any switchover.

Default

1

Parameters

1

sets the active SIM to SIM 1

2

sets the active SIM to SIM 2

auto

enables automatic failover between the two SIMs in a dual SIM deployment

b125-max-tx-power

Syntax

b125-max-tx-power *power-level*

no b125-max-tx-power

Context

config>card>mda>cellular

Description

This command configures the maximum transmit power level of the B125 radio module. The B125 power level depends on the installation height of the B125 variant antenna, and the value must be set based on the guidelines provided in the *SAR-Hm and SAR-Hmc Chassis Installation Guide* for B125 antenna locations.

For more information, see the *SAR-Hm and SAR-Hmc Chassis Installation Guide*.

Default

1

Parameters

power-level

the B125 antenna power level

Values 1 to 20

down-recovery-interval

Syntax

down-recovery-interval *interval*

no down-recovery-interval

Context

config>card>mda>cellular

Description

This command configures the length of time in which the cellular MDA must establish cellular service for a SIM or the length of time in which a BGP session must be established on the node before the node resets. It is used in conjunction with the **down-recovery-criteria** command.

When configured, this option provides a hardware reset to unblock any potential hardware lockup conditions related to the cellular radio modem or to guard against persistent cycling of automatic switchovers between SIMs in a dual SIM deployment. If the cellular MDA has not successfully achieved service or a BGP session has not been established on the node based on the configured **down-recovery-criteria** value within the specified length of time, the node resets.

Before resetting, the node will issue a log event stating that the node will reset within 60 seconds. This interval can be used to collect information for further debugging and analysis.

The **no** form of the command disables the **down-recovery-criteria** and the state of the cellular MDA or the BGP sessions on the node are not monitored other than for dual SIM operation and criteria configured for automatic failover (see failover-criteria for more information).

Default

no down-recovery-interval

Parameters

interval

the length of time, in minutes, before a down-recovery condition is declared

Values 1 to 240

down-recovery-criteria

Syntax

down-recovery-criteria *criterion* [*criterion*...(up to two)]

no down-recovery-criteria

Context

config>card>mda>cellular

Description

This command configures criteria used to detect a problem with the cellular radio modem. It is used in conjunction with the **down-recovery-interval** command. The options are **port** and **bgp**.

When the command is set to **port**, the node detects if any cellular port has connected to a wireless network and is operationally up within the configured **down-recovery-interval**. When a port connects successfully, the down-recovery timer stops. The down-recovery timer restarts when all PDN interfaces are operationally down.

When the command is set to **bgp**, the node detects if any BGP session configured on the node has come up within the configured **down-recovery-interval**. When a BGP session comes up, the down-recovery timer stops. The down-recovery timer restarts when all BGP sessions are down.

Both **port** and **bgp** can be set concurrently.

Default

port

Parameters

criterion

specifies the criterion to use for detecting a problem with the cellular radio modem

Values **port** — all cellular ports are monitored

bgp — all BGP sessions associated with PDNs are monitored

max-tx-power

Syntax

max-tx-power *maximum-tx-power*

Context

config>card>mda>cellular

Description

This command configures the maximum transmit power used by the cellular interface on the MDA of the 7705 SAR-Hmc. For information about supported variants, see the *7705 SAR-Hm/Hmc Software Release Notes*. This command is not supported on the 7705 SAR-Hm.

The command is used when higher gain antennas are deployed using spectrum where maximum power must be reduced to accommodate for the added gain.

The command adjusts the upper range of transmit power on the cellular interface. The transmit power range of the cellular interface on the MDA is -44 dBm to 23 dBm. The command can adjust this power range down by as much as 22 dB when the parameter is set within the supported range of 1 to 23 dBm.

Default

23 dBm

Parameters

maximum-tx-power

the transmit power

Values 1 to 23 dBm (in 1 dBm increments)

preferred-sim

Syntax

preferred-sim {**1** | **2**}

no preferred-sim

Context

config>card>mda>cellular

Description

This command configures which SIM to use when the node resets. The configuration is used in a dual SIM deployment when the **active-sim** command is set to **auto**. When the node resets, the system uses the preferred SIM to bring up the associated cellular port.

Note: Before setting the preferred SIM, the operator must ensure that the corresponding SIM is installed and configured.

Default

1

Parameters

1

sets the preferred SIM to SIM 1

2

sets the preferred SIM to SIM 2

sim

Syntax

sim *sim-card-number*

Context

config>card>mda>cellular

Description

This command enables the context to configure parameters for the specified SIM.

Parameters

sim-card-number

identifies the SIM

Values 1 or 2

band-list

Syntax

band-list *band-num* [*band-num*...(**up to 4 max**)]

no band-list

Context

config>card>mda>cellular>sim

Description

This command specifies a list of cellular bands that the cellular interface uses when searching for a cellular network to attach to. The list is configured per SIM. A band list can be configured for one or both SIMs in a dual SIM deployment and they can be different.

The bands that are available depend on the MDA variant on which the list is being configured; see the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for information.

A band list is considered invalid and will be rejected by the CLI if it contains more than the maximum number of bands allowed or if any band in the list is not supported by the MDA.

If the list contains bands that are not supported by the firmware for a specific carrier, the node will use only the bands that are supported by the firmware. For example, if the firmware supports bands B2, B5, B7, B13, and B66 but the **band-list** is configured with bands B2, B42, B48, and B71, the node will only allow B2 to be configured on the MDA because it is the only band on the list that is supported by the firmware.

If none of the bands on the list are supported by the firmware, the node ignores the configured **band-list** and reverts to enabling all bands on the MDA that are supported by the firmware. Enabling all supported bands ensures that the node can connect to the network if further actions are required to manage the node.

In a dual SIM deployment, a SIM switchover causes the MDA to reset, which enables the band list on the newly active SIM.

Up to three bands and one 3G band can be included on the band list. The **no** form of the command removes the list from the SIM.

Default

no band-list

Parameters

band-num

the band number to be added to the list, up to three bands and one 3G band

pin

Syntax

pin

pin *pin-value* [**hash** | **hash2**]

no pin

Context

config>card>mda>cellular>sim

Description

This command stores the SIM PIN in the system configuration file. This command does not change the PIN on the SIM.

Use the **pin** command to enter the PIN in the system configuration file from an interactive CLI session. The system prompts you to enter the PIN twice. If the two entered PINs do not match, the system rejects the configuration.

Use the **pin** command with a specified PIN value and the **hash** or **hash2** keyword to load the PIN in encrypted form in the configuration file.

The **no** form of this command removes the PIN from the system configuration.

Default

n/a

Parameters

pin-value

the 4-to-8 digit PIN code

hash

specifies that the PIN is entered in an encrypted form. If the **hash** or **hash2** keyword is not used, the PIN is assumed to be in an unencrypted, clear text form. For security, all PINs are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

hash2

specifies that the PIN is entered in a more complex, encrypted form that involves more variables than the PIN value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** keyword is not used, the PIN is assumed to be in an unencrypted, clear text form. For security, all PINs are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

failover-criteria

Syntax

failover-criteria

Context

config>card>mda>cellular>sim

Description

This command enables the context to configure the criteria that will cause an automatic SIM switchover in a dual SIM deployment.

The **failover-criteria** parameters are used when the **active-sim** command is set to **auto**. The parameters are configured per SIM, so each SIM can have different failover criteria. The system uses the criteria configured on the currently active SIM to determine when a switchover should occur.

Default

n/a

bgp-neighbor-state

Syntax

[**no**] **bgp-neighbor-state**

Context

config>card>mda>cellular>sim>failover-criteria

Description

This command sets the operational status of BGP sessions as a failover criterion for the specified SIM.

If the operational status of all BGP sessions remain down for the **failure-duration** interval, the system performs an automatic switch from the currently active SIM to the other SIM.

The **no** form of the command disables the **bgp-neighbor-state** from being used as a failover criterion.

Default

no bgp-neighbor-state

failure-duration

Syntax

failure-duration *minutes*

Context

config>card>mda>cellular>sim>failover-criteria

Description

This command configures the length of time before the SIM is considered to be in a failed state based on the specified failover criteria. The value is used for both configured failover criteria.

When the node detects a down state for the **failure-duration** time, the SIM is considered to be in a failed state and the node performs an automatic switch from the currently active SIM to the other SIM.

Note: It is recommended that the **failure-duration** be set to a high value so that the system does not perform frequent switches between SIMs.

Default

5

Parameters

minutes

the length of time, in minutes, before the SIM is considered to be in a failed state

Values 1 to 60

port-oper-state

Syntax

[**no**] **port-oper-state**

Context

config>card>mda>cellular>sim>failover-criteria

Description

This command sets the operational status of the cellular port as a failover criterion for the specified SIM.

If the operational status of the cellular port remains down for the **failure-duration** interval, the SIM is considered to be in a failed state and the system performs an automatic switch from the currently active SIM to the other SIM.

The **no** form of the command disables the **port-oper-state** from being used as a failover criterion.

Default

port-oper-state

rssi-threshold

Syntax

[**no**] **rssi-threshold**

Context

config>card>mda>cellular>sim>failover-criteria

Description

This command enables the RSSI threshold as a failover criterion for the specified SIM in a dual SIM deployment.

When the **rssi-threshold** command under the **config>card>mda>cellular>sim** context is enabled, if the RSSI signal level falls below the configured value for the RSSI threshold for the **failure-duration** time, the node performs an automatic switchover from the currently active SIM to the other SIM.

The **no** form of the command disables the RSSI threshold from being used as a failover criterion.

Default

no rssi-threshold

rssi-alarm-wait-time

Syntax

rssi-alarm-wait-time *wait-time*

Context

config>card>mda>cellular>sim

Description

This command sets the length of time that the node waits before raising or clearing an RSSI system alarm on the specified SIM.

