7705 SAR-Hm
7705 SAR-Hmc

Release 26.3.R1

Main Configuration Guide

3HE 27860 AAAA TQZZA
Edition: 01
March 2026

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

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.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2026 Nokia.

Table of contents

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

List of tables

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

List of figures

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

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 usage for functionality that is specifically related to the 7705 SAR-Hm series.

The 7705 SAR-Hm series of routers 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.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

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.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

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

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

2 Overview

The routers in the 7705 SAR-Hm series provide network connectivity over cellular networks, extending the reach of IP/MPLS networks and related services using cellular wireless infrastructures and WLAN technology.

The 7705 SAR-Hm series software is built from the Nokia Virtualized Service Router (VSR), based on SR OS software that powers the 7750 SR and 7950 XRS routers.

There are two chassis available in the series: the 7705 SAR-Hm and the 7705 SAR-Hmc. There are variants of each chassis based on the capabilities of the cellular radio module included in the unit.

See the SAR-Hm and SAR-Hmc Chassis Installation Guide for a list of radio options and bands supported for each variant.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

3 Basic system configuration

The 7705 SAR-Hm series of routers provides basic system configuration support as covered in the following topics:

- CLI usage
- File system management
- Boot options file
- ADP-Hm
- Basic system management
- Network Services Platform functional overview
- Debug commands
- Tools commands

3.1 CLI usage

For general information about CLI usage, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*, "Classic CLI overview".

3.2 File system management

The 7705 SAR-Hm series routers use the SR OS file system to store files used and generated by the system; for example, image files, configuration files, logging files, and accounting files.

The file commands allow you to copy, create, move, and delete files and directories, navigate to a different directory, and display file or directory contents and the image version. The routers in the 7705 SAR-Hm series use on-board flash memory for storing software images. The file system on the 7705 SAR-Hm series of routers is case sensitive.

For more information about file system management support, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*, "File management".

Note: The routers in the 7705 SAR-Hm series do not have cf1: or cf2: devices. They only have the cf3: device, which is provided via on-board flash memory.

3.2.1 7705 SAR-Hm series file system

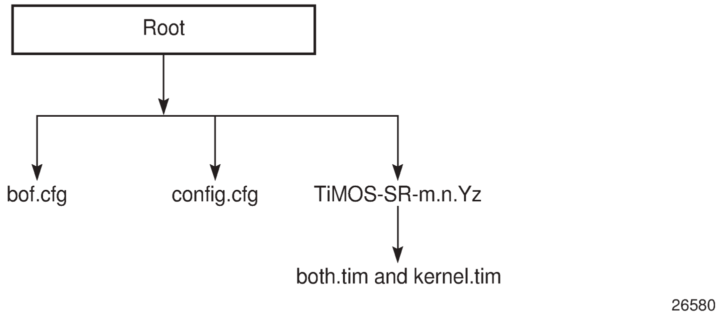
The system ships from the factory with the BOF configured with an empty primary-config, and with auto-discover enabled. Figure 1: Files on the integrated flash memory device shows the directory structure and filenames on the integrated flash memory device with the suggested BOF configuration for the primary-config and primary-image files.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

The primary-config file is typically located cf3:/config.cfg. Nokia recommends using the directory structure cf3:/TiMOS-SR-m.n.Yz to hold multiple releases. The location and filenames can be changed in the BOF if required.

Figure 1: Files on the integrated flash memory device



Files on the integrated flash memory device are:

- both.tim — application software file
- kernel.tim
- support.tim

Note: In releases before Release 19.10.R1, the system included the following files in addition to those listed above:

- boot.tim
- vxrom.bin
- u-boot.bin
- fman-ucode.bin
- mc7475_fw.bin

See the *7705 SAR-Hm and SAR-Hmc Software Release Notes* for more information.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide* for a full description of the TiMOS file system.

3.3 Boot options file

The primary copy of the system software is factory installed on the internal flash drive in directory cf3.

When the node is first powered on, by default the system searches for the bof.cfg file (also known as the BOF file) on the integrated flash. The system reads and executes the system initialization commands configured in the boot option file (BOF).

The BOF in the node is factory configured with Auto Discovery Protocol (ADP-HM) enabled. ADP-Hm starts automatically unless the auto-discover option is disabled.

The default ADP-Hm configuration in the BOF is as follows:

- auto-discover private.nokia.nsp.primary.nms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- auto-discover private.nokia.nsp.secondary.nms

For example:

```
*A:Dut-A# show bof
===============================================================================
BOF (Memory)
===============================================================================
    primary-image cf3:/TiMOS-19.10.R1/
 <lines removed...>

    console-speed    115200
    auto-discover    private.nokia.nsp.primary.nms
    auto-discover    private.nokia.nsp.secondary.nms
===============================================================================
*A:Dut-A#
```

ADP-Hm can be disabled manually by executing the **tools>perform>auto-boot terminate** command and saving the BOF. See Terminating ADP-Hm for more information.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*, "System Initialization and boot options" for more information about boot options.