If the RSSI signal level falls below the configured **rssi-threshold** value for the specified wait time, an alarm is raised. The alarm is raised only once, even if the RSSI signal level remains below the configured threshold indefinitely. After the alarm is raised, if the RSSI signal level rises to the configured **rssi-threshold** value or higher and remains at that level for the duration of the specified alarm wait time, the alarm is cleared.

The RSSI alarm wait time cannot be unset; the wait time always has a value.

Default

60 s

Parameters

wait-time

the length of time that the RSSI signal must be below or above the configured **rssi-threshold** before an alarm is raised or cleared

Values 1 s to 300 s

rssi-threshold

Syntax

rssi-threshold *rx-power*

no rssi-threshold

Context

config>card>mda>cellular>sim

Description

This command sets the RSSI threshold value.

If the RSSI signal level falls below this threshold for the duration of the **rssi-alarm-wait-time**, an alarm is raised. If the RSSI signal level then rises to or above the threshold value and remains at that level for the duration of the **rssi-alarm-wait-time**, the alarm is cleared.

The **no** form of the command removes the RSSI threshold value.

Default

no rssi-threshold

Parameters

rx-power

the RSSI threshold value

Values -113 dBm to -51 dBm

cbsd-authorization

Syntax

cbsd-authorization

Context

config>port>cellular

Description

This command enables the context to enable the authorization process on the PDN router interface so that the node can operate as a Category A or Category B Citizens Broadband Radio Service Device (CBSD) in the Citizens Broadband Radio Service (CBRS) B48 spectrum.

When this command is issued, all other functions on the PDN interface are blocked until the Spectrum Access System (SAS) authorizes the node to transmit on B48. This command is available only for the 7705 SAR-Hmc NA variant (3HE12472AA), the 7705 SAR-Hmc NA variant 2 (3HE12473AA), and the 7705 SAR-Hmc World variant (3HE12478AA).

Default

n/a

antenna-gain

Syntax

antenna-gain *gain*

no antenna-gain

Context

config>port>cellular>cbsd-authorization

Description

This command sets the antenna gain of the CBSD. The value configured for this command is added to the configured **max-tx-value** to calculate the maximum EIRP value used in the grant request to the SAS server.

The **no** form of the command resets the antenna gain to the default.

Default

0

Parameters

gain

the antenna gain in dBm

Values 0 to 24

category

Syntax

category {**a** | **b**}

Context

config>port>cellular>cbsd-authorization

Description

This command sets the category of the CBSD to either Category A or Category B. This value is used in the registration request to the SAS server and must match the value expected by the SAS.

Default

a

Parameters

a

defines the CBSD as Category A

b

defines the CBSD as Category B

client-tls-profile

Syntax

client-tls-profile *tls-profile-name*

no client-tls-profile

Context

config>port>cellular>cbsd-authorization

Description

This command names the client TLS profile that is used to authenticate the CBSD with the SAS server.

The TLS client profile must first be configured in the **config>system>security>tls** context. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* for the command description.

This command must be configured before issuing the **no shutdown** command in the **cbsd-authorization** context.

The **no** form of the command deletes the client TLS profile.

Default

n/a

Parameters

tls-profile-name

the name of an existing TLS client profile

sas-server-primary

Syntax

sas-server-primary *url-string*

no sas-server-primary

Context

config>port>cellular>cbsd-authorization

Description

This command sets the location of the primary SAS server. The URL is provided by the SAS administrator. The location of the primary SAS server must be configured before issuing the **no shutdown** command in the **cbsd-authorization** context.

The **no** form of this command deletes the primary SAS server location.

Default

n/a

Parameters

url-string

the link to the SAS primary server; it contains either the SAS server name or IP address

Values *login*:*pswd*@]*remote-locn*/*path*: up to 255 characters

login: the username

pswd: the user password

remote-locn: {*hostname* | *ipv4-address* | [*ipv6-address*]}[:*port*]

hostname: the hostname for the server

ipv4-address: a.b.c.d

ipv6-address:

x:x:x:x:x:x:x:x[-*interface*]

x:x:x:x:x:x:d.d.d.d[-*interface*]

x - [0 to FFFF]H

d - [0 to 255] D

interface - the interface for the link local address, up to 32 characters

port: 0 to 65535

path: the path to the specific resource being accessed

sas-server-secondary

Syntax

sas-server-secondary *url-string*

no sas-server-secondary

Context

config>port>cellular>cbsd-authorization

Description

This command sets the location of the optional secondary SAS server. The URL is provided by the SAS administrator. The location of the secondary SAS server must be configured before issuing the **no shutdown** command in the **cbsd-authorization** context.

The **no** form of this command deletes the secondary SAS server location.

Default

n/a

Parameters

url-string

the link to the SAS secondary server; it contains either the SAS server name or IP address

Values *login*:*pswd*@]*remote-locn*/*path*: up to 255 characters

login: the username

pswd: the user password

remote-locn: {*hostname* | *ipv4-address* | [*ipv6-address*]}[:*port*]

hostname: the hostname for the server

ipv4-address: a.b.c.d

ipv6-address:

x:x:x:x:x:x:x:x[-*interface*]

x:x:x:x:x:x:d.d.d.d[-*interface*]

x - [0 to FFFF]H

d - [0 to 255] D

interface - the interface for the link local address, up to 32 characters

port: 0 to 65535

path: the path to the specific resource being accessed

shutdown

Syntax

[**no**] **shutdown**

Context

config>port>cellular>cbsd-authorization

Description

This command shuts down the CBSD authorization process. If the node is already registered with the SAS server, this command deregisters the 7705 SAR-Hmc from the SAS.

The **no** form of the command enables the CBSD authorization process with the SAS server.

Default

n/a

userid

Syntax

userid *userid-string*

no userid

Context

config>port>cellular>cbsd-authorization

Description

This command sets the CBSD user ID that is used in the registration request to the SAS server. The CBSD user is the entity that has operational responsibility for the CBSD.

The **no** form of the command deletes the user ID.

Default

n/a

Parameters

userid

the user ID of the CBSD

pdn

Syntax

pdn

Context

config>port>cellular

Description

This command enables the context to configure PDN parameters for the cellular port.

Default

n/a

pdn-profile

Syntax

pdn-profile *pdn-profile-id*

no pdn-profile

Context

config>port>cellular>pdn

Description

This command assigns a PDN profile to the cellular port. The PDN profile must be configured at the system level before this command can be used; see Cellular PDN profile configuration commands for information.

The **no** form of this command assigns the default PDN profile to the PDN.

Default

no pdn-profile

Parameters

pdn-profile-id

the PDN profile identifier

Values 1 to 15

sync-system-time

Syntax

[**no**] **sync-system-time**

Context

config>port>cellular

config>card>mda>gnss

Description

This command enables the cellular interface or the GNSS receiver to obtain the system time. When enabled, the time received over the cellular interface or the GNSS receiver is used to synchronize the node system time.

The cellular interface and the GNSS receiver can be configured concurrently to obtain the system time. When the **sync-system-time** command is enabled concurrently on the cellular interface and on the GNSS receiver, the GNSS receiver takes priority when it establishes a lock.

Note: If NTP or SNTP is configured when the **sync-system-time** command is enabled, there is no time source precedence and either process can update the system time at its own discretion. Do not enable NTP or SNTP when the **sync-system-time** command is enabled unless NTP (or SNTP) and the cellular interface or GNSS receiver are using the same time source.

The **no** form of this command disables the cellular interface or the GNSS receiver from acquiring the system time.

Default

no sync-system-time

7.1.2.3 Cellular PDN profile configuration commands

pdn-profile

Syntax

pdn-profile *pdn-profile-number* [**create**]

no pdn-profile

Context

config>system>cellular

Description

This command creates a PDN profile with an associated ID when used with the **create** keyword.

The system supports a default PDN profile and up to 15 user-created PDN profiles.

The default PDN profile is used during the ADP-Hm process and cannot be modified.

The **no** form of this command deletes the PDN profile if the profile is not in use. If the profile is in use, the **no** form of the command cannot be executed.

Default

n/a

Parameters

pdn-profile-number

the PDN profile identifier

Values 1 to 15

create

the keyword used to create the PDN profile

apn

Syntax

apn *apn-name*

no apn

Context

config>system>cellular>pdn-profile

Description

This command configures the Access Point Name (APN) for the PDN profile.

The **no** form of this command removes the APN.

Default

no apn

Parameters

apn-name

a character string up to a maximum of 100 characters

authentication

Syntax

authentication {**pap** | **chap**}

no authentication

Context

config>system>cellular>pdn-profile

Description

This command configures the authentication type used by the PDN profile.

The **no** form of this command removes authentication from the PDN profile.

Default

n/a

Parameters

pap

sets the authentication type to PAP

chap

sets the authentication type to CHAP

password

Syntax

password *password* [**hash** | **hash2** | **custom**]

no password

Context

config>system>cellular>pdn-profile

Description

This command configures the password for PAP or CHAP authentication of the PDN profile. The password must be confirmed by entering it twice.

The **no** form of this command removes the authentication password from the PDN profile.

Default

no password

Parameters

password

a character string up to a maximum of 64 characters

hash

specifies that the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

hash2

specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone. This means that a hash2 encrypted variable cannot be copied and pasted. If the hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

custom

specifies the custom encryption to management interface

protocol

Syntax

protocol {**ipv4** | **ipv6**}

Context

config>system>cellular>pdn-profile

Description

This command configures the address type, either IPv4 or IPv6, that is learned by the PDN router interface during the PDN attachment process. When set to IPv4, the PDN router interface can operate in static cellular system mode, static cellular interface mode, or dynamic cellular interface mode. When set to IPv6, the PDN router interface can operate in either static cellular interface mode or dynamic cellular interface mode. For more information about the PDN router interface modes, see "PDN router interfaces" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

Default

ipv4

Parameters

ipv4

sets the IP address type for the PDN connection to IPv4

ipv6

sets the IP address type for the PDN connection to IPv6

username

Syntax

username *user-name*

no username

Context

config>system>cellular>pdn-profile

Description

This command configures the username for PAP or CHAP authentication of the PDN profile.