3.4 ADP-Hm

The Nokia NSP Network Functions Manager - Packet (NSP NFM-P) supports the Auto Discovery Protocol (ADP) process for the node. This process is known as ADP-Hm. The ADP-Hm process provides all initialization and commissioning functions automatically for a newly installed node.

After one or more SIMs have been installed in a 7705 SAR-Hm series node, when the node is powered on for the first time and any required password change has been made (see Prerequisites for ADP-Hm), the ADP-Hm process running on the node configures a cellular port using the SIM in SIM slot 1 and an Ethernet port (port 1/2/1), and establishes connectivity to the NSP NFM-P. The ADP-Hm process then waits for the NSP NFM-P to complete the discovery and configuration of the node.

This section describes the following topics:

- Prerequisites for ADP-Hm
- The ADP-Hm process
- The Console during the ADP-Hm process
- LED operation during the ADP-Hm process
- Terminating ADP-Hm

See Network Services Platform functional overview for information about NSP NFM-P management functions. See the *NSP NFM-P User Guide* for more information and procedures to manage the ADP-Hm process.

3.4.1 Prerequisites for ADP-Hm

The prerequisites to allow the ADP-Hm process to automatically discover a 7705 SAR-Hm series router are:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- An NSP NFM-P has been procured, installed, and is managing one or more head-end nodes defined for the cellular domain.
- A valid SIM card is inserted into SIM slot 1 on the node. For dual SIM operation a second SIM is inserted into SIM slot 2.
- For those variants of the 7705 SAR-Hm series node with a unique factory-set password which must be changed at first login, the new password must match the password expected by the NSP NFM-P being used to discover the node during the ADP-Hm process.
- The operator has determined whether the one-step or two-step process will be used by the NSP NFM-P and configures it as such.
- For each carrier private VPN service associated with each installed SIM, a route exists for the NFM-P from the carrier private VPN service or the private-LTE cellular Evolved Packet Core (EPC) toward the cellular domain head-end node or nodes that have reachability to the NSP NFM-P. These gateway nodes allow new 7705 SAR-Hm nodes running ADP-Hm to reach the NSP NFM-P.
- A route for the subnet of the cellular domain nodes exists from the cellular domain head-end node to the new node to be discovered. For initial installation of a cellular domain, IP addresses are typically allocated from a /24 or /18 IP address range and the associated routes can be used. In a dual SIM deployment, there must exist a route for the IP addresses associated with each SIM.
- A default Access Point Name (APN) or Virtual Private Network (VPN) service has been procured from the service provider for the SIMs that are installed in the node. If a fixed/static IP address for the IMSI associated with the SIM is required, the address can be allocated in two ways for each SIM:
  1. by direct Home Subscriber Server (HSS) allocation (such as when a mobile carrier assigns IP addresses for the SIM and IMSI).
  2. by a Radius/AAA/DHCP server owned by the enterprise operator. This method uses a process known as deferred IP allocation between the Home Subscriber Server (HSS) and the PGW of the wireless service provider. When the node first connects and authenticates with the HSS of the wireless provider, the default APN associated with the service indicates that the IP allocation is deferred to the enterprise Radius/AAA/DHCP server. After the PGW learns the static IP address from the server, it is sent to the node in the PDP address IE when the default bearer is established.
- The PGW to which the node will attach using the SIM in slot 1 is configured with additional Protocol Configuration Options (PCO) for the APN. The PCO must include the following two values:
  - dns-server-ipv4 primary – for example, config/mobile/pdn/apn/pco/dns-serveripv4 primary
  - dns-server-ipv4 secondary – for example, config/mobile/pdn/apn/pco/dns-serveripv4/backup
- A primary and secondary DNS server (available from a wireless provider or owned by an enterprise operator) are configured to resolve the NSP NFM-P IP primary and backup NSP NFM-P IP addresses.
- A SAR-Hm.xml file is loaded on the NSP NFM-P for the cellular domain where the node will reside after discovery. The XML file lists the SIM IMSIs for SIM slot 1 and the node's associated system IP addresses (if specified in the XML file) of each node that needs to be discovered. In a dual SIM deployment, the SIM in slot 2 is not referred to in this XML file. See the NSP NFM-P User Guide for more information about configuring cellular domains and the associated XML files.
- The operator has enabled ADP-Hm on the NSP NFM-P for the associated prefix addresses of the nodes to be discovered using ADP-Hm in the cellular domain.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

3.4.2 The ADP-Hm process

The following sections describe the three phases of the ADP-Hm process:

- Network discovery (phase 1)
- NSP NFM-P discovery (phase 2)
- NSP NFM-P configuration (phase 3)

3.4.2.1 Network discovery (phase 1)

When the node boots up initially, it runs the application load, executes the config file (which is empty), and then checks the BOF to determine if ADP-Hm needs to run. If ADP-Hm is enabled, the ADP-Hm process starts and performs the tasks listed below:

- The ADP-Hm process configures Ethernet port 1/2/1, which can be used for the first step of the two-step process if using Ethernet for step 1 is enabled on the NSP NFM-P. The following CLI output shows the configuration:

```
configure port 1/2/1
        ethernet
            mode network
            hold-time up 5 down 5
        exit
        no shutdown
    exit

    router Base
        interface "IF-1/2/1"
            port 1/2/1
            no shutdown
        exit
        interface "system"
            no shutdown
        exit
    exit
```

- The ADP-Hm process initializes the cellular port that uses SIM1 for PDN connectivity using the default PDN profile, which has a blank APN. When the cellular port attempts to connect to the network, it uses this PDN profile. If the carrier requires an APN other than the default in order for the cellular port to connect to the network, the cellular port can learn the correct APN from the network if the carrier supports that capability. If the carrier does not support devices learning the APN but requires an APN other than the default, then the operator must configure a PDN profile at the system level with the correct APN and assign that PDN profile to cellular port 1/1/1. See the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide* for details about configuring a PDN profile and assigning it to a cellular port.
- After the cellular port connects to the network, ADP-Hm assigns the name pdn1-sim1 to the PDN router interface. The name of the router interface must not change during the ADP-Hm process. The PDN router interface can operate in one of three modes. ADP-Hm uses the dynamic cellular interface IP mode of operation. See Dynamic cellular interface IPv4 mode for more information.
- The ADP-Hm process creates a loopback interface with a default name for the PDN interface (such as "pdn1-loopback"). No IP address is assigned to the loopback because it is operating in dynamic cellular interface IP mode.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- The ADP-Hm process uses this loopback interface as the unnumbered interface for the PDN router interface

The following CLI output shows the configuration:

```
configure router
        interface "pdn1-loopback"
            loopback
            no shutdown
         exit
        interface "pdn1-sim1" pdn
             port 1/1/1
             unnumbered "pdn1-loopback"
             no shutdown
         exit
    exit
exit
```

If the cellular network authenticates and accepts the new node onto the network, a default bearer is established and the following information is provided to the node for the APN to which the node connects:

- the IP address of the cellular interface
- the DNS server IP addresses

The configuration is not saved. (Phase 2) NSP NFM-P Discovery begins.

3.4.2.2 NSP NFM-P discovery (phase 2)

During the NSP NFM-P discovery phase, the node sends DNS query messages to the DNS server addresses discovered from the previous phase. The node then learns the IP addresses of the NSP NFP-P and sends SNMP traps toward the NSP NFP-P.

The following NSP NFM-P URL names are set for the **auto-discovery** command in the BOF by default:

- auto-discover private.nokia.nsp.primary.nms
- auto-discover private.nokia.nsp.secondary.nms

Note: The names can also be set to the following:

- another appropriate name, if required
- an IP address (which eliminates the requirement for a DNS server)

The node sends the DNS query message every 5 seconds until a DNS query response message is received with a valid IP address for the primary and secondary NSP NFM-P.

One IP address is required for the ADP-Hm process to continue to the next phase. If no DNS query response message is received, ADP-Hm will time-out and reboot the node. After reboot, the ADP-Hm process restarts from the beginning of Network Discovery (Phase 1).

After either the NSP NFM-P primary or secondary IP addresses are known by the node, the NSP NFM-P performs the following:

- SNMPv2 trap destinations are set to the NSP NFM-P IP addresses. Log 1 is used to set up the trap destinations.
- The node initiates an SNMP trap poll that sends a "Hello" notification trap message to the NSP NFM-P every 15 seconds.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- The node waits for the NSP NFM-P to process the Hello request and then ADP-Hm starts the NSP NFM-P Configuration (Phase 3).

3.4.2.3 NSP NFM-P configuration (phase 3)

In the third phase, the NSP NFM-P secures the node and carries out the remaining commissioning steps on the node.

Throughout this phase, the node sends an SNMPv3 trap to the NSP NFM-P every 15 seconds until the NSP NFM-P executes the **tools>perform>auto-boot complete** command.

There are two process options available on the NSP NFM-P during this phase. (See the NSP NFM-P user guides for more information about these options.)

1) One-step process – the NSP NFM-P performs all discovery and configuration activities on the node in one step. This allows ADP-Hm to run at the site location from start to finish. After Phase 3 is complete, the node is fully managed and secured. For more information about the one-step process, see One-step process details.

2) Two-step process – the NSP NFM-P configures critical security parameters on the node in the first step where operators can monitor progress in a DMZ or staging facility. The first step is performed using either the cellular interface or Ethernet port 1/2/1. After step one, the node is secured and fully managed by the NFM-P.

The node is powered down and if Ethernet was used during step one, the Ethernet cable is unplugged from port 1/2/1. The node is transported to the installation site where the operator performs the second step. When the node is installed and powered on, the NSP NFM-P completes the network-level configuration for the node. The NSP NFM-P configures such things as default tunnels and services to the head-end nodes, or optionally adds the node to an existing network group encryption (NGE) domain. For more information about the two-step process, see Two-step process details.

3.4.2.3.1 One-step process details

In the one-step process, the node is powered on and ADP-Hm completes the entire discovery and configuration of the node in one step.

The NSP NFM-P uses NETCONF over SSHv2 to configure SNMPv3 parameters, including the users and security encryption and authentication keys for SNMPv3. This information is based on the mediation policy configured for the cellular domain in the NSP NFM-P.

The NSP NFM-P then completes the configuration of the node. The following list summarizes the actions that the NSP NFM-P performs on the node:

1. Creates a strict security association between the chassis information, IMEI, and the SIM in SIM slot 1. After this association is made, the SIM cannot be inserted into another node and managed by the NSP NFM-P without operator intervention to instruct the NSP NFM-P to create a new association between the SIM and a new chassis.
2. Configures usernames and passwords, scope of control, and associated profiles.
3. Configures PDN profiles that are used to connect to the cellular network after ADP-Hm is complete. If dual SIM is enabled for the cellular domain in the NSP NFM-P, then the second cellular port and PDN router interface is configured.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

4. Downloads the required radio firmware version for SIM 1 and if dual SIM is enabled, it downloads the radio firmware version for SIM 2. The NSP NFM-P resets the radio so that SIM 1 uses the latest downloaded version.
5. Downloads the required software load and resets the node to use the latest version of the software.
6. Downloads the NGE key-group of the NGE domain associated with the cellular domain if the node is to enter the NGE domain. The PDN router interface is also configured with the key-group needed to enter the NGE domain.
7. If the cellular mode is Static Cellular Interface IP Mode or Dynamic Cellular Interface IP Mode, the NSP NFM-P performs the following configurations toward the head-end nodes of the cellular domain to establish an in-band management service. (For more information, see the Static cellular interface IPv4 mode, and Dynamic cellular interface IPv4 mode sections in this guide.)
   - Configures a BGP session to each head-end node in the cellular domain that is associated with the first cellular network. The BGP sessions are configured with the PDN router interface associated with SIM 1.
   - Configures a BGP session to each head-end in the cellular domain that is associated with the second cellular network when two SIMs are required. The BGP sessions are configured with the PDN router interface associated with SIM 2.
   - Configures an in-band management VPRN service used by the NSP NFM-P to manage the node in-band over the GRE-IMPLS tunnels over the cellular network. This VPRN service can optionally be NGE encrypted to provide an additional layer of security when managing nodes.
8. If dual SIM is enabled for the cellular domain, the NSP NFM-P performs a manual SIM switch to enable cellular service using the second SIM. It then confirms that the second cellular network and the in-band management VPRN service are working correctly. After the second SIM is verified, the NSP NFM-P performs another manual SIM switch and enables cellular service using the first SIM, as was used throughout the ADP-Hm process.

The NSP NFM-P is responsible for saving the configuration after the actions listed above are executed, and may save the configuration several times over the course of executing them.

After the above actions are completed, the NSP NFM-P stops the ADP-Hm process by executing **tools>perform>auto-boot complete** command.

NSP NFM-P then disables ADP-Hm so that the discovery process no longer runs; the NSP NFM-P does so by setting the **no auto-discover** command in the BOF and by clearing all DNS entries, if multiple entries existed.

The system and alarm status LEDs are set and the node is ready for further services configuration. For a description of how LEDs indicate the node status during the ADP-Hm process, see LED operation during the ADP-Hm process.

3.4.2.3.2 Two-step process details

In the two-step process, the node is powered on first in a staging area or DMZ for initial NSP NFM-P security configurations and then powered on a second time at the final site location to complete the commissioning process. For the first step, the node uses either the cellular interface or Ethernet port 1/2/1 to communicate with the NSP NFM-P during the commissioning process. The steps are as follows:

1. The node is powered on for the first time and items 1 to 5 as described in One-step process details are executed by the NSP NFM-P. The NSP NFM-P then issues the **tools>perform>auto-boot complete** command to indicate that step 1 of this process is complete and to stop the ADP-Hm process on the

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

node. The system Status LED on the node turns solid green and the Alarm LED continues to blink, indicating that step 1 has completed and the node can be powered off. For more information, see LED operation during the ADP-Hm process. If Ethernet port 1/2/1 was used for this step, the Ethernet cable is unplugged from the port. The node can be shipped to the site for final installation.

2. The node is powered on for the second time. Because the BOF is set to "auto-discover" it sends SNMPv3 traps to the NSP NFM-P to indicate that the ADP-Hm process is resuming. The NSP NFM-P resumes the ADP-Hm process and items 6 to 8 as described in One-step process details are executed. The NSP NFM-P then saves the configuration and completes the ADP-Hm process. The system Status and Alarm LEDs indicate that ADP-Hm is complete.