The **no** form of this command removes the username.

Default

n/a

Parameters

user-name

a character string up to a maximum of 255 characters

7.1.2.4 Ethernet configuration commands

duplex

Syntax

duplex {**full** | **half**}

Context

config>port>ethernet

Description

This command configures the duplex mode of a Fast Ethernet port when autonegotiation is disabled. If the port is configured to **autonegotiate**, this parameter is ignored.

The 7705 SAR-Hm only supports full-duplex mode.

Default

full

Parameters

full

sets the link to full-duplex mode

half

sets the link to half duplex mode

7.1.2.5 GNSS receiver configuration commands

constellation

Syntax

constellation {**gps** | **gps-glonass**}

Context

config>card>mda>gnss

Description

This command configures which GNSS system or systems will be used by the GNSS receiver. The configuration can be modified only when the GNSS service is shut down.

Default

gps

Parameters

gps

configures the GNSS receiver to use the American GPS GNSS system

gps-glonass

configures the GNSS receiver to use both the American GPS GNSS system and the Russian GLONASS GNSS system

nmea

Syntax

nmea

Context

config>card>mda>gnss

Description

This command enables the context for configuring NMEA parameters.

sentence-types

Syntax

sentence-types *sentence-type* [*sentence-type*...(**up to 4 max**)]

Context

config>card>mda>gnss>nmea

Description

This command configures NMEA sentence types that are sent from the GNSS receiver over the associated IP transport service when the service is configured for NMEA streaming. The following sentence types are supported: GGA, RMC, VTG, and GNS. For information about the sentence types, see NMEA 0183, *Standard For Interfacing Marine Electronic Devices*.

At least one sentence type must be specified, up to a maximum of four. Different sentence types can be specified concurrently so that multiple sentences can be streamed per NMEA sentence interval.

Default

gga

Parameters

sentence-type

an NMEA sentence type to be streamed

Values **gga** — this sentence is for time, position, and fix-related data for a GNSS receiver

rmc — this sentence is for time, date, position, course, and speed data provided by the GNSS receiver

vtg — this sentence is for vector track and speed relative to the ground

gns — this sentence is for time, position, and fix-related data for single or combined constellations for a GNSS receiver.

sentence-interval

Syntax

sentence-interval *interval*

Context

config>card>mda>gnss>nmea

Description

This command configures the intervals at which NMEA sentences are retrieved from the GNSS receiver and sent over the associated IP transport service configured for NMEA streaming.

Default

5 s

Parameters

interval

time, in seconds, between the sending of NMEA sentences

Values 1 to 3600

shutdown

Syntax

[**no**] **shutdown**

Context

config>card>mda>gnss>nmea

Description

This command enables or disables NMEA streaming from the GNSS receiver. The **no** form of the command enables NMEA streaming. Using the **shutdown** command disables NMEA streaming.

The node uses an IP transport service to send NMEA sentences from the GNSS receiver to remote hosts. For information about enabling IP transport for NMEA sentences, see "GNSS NMEA data IP transport service" in the *7705 SAR-Hm and SAR-Hmc Main Configuration Guide*.

Default

shutdown

shutdown

Syntax

[**no**] **shutdown**

Context

config>card>mda>gnss

Description

This command enables or disables the GNSS service on the GNSS receiver. Enabling the GNSS receiver causes MDA 1/1 to reset under the following conditions:

- when the configuration of the **constellation** command changes
- the first time the GNSS receiver is enabled after a firmware update of the cellular MDA

The **no** form of the command enables the GNSS service. Using the **shutdown** command disables the GNSS receiver and resets the position fix and associated information.

Default

shutdown

7.1.2.6 Serial interface configuration commands

serial

Syntax
serial

Context
config>port

Description
This command enables the context to configure parameters for an RS-232 serial port on the node.

Default
n/a

rs232

Syntax
rs232

Context
config>port>serial

Description
This command enables the context to configure RS-232 parameters for a serial port.

Default
n/a

character-length

Syntax
character-length {**6** | **7** | **8**}

Context
config>port>serial>rs232

Description

This command configures the number of data bits used to transmit a character. The value for this command cannot be 8 if the value for parity is anything other than no parity (that is, anything other than none) and the value for stop-bits is 2.

Default

8

Parameters

6

specifies six bits in a character

7

specifies seven bits in a character

8

specifies eight bits in a character

control-lead

Syntax

control-lead {**input** | **output**}

Context

config>port>serial>rs232

Description

This command enables access to the context to configure the input and output leads that carry control signals. Control signals provide the handshaking for call setup, teardown, and synchronization.

Default

n/a

input

Syntax

input

Context

config>port>serial>rs232>control-lead

Description

This command enables access to the context to configure the input control leads.

Default

n/a

dtr-dsr

Syntax

dtr-dsr {**high** | **low**}

Context

config>port>serial>rs232>control-lead>input

Description

This command configures the Data Terminal Ready (DTR) or Data Set Ready (DSR) input control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE where the input signal is DTR.

Default

high

Parameters

high

the input control lead is assumed to be on

low

the input control lead is assumed to be off

rts-dcd

Syntax

rts-dcd {**high** | **low**}

Context

config>port>serial>rs232>control-lead>input

Description

This command configures the Request To Send (RTS) or Data Carrier Detect (DCD) input control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE device where the input signal is RTS.

Default

high

Parameters

high

the input control lead is assumed to be on

monitor

Syntax

monitor

Context

config>port>serial>rs232>control-lead

Description

This command enables access to the context to monitor the input control leads. When monitoring is enabled on a control lead, the node polls the status of the control lead every second. Any change in state of the control lead causes an alarm to be raised. This functionality provides an indication to the operator of a problem in the DTE-to-DCE path; for example, it can indicate that the far-end device is disconnected.

Monitoring is enabled on a per-lead basis.

Default

n/a

dtr-dsr

Syntax

dtr-dsr {**on** | **off**}

Context

config>port>serial>rs232>control-lead>monitor

Description

This command enables monitoring on the Data Terminal Ready (DTR) or Data Set Ready (DSR) input control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE device where the input control lead is DTR.

Default

off

Parameters

on

monitoring is enabled on the lead

off

monitoring is disabled on the lead

rts-dcd

Syntax

rts-dcd {**on** | **off**}

Context

config>port>serial>rs232>control-lead>monitor

Description

This command enables monitoring on the Request To Send (RTS) or Data Carrier Detect (DCD) input control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE device where the input control lead is RTS.

Default

off

Parameters

on

monitoring is enabled on the lead

off

monitoring is disabled on the lead

output

Syntax

output

Context

config>port>serial>rs232>control-lead

Description

This command enables access to the context to configure the output control leads.

Default

n/a

cts-alb

Syntax

cts-alb {**high** | **low**}

Context

config>port>serial>rs232>control-lead>output

Description

This command configures the Clear To Send (CTS) or Analog Loopback (ALB) output control lead. The 7705 SAR-Hm series router acts as a DCE device where the output signal is CTS.

Default

high

Parameters

high

the output control lead is forced on

low

the output control lead is forced off

dcd-rts

Syntax

dcd-rts {**high** | **low**}

Context

config>port>serial>rs232>control-lead>output

Description

This command configures the Data Carrier Detect (DCD) or Request To Send (RTS) output control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE device where the output signal is DCD.

Default

high

Parameters

high

the output control lead is forced on

low

the output control lead is forced off

ri-rdl

Syntax

ri-rdl {**high** | **low**}

Context

config>port>serial>rs232>control-lead>output

Description

This command configures the Ring Indicator (RI) or Remote Digital Loopback (RDL) output control lead. This command is only supported on the 7705 SAR-Hm that acts as a DCE device where the output signal is RI.

Default

high

Parameters

high

the output control lead is forced on

low

the output control lead is forced off

hold-time

Syntax

hold-time {[**up** *hold-time-up*] [**down** *hold-time-down*]}

no hold-time

Context

config>port>serial>rs232

Description

This command configures the serial link dampening timers in 100s of milliseconds, which guards against reporting excessive interface transitions. When implemented, subsequent transitions of the interface from one state to another are not advertised to upper layer protocols until the configured timer has expired.

Default

no hold-time

Parameters

hold-time-up

the hold-timer for link-up event dampening. A value of zero (0) indicates that an up transition is reported immediately.

Values 0 to 100 (in 100s of milliseconds)

hold-time-down

the hold-timer for link-down event dampening. A value of zero (0) indicates that a down transition is reported immediately.

Values 0 to 100 (in 100s of milliseconds)

loopback

Syntax

loopback bidir-e

no loopback

Context

config>port>serial>rs232

Description

This command puts the specified interface into a loopback mode. The corresponding interface must be in a shutdown state in order for the loopback mode to be enabled.

In the serial context, it is possible to configure a a bidirectional loopback E. A bidirectional loopback is a circuit loopback that loops traffic from the line back to the line. Bidirectional loopback E takes place on the data device side of the adapter card, and is closer to the line.

This command is not saved in the system configuration between boots.

The **no** form of this command disables the loopback on the interface.

Default

no loopback

Parameters

bidir-e

configures a bidirectional loopback E

parity

Syntax

parity {**odd** | **even** | **mark** | **space**}

no parity

Context

config>port>serial>rs232

Description

This command configures the parity bit in a character. Parity is an error detection method that adds an extra bit to each character, based on the number of 0s or 1s in the character.

The value for this command must be **no parity** (that is, none) if the character-length value is 8 and the stop-bits value is 2.

The **no** form of this command disables the parity bit in a character.

Default

no parity

Parameters

odd

the parity bit is set to 0 or 1 to make the total number of 1s in the set of bits odd

even

the parity bit is set to 0 or 1 to make the total number of 1s in the set of bits even

mark

the parity bit is present but not used and is always set to 1

space

the parity bit is present but not used and is always set to 0

speed

Syntax

speed {**600** | **1200** | **2400** | **4800** | **9600** | **19200** | **38400** | **57600** | **115200**}

Context

config>port>serial>rs232

Description

This command configures the speed of the interface. The speed also determines the DS0 timeslots assigned to the channel group.

Default

9600

Parameters

600

sets the link speed to 600 b/s

1200
sets the link speed to 1200 b/s

2400
sets the link speed to 2400 b/s

4800
sets the link speed to 4800 b/s

9600
sets the link speed to 9600 b/s

19200
sets the link speed to 19 200 b/s

38400
sets the link speed to 38 400 b/s

57600
sets the link speed to 57 600 b/s

115200
sets the link speed to 115 200 b/s

stop-bits

Syntax

stop-bits {**1** | **2**}

Context

config>port>serial>rs232

Description

This command configures the number of stop bits used to signify the end of a character.

This command cannot have a value of 2 if the character-length value is 8 and the parity value is anything other than **no parity** (that is, anything other than none).

Default

1

Parameters

1
specifies one stop bit in a character

2
specifies two stop bits in a character

7.1.2.7 Raw socket configuration commands

7.1.2.7.1 Raw socket port configuration commands

Note: The speed command must be set to a value that supports raw sockets; see Serial interface configuration commands for the required information.

socket

Syntax

socket

Context

config>port>serial>rs232

Description

This command creates a raw socket on an RS-232 port.

The **no** form of the command deletes the socket from the serial port.

Default

n/a

rx

Syntax

rx

Context

config>port>serial>rs232>socket

Description

This command enables the context to configure parameters for data packets received over a serial port's raw socket.

Default

n/a

eop

Syntax

eop

Context

config>port>serial>rs232>socket>rx

Description

This command enables the context to configure end of packet (EOP) parameters for data packets received over the raw socket.

Note: An EOP is declared by whichever EOP condition is encountered first.

idle-timeout

Syntax

idle-timeout *milliseconds*

Context

config>port>serial>rs232>socket>rx>eop

Description

This command specifies how long a serial port can remain idle before an EOP is declared and the packet is sent over the raw socket.

Default

50 ms

Parameters

milliseconds

the length of time, in milliseconds, that a serial port can remain idle before an EOP is declared

Values 10 to 5000

length

Syntax

length *bytes*

Context

config>port>serial>rs232>socket>rx>eop

Description

This command specifies the number of characters (converted to bytes) received on the serial port that triggers the node to encapsulate the characters in an IP transport packet and send it over a VPRN service.

Default

1500

Parameters

bytes

the number of characters (in bytes) to trigger sending an IP transport packet

Values 1 to 1500

special-char

Syntax

special-char *value*

no special-char

Context

config>port>serial>rs232>socket>rx>eop

Description

This command specifies a special character that, if received on the serial port, declares EOP and triggers the node to encapsulate previously received queued characters in an IP transport packet and send it over a VPRN service.

Note: Other than declaring the EOP, the special character is otherwise treated as regular data; that is, it is added to the packet.

The **no** form of the command disables checking for a special character.

Default

no special-char

Parameters

value

specifies the special character, in a decimal or hexadecimal format, that triggers end of packet

Values 0 to 255, or 0x00 to 0xFF

squelch-delay

Syntax

squelch-delay *seconds*

no squelch-delay

Context

config>port>serial>rs232>socket>rx

Description

This command specifies how long a serial port can receive a continuous data stream before an alarm is raised indicating that the serial port has locked up and triggering the squelching function.

The **no** form of the command disables the squelching function on the serial port.

Default

no squelch-delay

Parameters

seconds

the number of seconds that a serial port can receive data before the squelching function is triggered

Values 1 to 120

squelch-reset

Syntax

squelch-reset

Context

config>port>serial>rs232>socket>rx

Description

This command allows an operator to manually clear squelching on a serial port's raw socket without having to configure a time limit on the squelching function.

Squelching can also be set to clear automatically after a time limit has been reached with the unsquelch-delay command.

Default

n/a

unsquelch-delay

Syntax

unsquelch-delay *seconds*

no unsquelch-delay

Context

config>port>serial>rs232>socket>rx

Description

This command clears squelching on a raw socket by setting a limit on the amount of time that squelching can remain active on the port. When the time limit is reached, the auto-clear function is enabled and the serial port's raw socket is put back into a normal state.

Squelching can also be cleared manually with the squelch-reset command.

The **no** form of the command disables the auto-clear function on a serial port.

Default

no unsquelch-delay

Parameters

seconds

the number of seconds before the auto-clear function is activated

Values 1 to 120

tx

Syntax

tx

Context

config>port>serial>rs232>socket

Description

This command enables the context to configure parameters for data packets transmitted over a serial port's raw socket.

inter-session-delay

Syntax

inter-session-delay *milliseconds*

Context

config>port>serial>rs232>socket>tx

Description

This command specifies a time delay that the node inserts between a session's data that is being transmitted over a serial port and the next queued session's data. The next session's data is not sent until the current session's data is sent and the **inter-session-delay** is reached.

Default

10 ms

Parameters

milliseconds

the time delay, in milliseconds, between a session's data that is being transmitted over a serial port and the next queued session's data

Values 0 to 5000

7.1.2.8 WLAN MDA radio configuration commands

wlan-radio

Syntax

wlan-radio

Context

config>card>mda

Description

This command enables the context to configure WLAN radio commands.

Default

n/a

bandwidth

Syntax

bandwidth {**20MHz** | **40MHz**}

Context

config>card>mda>wlan-radio

Description

This command sets the channel bandwidth of the WLAN radio.

Default

20MHz

Parameters

20MHz

sets the channel bandwidth to 20 MHz

40MHz

sets the channel bandwidth to 40 MHz

beacon-interval

Syntax

beacon-interval *milliseconds*

Context

config>card>mda>wlan-radio

Description

This command sets the beacon interval for the WLAN radio. The interval is the frequency with which an AP broadcasts a packet in order to synchronize with the wireless network.

Default

200

Parameters

milliseconds

the interval at which an AP broadcasts a packet that is used to synchronize with the wireless network

Values 75 to 999

channel

Syntax

channel {**auto** | *channel-id*}

Context

config>card>mda>wlan-radio

Description

This command sets the channel of the WLAN radio. The *channel-id* values that are available for this command depend on the configured **country** and **frequency-band**. See the Appendix for the available values.

When the WLAN radio channel is set to **auto**, the node scans the frequency bands supported by the configured **county** for the most appropriate channel.

Default

auto

Parameters

auto

specifies that the WLAN radio selects the most appropriate channel

channel-id

see the Appendix

country

Syntax

[**no**] **country** *country-string*

Context

config>card>mda>wlan-radio

Description

This command configures the country name for the WLAN radio. Because the values configured for the **channel** and **bandwidth** commands depend on the **country** configuration, the country name must be configured before any other MDA parameters. The country name must be configured in order to enable the radio; otherwise, executing a **no shutdown** command returns an error.

The **no** form of the command removes the specified country from the WLAN radio and resets the MDA **frequency-band**, **channel**, and **bandwidth** commands to their default values. The **no** form can only be executed when the WLAN radio is shut down.

Default

n/a

Parameters

country-string

the name of the country

Values australia, belgium, bolivia, brazil, canada, chile, colombia, france, germany, india, iran, italy, japan, malaysia, mexico, new-zealand, peru, russia, singapore, south-africa, usa, venezuela

frequency-band

Syntax

frequency-band {**2400** | **5000**}

Context

config>card>mda>wlan-radio

Description

This command sets the frequency band for the WLAN radio.

Default

2400

Parameters

2400

sets the frequency band to 2.4 GHz

5000

sets the frequency band to 5.0 GHz

shutdown

Syntax

[**no**] **shutdown**

Context

config>card>mda

config>card>mda>wlan-radio

Description

In the **config>card>mda>wlan-radio** context, this command shuts down the WLAN radio. When the radio is turned off, a configured AP or station becomes operationally down. The **no** form of this command enables the WLAN radio, and any configured WLAN ports that are operationally down can begin operating.

In the **config>card>mda** context, this command shuts down the WLAN MDA and puts the WLAN radio into reset mode. Any WLAN ports configured under the MDA become operationally down. The **no** form of this command brings the WLAN radio out of reset.

Default

shutdown

7.1.2.9 WLAN port configuration commands

port

Syntax

port *port-id*

Context

config

Description

This command configures a WLAN port. The WLAN port identifiers for the WLAN MDA are fixed and represent either an access point (AP) or the station, with the following configuration:

- port 1/4/1 is always AP 1
- port 1/4/2 is always AP 2
- port 1/4/3 is always AP 3
- port 1/4/4 is always station 1

Default

n/a

Parameters

port-id

specifies the physical port ID in the format *slot/mda/port*, where the slot ID is always 1, the MDA is always 4, and the port ID is 1 to 4

description

Syntax

description *description-string*

no description

Context

config>port

Description

This command creates a text description for a configuration context to help identify the content in the configuration file.

The **no** form of this command removes any description string from the context.

Default

n/a

Parameters

description-string

description character string. Allowed values are any string up to 80 or 160 characters long (depending on the command) composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $,or spaces), the entire string must be enclosed within double quotes.

shutdown

Syntax

[**no**] **shutdown**

Context

config>port

Description

This command administratively disables the specified WLAN port. When disabled, no configurations can be changed or removed and no statistics can be reset. The operational state of the port is also disabled.

When a WLAN AP on the node is shut down, the following occurs.

- All WLAN clients connected to the AP are released.
- If the AP is configured as a SAP toward the WLAN gateway, the SAP and associated service become operationally down.

When the WLAN station on the node is shut down, the following occurs.

- The station disconnects from the AP it was connected to.
- The station stops trying to connect to the networks in its network list.
- If any WLAN APs are configured on the node and they are not shut down, they will stay up and continue using the channel that was in use before the shutdown of the station.

Issuing the **no shutdown** command enables the specified port when the WLAN MDA is also enabled.

When the WLAN station port is enabled, the following occurs.