When Ethernet port 1/2/1 is used for step 1 of the two-step process, a DHCP server is reachable over the Ethernet interface. The DHCP OFFER or REQ messages sent from the node to the DHCP server contain the following options:

- chaddr—the client MAC address
- Option 50—the requested IP address; this address is the same as the address contained in the yiaddr field that was received in the DHCP OFFER message
- Option 53—the DHCP message type (REQUEST)
- Option 54—the DHCP server address; this address is the same as the address received in the OFFER message
- Option 51—the IP address lease time; this value is the same as the lease time received in the OFFER message
- Option 60—the vendor class identifier; this value is the same as the vendor class identifier in the DISCOVER message
- Option 61—the client identifier; this value is the same as the client identifier in the DISCOVER message
- Option 55—the parameter request list:
  - Option 1—the subnet mask value
  - Option 3—the router option (unused if not enabled in the CLI)
  - Option 6—the DNS server option (unused if not enabled in the CLI)
  - Option 54—the DHCP server address
  - Option 121—the static-route option (unused if not enabled in the CLI)

The DHCP server returns the following options:

- Option 3—the router option; the router is installed as the default gateway address
- Option 6—the DNS server option; the DNS server is installed in the list of DNS servers for the node (up to six servers are supported on the node)
- Option 121—the static-route option; the static route is installed as a route for the router interface on Ethernet port 1/2/1

3.4.3 The Console during the ADP-Hm process

The Console port can be used to establish a CLI session on a 7705 SAR-Hm series node so that the progress of the ADP process can be monitored. For information about using the Console port to establish a CLI session, see the *SAR-Hm and SAR-Hmc Chassis Installation Guide*, "Establishing a console connection".

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

During ADP, the node may reset periodically. The Console session is lost during reset and you must log in to the node again.

Note: If NSP and ADP are not available in your network, the console port can be used as the interface to discover, configure, and manage a 7705 SAR-Hm series node.

You can use the **tools>perform>auto-boot** command to monitor the ADP process.

In the following example, no ports on the router have been discovered yet.

```
*A:Dut-A# tools dump auto-boot
===============================================================================
Automated-Provisioning
===============================================================================
Status          : Connecting-To-Network
Failures        : None

Start Time      : TUE MAR 07 17:12:22 2023
End Time        : Never

NMS         (1) : Not Configured
NMS         (2) : Not Configured
-------------------------------------------------------------------------------
Registered Ports
-------------------------------------------------------------------------------
1/1/1                                                        WAITING-FOR-NETWORK
```

During ADP, **show** commands can be used to monitor the interface discovery processes. For example, you can use the **show port 1/1/1** to verify the status of the cellular port.

```
A:Dut-A# show port 1/1/1
===============================================================================
Cellular Interface
===============================================================================
Description       : Cellular
Interface         : 1/1/1                IfIndex           : 35684352
Admin State       : up                   Oper State        : up
IMEI              : 00-102700-033329-6
Network Status    : registered-home      Radio Mode        : lte
Band              : 4                    Channel           : 2175
RSSI              : -85 dBm              RSRP              : -84 dBm
Tracking Area Code: 0001                 Cell Identity     : 00000101
                                         Phys Cell Identity: 500
-------------------------------------------------------------------------------
SIM Card
-------------------------------------------------------------------------------
SIM Card 1        : installed
Locked            : no                   PIN status        : ready
PIN retries left  : 3                    PUK retries left  : 10
ICCID             : 89442016100100000205 IMSI              : 001001000000020
SIM Card 2        : not installed
-------------------------------------------------------------------------------
Packet Data Network
-------------------------------------------------------------------------------
PDN State         : connected            IP Address        : 10.99.16.53
Primary DNS       : 8.8.8.8              Secondary DNS     : 4.4.4.4
APN               : internet
===============================================================================
===============================================================================
Port Statistics
===============================================================================
                                                   Input                 Output
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
-------------------------------------------------------------------------------
Packets                                                1                      0
Discards                                               0                      0
Unknown Proto Discards                                 0
```

3.4.4 LED operation during the ADP-Hm process

The system Status and Alarm LEDs indicate the current status of the node during the ADP-Hm process. Table 2: LED operations during the ADP-Hm process describes LED operation during the ADP-Hm process.

Note: The ADP-Hm process does not inhibit the RSSI signal strength LEDs so that installers can use the RSSI LEDs to optimize the position of the antennas when the ADP-Hm process is running.