- The WLAN APs on the node that were operationally up go down and only come back up when the station connects to a remote AP. The channel selected by the station is then used by the WLAN APs.
- The station scans for an available network from its list of candidate networks.
- When it connects to a valid network, the AP on the node will also use the channel that was used to connect the station (when the **channel** command is set to auto).

The **no** form of this command administratively enables the specified port.

Default

shutdown

wlan

Syntax

wlan

Context

config>port

Description

This command enables the context to configure WLAN port parameters.

Default

n/a

access-point

Syntax

access-point

Context

config>port>wlan

Description

This command enables the context to configure WLAN AP port parameters.

broadcast-ssid

Syntax

[**no**] **broadcast-ssid**

Context

config>port>wlan>access-point

Description

This command enables a WLAN AP to broadcast the network SSID.

The **no** form of the command disables the broadcast of the network SSID.

Default

no broadcast-ssid

client-limit

Syntax

client-limit *clients*

Context

config>port>wlan>access-point

Description

This command configures the maximum number of clients that can connect to a WLAN AP concurrently.

Default

24

Parameters

clients

the number of concurrent clients that can connect to a WLAN AP

Values 1 to 24

client-timeout

Syntax

client-timeout *seconds*

Context

config>port>wlan>access-point

Description

This command configures the timeout period for inactive clients. If a client does not send or receive data over the WLAN connection within the specified period, the client is disconnected from the WLAN AP.

Default

300

Parameters

seconds

the length of time, in seconds, that a WLAN AP waits before disconnecting an inactive client

Values 60 (1 minute) to 86400 (24 hours)

shutdown

Syntax

[**no**] **shutdown**

Context

config>port>wlan>access-point>dhcp

Description

This command disables the DHCP relay function for a WLAN AP.

The **no** form of the command enables the DHCP relay function on an AP. When a DHCP request is received by a client trying to connect to the AP, the node inserts Option 82 with specific information needed to connect to the WLAN gateway. If an Option 82 sub-option is already present in the DHCP request, it is replaced with the version expected by the WLAN gateway.

Default

shutdown

dot1x

Syntax

dot1x

Context

config>port>wlan>access-point

Description

This command enables the context to configure dot1X parameters for a WLAN AP port.

radius-plcy

Syntax

radius-plcy *policy-name*

no radius-plcy

Context

config>port>wlan>access-point>dot1x

Description

This command specifies a RADIUS policy for a WLAN AP to use when network WLAN security is set to **wpa2-enterprise**.

The RADIUS policy name must have already been configured under the **config>system>security>dot1x** context before executing this command. For information about configuring a RADIUS policy name, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

The **no** form of the command clears the RADIUS policy name from a WLAN AP port.

Default

n/a

Parameters

policy-name

the RADIUS policy to use for a WLAN AP

re-auth-period

Syntax

re-auth-period *seconds*

Context

config>port>wlan>access-point>dot1x

Description

This command configures the reauthentication period when network LAN security for a WLAN AP is set to **wpa2-enterprise**. Clients that are connected to the WLAN AP must reauthenticate after the reauthentication period expires.

Default

300

Parameters

seconds

the intervals at which clients that are connected to a WLAN AP must reauthenticate

Values 1 to 9000

mode

Syntax

mode {**access** | **network**}

Context

config>port>wlan

Description

This command sets the mode of a WLAN port to access or network. All WLAN ports can operate either as access ports or network ports. By default, WLAN ports 1/4/1 to 1/4/3 operate in access mode and WLAN port 1/4/4 operates in network mode.

Default

access for WLAN ports 1/4/1 to 1/4/3, network for WLAN port 1/4/4

Parameters

access

sets the WLAN port mode to access

network

sets the WLAN port mode to network

network

Syntax

network *network-id* **ssid** *ssid-name* [**create**]

no network

Context

config>port>wlan

Description

This command configures the network identifier and the network service set identifier (SSID). The network SSID can be changed only when the WLAN port is shut down.

The SSID defines the name of the WLAN network. The WLAN AP ports use this name to allow WLAN clients to connect to their offered WLAN network.

The WLAN station port uses the network ID and associated SSID to connect to a remote AP. Up to 10 network numbers and associated SSID can be configured for the WLAN station port; however, only one network can be active and connected to the station at a time.

Operators must configure security parameters for each network SSID specified.

The **no** form of this command removes the network and all the configurations within the network context.

Default

n/a

Parameters

network-id

the network identifier, from 1 to 10

ssid-name

a 32-character string that defines the SSID

create

keyword used to create the network SSID

wlan-security

Syntax

wlan-security [**type** {**wpa2-psk** | **wpa2-enterprise**}]

no wlan-security

Context

config>port>wlan>network

Description

This command configures the network security type for the specified WLAN interface.

When no security type is set, the WLAN interface is considered to be open. When the security type is set to **wpa2-psk**, the WPA2-PSK passphrase must be configured.

When a WLAN AP port is configured for WPA2-Enterprise security, operators must configure a RADIUS policy under the **config>system>security>dot1x** context in the CLI. For information about configuring a RADIUS policy in this context, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The dot1x RADIUS policy ID used to configure the RADIUS policy is then configured on the WLAN AP port using the **config>port>wlan>access-point>dot1x>radius-plcy** command, in order to authenticate clients connecting to the WLAN AP.

When the WLAN station port is configured for WPA2-Enterprise security, operators must configure the authentication type as one of EAP-TTLS, EAP-FAST, or EAP-PEAP using the **authentication** command.

The **no** form of the command disables security and the WLAN interface is considered to be open.

Default

no wlan-security

Parameters

type

keyword used to select the security type

wpa2-psk

the WLAN interface uses WPA2-PSK security

wpa2-enterprise

the WLAN interface uses WPA2-Enterprise security

wpa-encryption

Syntax

wpa-encryption [**tkip** | **aes**]

no wpa-encryption

Context

config>port>wlan>network>wlan-security

Description

This command sets the WPA2 encryption type when network WLAN security is configured as either **wpa2-psk** or **wpa2-enterprise**.

When WLAN security is set to either **wpa2-psk** or **wpa2-enterprise**, the encryption type defaults to **aes**.

The **no** form of the command removes the configured encryption type.

Default

aes

Parameters

tkip

sets the encryption type to TKIP

aes

sets the encryption type to AES

wpa-passphrase

Syntax

wpa-passphrase *ascii-passphrase* [**hash** | **hash2**]

no wpa-passphrase

Context

config>port>wlan>network>wlan-security

Description

This command configures the WPA2-PSK passphrase when network WLAN security is configured as **wpa2-psk**. The passphrase is a pre-shared alphanumeric string that is used to connect potential clients to an AP on the node.

The **no** form of the command clears the passphrase. The default setting is the string **passphrase**.

Default

passphrase

Parameters

ascii-passphrase

a 63-character alphanumeric string that identifies the passphrase to use for WPA2-PSK security

hash

specifies that the hash key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

hash2

specifies that the hash key is entered in a more complex, encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

station

Syntax

station

Context

config>port>wlan>network>wlan-security

Description

This command enters the context to configure WLAN station port parameters.

Default

n/a

authentication

Syntax

authentication {**eap-ttls** | **eap-fast** | **eap-peap**}

no authentication

Context

config>port>wlan>network>wlan-security>station

Description

This command configures the type of network authentication to be used by the WLAN station when the **wlan-security** parameter is set to **WPA2-enterprise**.

Default

none

Parameters

eap-ttls

sets the authentication type for the WLAN station to EAP-TTLS

eap-fast

sets the authentication type for the WLAN station to EAP-FAST

eap-peap

sets the authentication type for the WLAN station to EAP-PEAP

password

Syntax

password *password-string* [**hash** | **hash2**]

no password

Context

config>port>wlan>network>wlan-security>station

Description

This command configures the password that the station uses to access the network when the authentication method requires a password.

Default

n/a

Parameters

password-string

the password to be authenticated

hash

specifies that the hash key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

hash2

specifies that the hash key is entered in a more complex, encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the specified **hash** or **hash2** parameter.

username

Syntax

username *username-string*

no username

Context

config>port>wlan>network>wlan-security>station

Description

This command configures the name that the station uses to access the network when the authentication method requires a username.

Default

n/a

Parameters

username-string

the username to be authenticated, up to 64 characters

7.2 Show, clear, and tools commands

Note: The commands described in this section apply specifically to 7705 SAR-Hm series nodes. All other applicable commands supported on the nodes are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* and the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*.

7.2.1 Command hierarchies

- Show commands
- Clear commands
- Tools commands

7.2.1.1 Show commands

7.2.1.1.1 Cellular MDA commands

```
show
    - mda port-id [detail]
```

7.2.1.1.2 Cellular port commands

```
show
    - port port-id [detail]
```

7.2.1.1.3 GNSS receiver commands

```
show
    - mda 1/1
        - gnss
```

7.2.1.1.4 Serial and raw socket commands

```
show
    - port 1/3/1
```

7.2.1.1.5 WLAN radio commands

```
show
    - mda 1/4 [detail]
    - port port-id [statistics] [detail]
```

7.2.1.2 Clear commands

7.2.1.2.1 Cellular port commands

```
clear
    - port port-id statistics
```

7.2.1.2.2 Socket statistics commands

```
clear
    - port 1/3/1 statistics
```

7.2.1.2.3 WLAN statistics commands

```
clear
    - port port-id statistics
```

7.2.1.3 Tools commands

7.2.1.3.1 Tools perform commands

```
tools
    - perform
        - auto-boot {complete | retry | terminate}
        - [no] auto-boot echo [debugger]
```

```
tools
    - perform
        - cellular
            - diag-port-access listening-port tcp-port start
            - diag-port-access stop
```

```
tools
    - perform
        - mda 1/1
            - cellular
                - at-command at-command
                - force-sim-switch
                - sim {1 | 2}
                    - change-pin
                    - lock-sim
                    - unblock-sim
                    - unlock-sim
                - update-firmware firmware-file
                - update-firmware firmware-file sim 1 | 2
        - mda 1/4
```

```
            - wlan
                - scan
```

```
tools
    - perform
        - port 1/1/{1 | 2}
            - cellular
                - cbsd-authorization
                    - reset
```

7.2.1.3.2 Tools dump commands

```
tools
    - dump
        - cellular
            - diag-port-access
                - status
```

```
tools
    - dump
        - port 1/1/{1 | 2}
            - cellular
                - cbsd-authorization [clear]
        - mda 1/4
            - wlan
                - last-scan-result
```

7.2.2 Command descriptions

- Show commands
- Clear commands
- Tools commands

7.2.2.1 Show commands

- Show cellular MDA commands
- Show cellular port commands
- Show GNSS receiver commands
- Show serial and raw socket commands
- Show WLAN radio commands

Note: The command outputs shown in this section are examples only; actual displays may differ depending on supported functionality and user configuration.

7.2.2.1.1 Show cellular MDA commands

mda

Syntax

mda *mda-id* [**detail**]

Context

show

Description

This command displays information about the cellular MDA.

When a **band-list** is configured, the output shows the following information:

- the bands that are supported globally on the MDA and whether 3G is available
- the bands that are supported by the firmware on the active SIM and whether 3G is included
- the list of bands configured for each SIM
- whether a configured band list on the active SIM is in use. If only a subset of bands on the list is supported by the firmware on the active SIM, the field shows only those bands.

The Band list in-use field shows the "all bands enabled by fw" message when:

- there is no band list configured
- a band list is configured with bands that are valid for the MDA but are not supported by the current firmware
- none of the bands on the band list are supported by the firmware on the active SIM

Parameters

mda-id

the identifier for the cellular MDA

Values 1/1

Output

The following output is an example of cellular MDA information.

Output example

```
*A:Dut-A# show mda 1/1 detail
===============================================================================
MDA 1/1 detail
===============================================================================
Slot  Mda   Provisioned Type                          Admin     Operational
               Equipped Type (if different)           State     State
-------------------------------------------------------------------------------
1     1     i2-cellular                               up        up
MDA Specific Data
```

```
    Maximum port/connector count  : 2
    Num ports/connectors equipped : 2
    Capabilities                  : Wireless, Cellular
    Fail On Error                 : Disabled
Hardware Data
    Platform type                 : 7705
    Part number                   : 3HE11600AAAA0125
    CLEI code                     : INM2100DRA
    Serial number                 : NS215062172
    Manufacture date              : 12182021
    Manufacturing deviations      : D04829
    Manufacturing assembly number :
    Administrative state          : up
    Operational state             : up
    Temperature                   : 35C
    Temperature threshold         : 75C
    Over-temperature status       : ok
    Software boot (rom) version   : (Not Specified)
    Software version              : (Not Specified)
    Time of last boot             : 2022/10/05 11:29:32
    Current alarm state           : alarm cleared
    Base MAC address              : f8:ba:e6:bc:39:44
    Firmware version              : ATT 02.32.11.00 002.070_005
Cellular MDA Information
    Configured active SIM card    : SIM 1
    Actual active SIM card        : SIM 1
    Automatic SIM switch status   : N/A
    SIM 1 firmware                : ATT 02.32.11.00 002.070_005
    SIM 2 firmware                : GENERIC 02.38.00.00 002.082_000
    No service reset interval     : disabled
    No service reset status       : N/A
    Bands supported on MDA        : b1 b2 b3 b4 b5 b7 b8 b12 b13 b20 b25 b26
                                    b29 b30 b41 3g
    Bands enabled by active fw    : b1 b2 b3 b4 b5 b7 b8 b12 b13 b20 b25 b26
                                    b29 b30 b41 3g
    Band list in-use              : b2 b5 b12
    SIM card number               : 1
        Band list configured      : b2 b5 b12
        RSSI threshold            : none
        RSSI alarm wait time      : 60 seconds
        Failure criteria          : port
        Failure duration          : 5 minutes
    SIM card number               : 2
        Band list configured      : none
        RSSI threshold            : none
        RSSI alarm wait time      : 60 seconds
        Failure criteria          : port
        Failure duration          : 5 minutes
===============================================================================
```

7.2.2.1.2 Show cellular port commands

port

Syntax

port *port-id* [**detail**]

Context

show

Description

This command displays operational state information for a cellular port, including information for the cellular PDN interface, the installed SIM, and the packet data network (PDN). It also displays port statistics.

The CBSD information is available only for the 7705 SAR-Hmc NA variant (3HE12472AA), the 7705 SAR-Hmc NA variant 2 (3HE12473AA), and 7705 SAR-Hmc World variant (3HE12478AA) when the PDN router interface is configured to operate as a CBSD.

Parameters

port-id

the identifier for the cellular port

Values 1/1/1 or 1/1/2

Output

The following output is an example of cellular interface information.

Output example

```
*A:Dut-A# show port 1/1/1 detail
===============================================================================
Cellular PDN Interface
===============================================================================
Description       : Cellular
Interface         : 1/1/1               IfIndex           : 35684352
Admin State       : up                  Oper State        : up
State Change Count: 1
IMEI              : 35-241842-015157-1
Sync System Time  : Disabled
Network Status    : registered-home      Radio Mode        : lte
Band              : 48                  Channel           : 55990
RSSI              : >= -51 dBm          RSRP              : -52 dBm
RSRQ              : >= -3 dB            SINR              : +30.0 dB
Tracking Area Code: 0001                Cell Identity     : 01a2d001
-------------------------------------------------------------------------------
SIM Card 1
-------------------------------------------------------------------------------
Description       : (Not Specified)
Specified Firmware: GENERIC 01.14.03.00 002.036_001
Equipped          : yes
Locked            : no                  PIN status        : ready
PIN retries left  : 3                   PUK retries left  : 10
ICCID             : 8988211000000484017  IMSI              : 001001000048401
-------------------------------------------------------------------------------
Packet Data Network
-------------------------------------------------------------------------------
PDN Profile       : 1                   Protocol          : IPv4
Configured APN    : internet
PDN State         : connected
IP Address        : 10.30.28.11
Primary DNS       : 8.8.8.8
Secondary DNS     : 8.8.4.4
IP MTU            : 1500
APN               : internet
```

```
-------------------------------------------------------------------------------
CBSD
-------------------------------------------------------------------------------
Admin State             : enabled
Oper State              : up
User ID                 : V8User5
Antenna Gain            : 7 dBm
Category                : A
Client TLS              : sas_harness_client_tls_profile
Primary SAS Server      : https://10.0.4.102:8080/v1.2
Secondary SAS Server    :
SAS Server in Use       : primary
SAS Server IP           : 10.0.4.102
FCC ID                  : AS57705SARHMC-2A
CBSD ID                 : 1004
Grant ID                : 2006
Registration State      : registered
Grant State             : authorized
Grant Expiry Time       : 2022/09/18 05:03:30 UTC
Tx Expiry Time          : 2022/09/17 05:03:31 UTC
Heartbeat Interval      : 60 seconds
Channel Type            : pal
-------------------------------------------------------------------------------
CBSD Statistics
-------------------------------------------------------------------------------
Type                Requests            Successes           Failures
-------------------------------------------------------------------------------
Registration        1                   1                   0
Grant               1                   1                   0
Heartbeat           1                   1                   0
-------------------------------------------------------------------------------
===============================================================================
===============================================================
Bearer Information
===============================================================
Bearer Id   Bearer Type   QCI   UL GBR   UL MBR   DL GBR   DL MBR
---------------------------------------------------------------
        5       default     9
===============================================================
===============================================================================
Port Statistics
===============================================================================
                                                    Input                 Output
-------------------------------------------------------------------------------
Packets                                               81                     99
Discards                                               0                      0
Unknown Proto Discards                                 0
===============================================================================

A:Dut-A#
```

7.2.2.1.3 Show GNSS receiver commands

```
gnss
```

Syntax

gnss

Context

show>mda

Description

This command displays detailed GNSS information, including position and satellite information.

If a GNSS fix is acquired and then subsequently lost by the node, the last known GNSS fix data continues to be displayed in the CLI. When a GNSS fix is reacquired, the GNSS data is updated to match the new fix.

The last GNSS fix data is not preserved after a **power-cycle**, **admin reboot**, **clear mda 1/1,** or **shutdown** command is issued for GNSS.

Output

The following output is an example of GNSS information.

Output example

```
*A:Dut-A#: show mda 1/1 gnss
===============================================================================
GNSS Information
===============================================================================
Admin State                       : Enabled
Oper State                        : Up
Satellite  Constellation          : gps-glonass
NMEA Sentence Streaming           : Enabled
  Sentences                       : gga rmc vtg gns
  Sentence Interval (seconds)     : 5
-------------------------------------------------------------------------------
Acquired Fix                      : Yes
Time                              : 2018/07/27 12:59:47 UTC
Position (degrees)                : 45.34810, -75.92147
Position (degrees minutes seconds) : 45 20'53.1"N, 75 55'17.2"W
Altitude above mean sea level     : 124.8 meters
Heading                           : 0.0 degrees
Speed                             : 0.0 kph
===============================================================================

========================================
Visible Satellites
========================================
   #    type  elevation  azimuth  SNR(dB)
----------------------------------------
   1     gps         22      158       43
   7     gps         73      229       53
   8     gps         64       54       57
   9     gps          8      209       44
  11     gps         48      165       49
  13     gps          9      324       40
  16     gps          2       90       40
  18     gps         38      135       54
  27     gps         27       50       49
  28     gps         29      284       46
  30     gps         52      296       51
  69 glonass          7      302       31
  70 glonass          4      352       43
  77 glonass         49      113       44
  78 glonass         68      343       53
  79 glonass         28      316       47
  81 glonass         18      199       42
  86 glonass          0       28       45
```

```
  87 glonass         54       43       44
  88 glonass         66      177       43
-------------------------------------------
No. of visible satellites: 20
===========================================
*A:Dut-A#
```

7.2.2.1.4 Show serial and raw socket commands

port

Syntax

port 1/3/1

Context

show

Description

This command displays serial and raw socket information.