Table 2: LED operations during the ADP-Hm process

ADP-Hm status/ phase	Status	Alarm
Before ADP-Hm starts	Green (blinking): Indicates that the system is booting up the TiMOS image and running hardware and software diagnostics	—
Network discovery	Green (blinking)	Amber (one blink followed by a pause). The cellular interface LEDs are also active and provide feedback about the cellular interface (showing link status and signal strength). For more information, see the *SAR-Hm and SAR-Hmc Chassis Installation Guide*, "7705 SAR-Hm LEDs".
NSP NFM-P discovery	Green (blinking)	Amber (two blinks followed by a pause then repeats).
NSP NFM-P configuration	Green (blinking)	Amber (three blinks followed by a pause, then repeats): This blinking occurs during the one-step or two-step process during the NSP NFM-P configuration phase.
	Green (solid): Indicates that the ADP-Hm process has completed step one of the two-step process and the system is ready to be powered down, installed at its final location and powered back up to complete step two of the two-step process.	
ADP-Hm complete	Green (solid): Indicates one of the following: • ADP-Hm is disabled and the system is operationally up. • the ADP-Hm process is complete for the one-step process and the system is operationally up.	The Alarm LED displays the current alarm state. For more information, see the *SAR-Hm and SAR-Hmc Chassis Installation Guide*, "7705 SAR-Hm LEDs".

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

ADP-Hm status/ phase	Status	Alarm
	• the ADP-Hm process completed step two of the two-step process and the system is operationally up.	

3.4.5 Terminating ADP-Hm

ADP can be disabled manually by executing the **bof no auto-discover** command and saving the BOF.

To terminate ADP-Hm:

1. Perform one of the following:
   - **a.** At boot up, the system displays a warning and a prompt about terminating Auto-Discovery. Type y to terminate Auto-Discovery. For example:

```
WARNING: Auto-discovery is currently running on this system.
It is recommended that Auto-Discovery be terminated before making
configuration changes using this session; otherwise, any changes made during this
process may result in Auto-Discovery failing to complete successfully and/
or lost configuration.

Do you wish to terminate Auto-Discovery (y/n?) y
```

   - **b.** Use the **tools>perform>auto-boot terminate** command. For example:

```
tools# perform auto-boot terminate
```

2. Reboot the node. After reboot, the warning message disappears and auto-discovery is removed from the BOF. For example:

```
*A:Dut-A# show bof
===============================================================================
BOF (Memory)
===============================================================================
    primary-image cf3:/TiMOS-19.10.R1/

 <lines removed...>

    console-speed    115200
===============================================================================
*A:Dut-A#
```

3.5 Basic system management

For general information about basic system management support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*, "System management":

- System management commands
  - System information
  - System time

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

    - Time zones
    - NTP
- Administrative tasks
  - Saving configurations
  - Specifying post-boot configuration files
- System router instances
- System configuration process overview
- General configuration notes
- Configuring system management features
- Basic system configuration
- Common configuration tasks

3.5.1 BOF and configuration file encryption

The 7705 SAR-Hm series of routers provides operators the option to encrypt the BOF and configuration files. For information, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*, "BOF and configuration file encryption".

3.6 Network Services Platform functional overview

The Nokia Network Services Platform (NSP) is a group of interoperating network management modules that provide comprehensive end-to-end management of a wide range of network domains and topologies.

The Nokia NSP Network Functions Manager - Packet (NSP NFM-P) is used to discover, configure, and manage the nodes and related cellular domains. The NSP NFM-P provides the following specific functions. (See the NSP NFM-P User Guide for more information.)

- creates and manages the cellular domains. A cellular domain is a group of nodes where each node in the group connects to the same head-end nodes, shares the same deployment modes of operation, and is part of the same NGE domain. For more information about deployment modes of operation, see the PDN router interfaces section of this guide.
- drives the ADP-Hm process for each new node to be discovered in a cellular domain. For static cellular interface IP and dynamic modes of operation, the NSP NFM-P creates a management VPRN service for in-band management of each node.
- manually adds or removes nodes to and from cellular domains
- supports the XML input lists of the SIM IMSI values that are expected to participate in the cellular domain and initiate the ADP-Hm process within the cellular domain. These lists include the SIM information and optionally, the system IP for node boot-strap process.
- creates a security association between the SIM, IMEI, and the chassis identifier for each node being managed such that unexpected changes are flagged as potential security violations to the operator.
- supports a configurable NSP NFM-P polling interval for nodes. Configurable polling is intended to minimize traffic between the NSP NFM-P and a large-scale deployment of nodes. To that end, the

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

NSP NFM-P also polls the status of the BGP sessions between head-end nodes and the nodes in the cellular domain in order to monitor the reachability and status of the nodes in the cellular domain.

3.7 Debug commands

The 7705 SAR-Hm series of routers supports **debug** commands that enable detailed debug information for various protocols.

Debug output is generally displayed by configuring a log using **from debug-trace**.

The currently enabled debug can be seen using the **show debug** command.

A debug configuration does not persist when the router reboots. The **admin debug-save** command can be used to save the debug configuration. The resulting file can be **exec**'ed later as needed.

Individual **debug** commands are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

3.8 Tools commands

The 7705 SAR-Hm series of routers supports **tools** commands. The **tools** commands provide two primary functions: dump and perform.

The **tools dump** commands are used to provide additional detailed and enhanced information about various aspects of the router.

The **tools perform** commands provide the ability to trigger a variety of actions on the router.

Individual **tools** commands are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools CLI Command Reference Guide*.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

4 System management

The 7705 SAR-Hm series of routers supports system management parameters as covered in the following topics:

- Security
- SNMP
- Event logs
- Public key infrastructure
- In-band management over cellular

4.1 Security

For general information about system security support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, "Security":

- Authentication, authorization, and accounting
  - Authentication
    - Local authentication
    - RADIUS authentication
    - TACACS+ authentication
  - Authorization
    - Local authorization
    - RADIUS authorization
    - TACACS+ authorization
  - Security controls
- RADIUS VSAs
- TACACS+ services and VSAs
- Control and management traffic protection
  - TTL security
  - Management Access Filter
- Other security features
  - SSH
    - SSH PKI authentication
    - MAC client and server list
    - KEX client and server list
    - Host key algorithm list

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

        - Regenerate the SSH key without disabling SSH
    - Exponential login backoff
    - User lockout
    - CLI login scripts
    - File access controls
    - 802.1x network access control
    - TCP enhanced authentication option
- Configuring security with CLI

Note: On the 7705 SAR-Hm and 7705 SAR-Hmc, 802.1x network access control is supported only WLAN interface access points.

For descriptions of security commands, see 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*.

4.2 SNMP

For general information about SNMP support, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, "SNMP".

4.3 Event logs

For general information about event log support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, "Event and accounting logs":

- Logging overview
- Log destinations
    - Console
    - Session
    - CLI logs
    - Memory logs
    - Log and accounting files
        - Log file encryption
    - SNMP trap group
    - Syslog
- Event logs
- Configuration notes
- Configuring logging with CLI

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

4.4 Public key infrastructure

For general information about public key support, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, "Public key infrastructure".

4.5 TLS

For general information about TLS support, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, "TLS".

4.6 In-band management over cellular

The 7705 SAR-Hm series of routers supports the following modes of operation over a cellular network:

- static cellular system IPv4 mode
- static cellular interface IPv4 mode or IPv6 mode
- dynamic cellular interface IPv4 mode or IPv6 mode

The way in which the node is managed depends on which mode of operation is in use. See Services over the cellular PDN interface for more information about the modes of operation.

When a cellular port on the node is operating in static cellular system IP mode, the system IP address is identical to the cellular IP address assigned during the initial PDN attachment process. To manage the node in this mode, the NSP NFM-P or other network management platform reaches the node without using the system IP address directly over the cellular network. This is the only mode that does not require a pre-established in-band management service to manage the node.

When a cellular port on the node is operating in static cellular interface IP mode or dynamic cellular interface IP mode, the NSP NFM-P or other network management platform can only reach the node through an in-band management VPRN service. For these modes of operation, the system IP address used to manage the node is private and differs from the cellular port IP address assigned when connecting to the cellular network. The system IP address must be advertised from the 7705 SAR-Hm series node to the head-end node by the in-band management VPRN service. Routing in the private IP/MPLS network past the head-end node must allow management traffic to reach the head-end node which will then send the management traffic over the VPRN to the node being managed.

The NSP NFM-P automatically configures the required in-band management VPRN service during the ADP-Hm process; see ADP-Hm for more information.

On the 7705 SAR-Hm series nodes, there are two methods for enabling in-band management over a VPRN service:

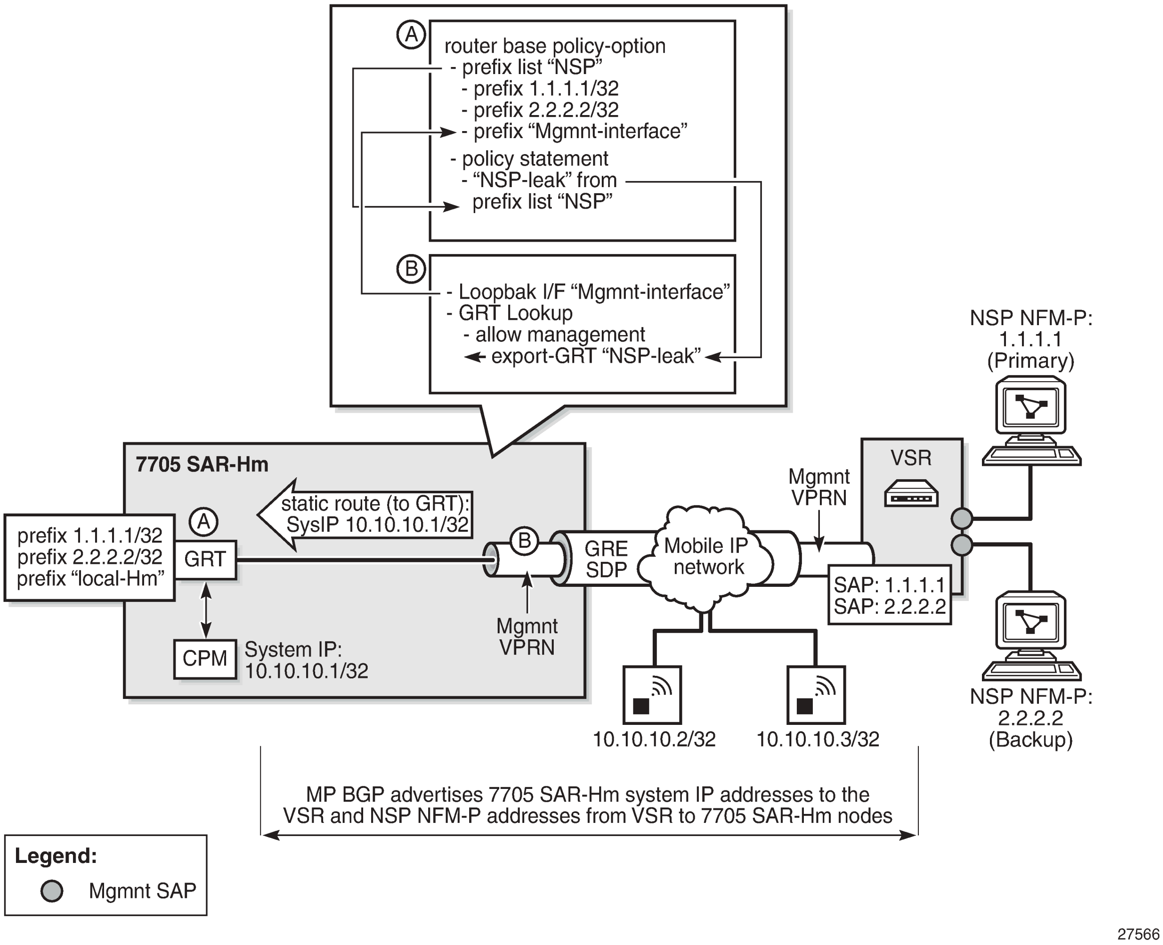
- performing a Global Routing Table (GRT) lookup and VPRN-to-GRT route leaking
- using port cross-connect

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

4.6.1 GRT lookup and VPRN-to-GRT route leaking

Figure 2: GRT lookup and VPRN-to-GRT route leaking shows the GRT lookup and VPRN-to-GRT route leaking option for in-band management over a VPRN on the 7705 SAR-Hm.

Figure 2: GRT lookup and VPRN-to-GRT route leaking



In-band management using the GRT lookup and VPRN-to-GRT route leaking option is enabled by configuring the following elements:

- A base router policy statement that includes a prefix list used to leak VPRN reachable addresses to the GRT. This prefix list includes the NSP NFM-P addresses and the management loopback interface that allows the CPM to respond to management queries or commands from the NSP NFM-P.
- A management loopback interface configured under the VPRN to allow the CPM to respond to management queries from the NSP NFM-P.
- A static route from the VPRN to the GRT for the system IP address of the node
- Enable a GRT lookup from the VPRN to the GRT so that management traffic received over the VPRN from the NSP NFM-P to the 7705 SAR-Hm series node can reach the CPM. This uses the **grt-lookup**, **enable-grt**, and **allow-local-management** CLI commands in the **config>service>vprn** context.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

For descriptions of these commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

- A VPRN-to-GRT route leak that populates the GRT routing table with addresses that are reachable by the VPRN, using the **export-grt** command. For a description of this command, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*. The reachable addresses include those for the NSP NFM-P and the local management loopback interface that allows responses from the CPM to return to the corresponding VPRN.

The following CLI output shows a configuration example of in-band management using GRT lookup and VPRN-to-GRT route leaking, based on Figure 2: GRT lookup and VPRN-to-GRT route leaking.

```
#--------------------------------------------------
echo "Policy Configuration"
#--------------------------------------------------
        policy-options
            begin
            prefix-list "NSP"
                prefix 1.1.1.1/24 exact
                prefix 2.2.2.2/24 exact
                prefix 192.168.255.0/32 exact
            exit
            policy-statement "NSP-leak"
                entry 10
                    from
                        prefix-list "NSP"
                    exit
                    action accept
                    exit
                exit
            exit
            commit
        exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 name "1" create
            description "Default customer"
        exit
        vprn 1 name "1" customer 1 create
            interface "NSP" create
            exit
        exit
        vprn 1 name "1" customer 1 create
            route-distinguisher 65650:1
            auto-bind-tunnel
                resolution-filter
                    gre
                exit
                resolution filter
            exit
            vrf-target target:65650:1
            interface "Mgmnt-interface" create
                address 192.168.255.0/32
                loopback
            exit
            static-route-entry 10.10.10.1/32
                grt
                    no shutdown
                exit
            exit
            grt-lookup
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