Output

The following output is an example of serial and raw socket information.

Output example

```
*A:Dut# show port 1/3/1
===============================================================================
Serial RS-232 Interface
===============================================================================
Description        : RS-232 Serial
Interface          : 1/3/1                  Port IfIndex         : 39878656
Admin Status       : down                   Oper Status          : down
Physical Link      : no                     Mode                 : access
Device Mode        : asynchronous           Speed                : 9600
Character Length   : 8                      Parity               : none
Stop Bits          : 1
Device Gender      : dce                    Duplex               : full
Last State Change  : 07/17/2017 17:20:13
Loopback           : none
Hold time up       : 0 milliseconds
Hold time down     : 0 milliseconds
===========================================
Serial Control Leads
===========================================
Inputs          Cfg         Netw  Line  Mon
-------------------------------------------
dtr-dsr [DTR] : high              0     off
rts-dcd [RTS] : high              0     off
Outputs         Cfg         Netw  Line
-------------------------------------------
dcd-rts [DCD] : high              1
cts-alb [CTS] : high              1
ri-rdl  [RI]  : high              1
```

```
===============================================================================
===============================================================================
Serial Socket
===============================================================================
EOP Length         : 1500                    Squelch Delay        : Disabled
EOP Idle Timeout   : 50                      Unsquelch Delay      : Disabled
EOP Special Char   : Disabled                Inter-Session Delay  : 10
Squelch Status     : off
===============================================================================
============================================================
Socket Statistics
============================================================
                                                        Count
------------------------------------------------------------
Characters received                                         0
Characters transmitted                                      0
End of packet idle timeout                                  0
End of packet length                                        0
End of packet special character                             0
Ingress forwarded packets                                   0
Egress forwarded packets                                    0
Ingress dropped packets                                     0
Egress dropped packets                                      0
Squelch activated                                           0
============================================================
*A:Dut#
```

7.2.2.1.5 Show WLAN radio commands

mda

Syntax

mda 1/4 [**detail**]

Context

show

Description

This command displays WLAN radio MDA information.

Output

The following output is an example of WLAN radio MDA information.

Output example

```
*A:Dut# show mda 1/4 detail
===============================================================================
WLAN Radio Data
    Radio                       : 1
    Type                        : Wifi Dualband 2.4/5.0 GHz
    Administrative state        : up
    Operational state           : up
    Country                     : canada
```

```
    Beacon Interval               : 200 msecs
    Cfg.  Band/Channel/Width      : 2400 MHz/Ch.1/20 MHz
    Oper. Band/Channel/Width      : 2400 MHz/Ch.1/20 MHz
    Oper. Center Frequency        : 2412 MHz
===============================================================
*A:Dut#
```

port

Syntax

port *port-id* [**statistics**] [**detail**]

Context

show

Description

This command displays WLAN radio port statistics and RADIUS configuration information.

Parameters

port-id

specifies the physical port identifier in the format *slot/mda/port*, where *slot* is always 1, *mda* is always 4, and *port* is 1 to 4

statistics

shows ingress and egress statistics for the port

detail

shows more information about the WLAN port

Output

The following output is an example of WLAN radio port information.

Output example

```
*A:Dut# show port 1/4/1
===============================================================================
Wireless LAN Interface
===============================================================================
Description        : Wireless LAN
Interface          : 1/4/1                   Port IfIndex         : 41975808
Admin Status       : up                      Oper Status          : up
Oper Flags         :
Last State Change  : 05/14/2021 08:52:32

Hardware Address   : cc:66:b2:0a:dd:05

Mode               : WLAN Access Point

-------------------------------------------------------------------------------
RF Interface
-------------------------------------------------------------------------------
Frequency          : 2437 MHz
Band/Channel       : 2400 MHz/Ch.6           Channel Width        : 20 MHz
```

```
-------------------------------------------------------------------------------
Network Parameters
-------------------------------------------------------------------------------
SSID               : kansarhmrtb5
Security           : wpa2-psk
Passphrase         : **********
Encryption         : aes


SSID Broadcast     : enabled
Client Idle Timeout: 300 secs                Client Limit         : 24
DHCP Relay         : disabled                DHCP Action          : replace
Auth Radius Policy : N/A
  Re-Auth Period   : 3600 secs

-------------------------------------------------------------------------------
Connected Clients
-------------------------------------------------------------------------------
Client             Authorized                          Connect Time
-------------------------------------------------------------------------------
00:23:a7:f0:8f:8b  Yes                                 05/14/2021 08:54:35
-------------------------------------------------------------------------------
Count: 1 (Limit: 24)
-------------------------------------------------------------------------------

===============================================================================
=============================================================
Access Point Statistics
=============================================================
                                                        Count
-------------------------------------------------------------
Client attaches                                             1
Client detaches                                             0
Successful authentications                                  1
Failed authentications                                      0
=============================================================
===============================================================================
Port Statistics
===============================================================================
                                                   Input                Output
-------------------------------------------------------------------------------
Packets                                              2                     2
Discards                                             0                     0
Unknown Proto Discards                               0
===============================================================================
```

```
A:Dut-A>config>port# show port 1/4/4
===============================================================================
Wireless LAN Interface
===============================================================================
Description        : Wireless LAN
Interface          : 1/4/4                   Port IfIndex         : 42074112
Admin Status       : up                      Oper Status          : up
Oper Flags         :
Last State Change  : 05/14/2021 08:54:36

Hardware Address   : cc:66:b2:0a:da:1a

Mode               : WLAN Station

-------------------------------------------------------------------------------
RF Interface
```

```
-------------------------------------------------------------------------------
Frequency          : 2437 MHz
Band/Channel       : 2400 MHz/Ch.6           Channel Width        : 20 MHz

-------------------------------------------------------------------------------
Network Parameters
-------------------------------------------------------------------------------
SSID               : kansarhm8b
Security           : none
Connected          : yes
Connection Time    : 2022/09/30 17:44:18     Duration             : 0d 00:00:08
BSSID              : 00:23:a7:8e:d9:04       Channel Number       : 1
Rx Signal Level    : -39 dBm                 Frequency            : 2412 MHz
-------------------------------------------------------------------------------
SSID               : kanlnx963
Security           : none

-------------------------------------------------------------------------------
SSID               : abcd
Security           : wpa2-psk
Passphrase         : **********
Encryption         : aes

===============================================================================
===============================================================================
Port Statistics
===============================================================================
                                                    Input                Output
-------------------------------------------------------------------------------
Packets                                                 2                     2
Discards                                                0                     0
Unknown Proto Discards                                  0
===============================================================================
```

7.2.2.2 Clear commands

- Clear cellular port commands
- Clear raw socket statistics commands
- Clear WLAN statistics commands

7.2.2.2.1 Clear cellular port commands

port

Syntax

port *port-id* **statistics**

Context

clear

Description

This command clears statistical information for a cellular interface port.

Parameters

port-id

specifies the cellular port, from 1/1/1 to 1/1/2

statistics

clears statistical information

7.2.2.2.2 Clear raw socket statistics commands

port

Syntax

port 1/3/1 statistics

Context

clear

Description

This command clears raw socket statistical information for a serial port.

Parameters

statistics

clears statistical information

7.2.2.2.3 Clear WLAN statistics commands

port

Syntax

port *port-id* **statistics**

Context

clear

Description

This command clears WLAN statistical information for a WLAN port.

Parameters

port-id

the WLAN port identifier

Values 1/4/1 to 1/4/4

statistics

clears statistical information

7.2.2.3 Tools commands

- Tools perform commands
- Tools dump commands

7.2.2.3.1 Tools perform commands

at-command

Syntax

at-command *at-command*

Context

tools>perform>mda>cellular

Description

This command executes an ATtention (AT) command on the cellular port. AT commands are instruction commands that are used to control a modem. The commands are issued to the modem, and responses to the commands from the modem are displayed directly on the CLI console.

These commands can also be used to view operational information about the cellular port.

WARNING:
Risk of service outage. Do not change any **at-command** settings.

Note:

- The commands are reserved for use by Nokia personnel only.
- Some commands may take up to several minutes to complete.

Parameters

at-command

a supported AT command

Values up to 256 characters; must be preceded by the string "at"

auto-boot

Syntax

auto-boot {**complete** | **retry** | **terminate**}

[**no**] **auto-boot echo** [**debugger**]

Context

tools>perform

Description

This command is used to configure the status of the ADP-Hm process running on the node.

The **auto-reboot echo** command controls the echo of log updates to the console. When the **debugger** parameter is specified, auto-boot debug logs are sent to the console.

Parameters

complete

specifies that the ADP-Hm process is complete

retry

specifies that the ADP-Hm process is being retried

terminate

specifies that the ADP-Hm process has been terminated

diag-port-access

Syntax

diag-port-access listening-port *port-number* **start**

diag-port-access stop

Context

tools>perform>cellular

Description

This command enables or disables the TCP port used by the TCP server for remote access to the cellular diagnostics port on the node. When enabled, third-party applications use the port to connect directly to the cellular modem to stream binary diagnostic information from the cellular radio in real time.

Parameters

listening-port *port-number* **start**

specifies that the TCP port used by the TCP server is enabled for remote access to the cellular diagnostics port

Values 1024 to 49151

listening-port stop

specifies that the TCP port used by the TCP server is disabled for remote access to the cellular diagnostics port

force-sim-switch

Syntax

force-sim-switch

Context

tools>perform>mda>cellular

Description

This command manually forces a SIM activity switch. This command is used in a dual SIM deployment when the **active-sim** command is set to **auto**.

update-firmware

Syntax

update-firmware *firmware-file*

update-firmware *firmware-file* **sim 1** | **2**

Context

tools>perform>mda>cellular

Description

This command preloads the correct firmware onto the cellular modem when specific firmware is needed to attach to a cellular network.

The 7705 SAR-Hm supports the **update-firmware** *firmware-file* **sim 1** | **2** command. The command updates the firmware for the specified SIM. This form of command is supported only on the 7705 SAR-Hm, and specifying either **sim 1** or **sim 2** is mandatory. The firmware is updated only after the system reboots. When the command is executed, a prompt appears asking the operator whether to proceed with a reboot in order to update the firmware. Entering **y** at the prompt reboots the system immediately and the firmware is updated. Entering **n** at the prompt postpones the reboot and the firmware is updated the next time the system is rebooted.

For the 7705 SAR-Hm, in a dual SIM deployment, to update the firmware on both SIMs at the same time, the operator must execute the **update-firmware** command for the first SIM and enter **n** at the reboot prompt. The operator must then execute the **update-firmware** command for the second SIM and enter **y** at the reboot prompt in order to proceed with a system reboot. The firmware for both SIMs is updated when the reboot is complete. If the operator enters **n** at the second reboot prompt, the reboot is postponed and the firmware for both SIMs is updated the next time the system is rebooted.

The command can be executed on the SIMs in either order, SIM 1 first or SIM 2 first.

The firmware for both SIMs can be updated individually, but this requires the system to be rebooted twice.

If the **update-firmware** command is executed multiple times for the same SIM but with different firmware files and no reboot occurs at the time the command is executed, when a system reboot does occur, the firmware is updated with the last firmware file specified in the command.

The 7705 SAR-Hmc supports the **update-firmware** *firmware-file* command.

The firmware that is bundled with SR OS is considered the default firmware for the radio module on the 7705 SAR-Hmc. If the **update-firmware** command is not used, the radio module uses the default firmware and system upgrades to a newer version of SR OS will automatically use the firmware version that is bundled in SR OS. If the **update-firmware** command is used, the radio module uses the version of firmware specified in the command and when the system upgrades to a newer version of SR OS, the radio module continues using the version of firmware specified in the command and ignores the bundled version of firmware in SR OS.

The **update-firmware** command is used to specify the version of firmware that will be used by the radio module on both SIMs (the firmware cannot be updated per SIM). The command overwrites the firmware currently used by the radio module, which can be the default firmware automatically loaded by SR OS or another specified version of firmware. When the system is rebooted, this updated firmware is used by the radio module.

To return to the default firmware, the operator must execute the **update-firmware** command using "default" as the specified firmware file. Using "default" informs the system that the current version of firmware must be discarded and replaced with the firmware version that is bundled with SR OS.

When this command is executed, the operator prompted to proceed with a reboot in order to update the firmware. Entering **y** at the prompt reboots the system immediately and the firmware is updated. Entering **n** at the prompt postpones the reboot and the firmware is updated the next time the system is rebooted.

Parameters

firmware-file

specifies a cellular radio firmware file located on the cf3: file system. If "default" is specified, the firmware is updated to use the bundled version of firmware in SR OS.

change-pin

Syntax

change-pin

Context

tools>perform>mda>cellular>sim

Description

This command launches an interactive CLI session to change the PIN on the SIM.

Note:

- Ensure that the specified SIM is the currently active SIM.

- It is not possible to change the PIN on a SIM unless the SIM is locked. See the lock-sim command.

When a SIM is procured from a carrier, the SIM PIN is set to a default value. When this command is issued, the CLI prompts the user to enter the current PIN once and then correctly enter the new PIN twice in order to change it.

WARNING:

- When an operator successfully locks a SIM, unblocks a SIM, or changes a SIM PIN, the system updates the PIN value in the system configuration. However, the system does not automatically save the system configuration containing the new PIN. The operator must perform an **admin>save** command immediately after changing the PIN in order to save the new PIN in the system configuration file and avoid potential service interruptions such as the node becoming unreachable.
- If the SIM becomes blocked when setting the PIN remotely using in-band management over a cellular port, the node will be unreachable. Physical access to the node will be required to unblock the SIM.

lock-sim

Syntax

lock-sim

Context

tools>perform>mda>cellular>sim

Description

This command enables the PIN verification function on the SIM and locks the SIM. When locked, the SIM can only be accessed if the operator enters the PIN stored in the configuration file.

Note: Ensure that the specified SIM is the currently active SIM.

When this command is issued, the CLI prompts the user to enter the current PIN in order to lock the SIM.

WARNING:

- When an operator successfully locks a SIM, unblocks a SIM, or changes a SIM PIN, the system updates the PIN value in the system configuration. However, the system does not automatically save the system configuration containing the new PIN. The operator must perform an **admin>save** command immediately after changing the PIN in order to save the new PIN in the system configuration file and avoid potential service interruptions such as the node becoming unreachable.
- If the SIM becomes blocked when setting the PIN remotely using in-band management over a cellular port, the node will be unreachable. Physical access to the node will be required to unblock the SIM.

unblock-sim

Syntax

unblock-sim

Context

tools>perform>mda>cellular>sim

Description

This command unblocks a SIM that is currently blocked as a result of too many attempts being made to access the SIM using an incorrect PIN.

Note: Ensure that the specified SIM is the currently active SIM.

When this command is issued, the CLI prompts the user to enter the personal unblocking key (PUK) for the SIM and then enter a new PIN value twice. The PUK is acquired from the service provider or administrator and is also stored on the SIM. The lock/unlock state of the SIM does not change when it becomes unblocked.

WARNING:

- When an operator successfully locks a SIM, unblocks a SIM, or changes a SIM PIN, the system updates the PIN value in the system configuration. However, the system does not automatically save the system configuration containing the new PIN. The operator must perform an **admin>save** command immediately after changing the PIN in order to save the new PIN in the system configuration file and avoid potential service interruptions such as the node becoming unreachable.
- If the SIM becomes blocked when setting the PIN remotely using in-band management over a cellular port, the node will be unreachable. Physical access to the node will be required to unblock the SIM.

unlock-sim

Syntax

unlock-sim

Context

tools>perform>mda>cellular>sim

Description

This command disables the PIN verification function on the SIM and unlocks the SIM. When unlocked, the PIN is not required in order to access the SIM.

Note: Ensure that the specified SIM is the currently active SIM.

When this command is issued, the CLI prompts the user to enter the current PIN in order to unlock the SIM.

reset

Syntax

reset

Context

tools>perform>port>cellular>cbsd-authorization

Description

This command resets the CBSD authorization process so that it restarts from the beginning.

scan

Syntax

scan

Context

tools>perform>mda>wlan

Description

This command performs an SSID scan on the WLAN MDA. The WLAN MDA must be configured before the scan can be executed.

Note: Executing this command disconnects the WLAN station port if it is connected to a remote AP and shuts down any configured WLAN AP ports that are enabled.

When the scan is complete, the WLAN station port attempts to reconnect to the remote AP that it was previously connected to, and the configured WLAN APs are re-enabled so that AP clients can reconnect.

7.2.2.3.2 Tools dump commands

diag-port-access

Syntax

diag-port-access status

Context

tools>dump>cellular

Description

This command retrieves information about the TCP server used for remote access to the cellular diagnostics port.The listening port is the TCP port used by the TCP server.

When the TCP server is not enabled, the CLI shows the server status as "disabled" and the server state as "down". The CLI shows the listening port status as "none".

When the TCP server is enabled with a specific port number but no client is connected, the CLI shows the server status as "enabled" and the server state as "waiting for client". The listening port field indicates the TCP port number.

When the TCP server is enabled and a client is connected, the CLI shows the server status as "enabled". It also shows the server state as "client connected" along with the client IP address and client port number. The listening port field indicates the TCP port number.

cbsd-authorization

Syntax

cbsd-authorization [**clear**]

Context

tools>dump>port>cellular

Description

This command shows detailed information about the CBSD authorization process, including the contents of the last sent messages and last received messages for:

- CBSD registration
- spectrum inquiry
- grant requests
- heartbeats
- grant relinquishments
- CBSD deregistration

Parameters

clear

clears all CBSD information

last-scan-result

Syntax

scan

Context

tools>dump>mda>wlan>last-scan-result

Description

This command displays the results of the last SSID scan on the WLAN MDA.

8 Appendix

The channel and channel size of a WLAN access point (AP) depends on the country. Table 8: Channel identifier and size per country lists the channel identifier and bandwidth per country.

Table 8: Channel identifier and size per country

Frequency	Bandwidth	Channel	Country																				
			Australia	Belgium	Canada	France	Germany	India	Iran	Italy	Japan	Malaysia	Mexico	New Zealand	Russia	Singapore	South Afr	USA	Bolivia	Brazil	Chile	Colombia	Peru	Venezuela
2.4	20	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		10	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		11	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		12	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
		13	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
2.4	40	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

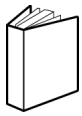
Frequency	Bandwidth	Channel	Country																				
			Australia	Belgium	Canada	France	Germany	India	Iran	Italy	Japan	Malaysia	Mexico	New Zealand	Russia	Singapore	South Afr	USA	Bolivia	Brazil	Chile	Colombia	Peru	Venezuela
		6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
		8	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
		9	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
		10	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		11	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		12	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		13	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
5	20	36	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		40	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		44	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		48	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		149	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
		153	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
		157	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
		161	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
		165	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
	40	36	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		40	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		44	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
		48	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		149	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y
		153	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		157	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y

Frequency	Bandwidth	Channel	Country																				
			Australia	Belgium	Canada	France	Germany	India	Iran	Italy	Japan	Malaysia	Mexico	New Zealand	Russia	Singapore	South Afr	USA	Bolivia	Brazil	Chile	Colombia	Peru	Venezuela
		161	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
		165	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

9 Standards and protocol support

See the software guides from the SR documentation suite for a list of standards and protocols supported by the SR OS. Use the features and descriptions in this documentation set and in the relevant software release notes to identify the related standards and protocols that are supported by the 7705 SAR-Hm series.

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback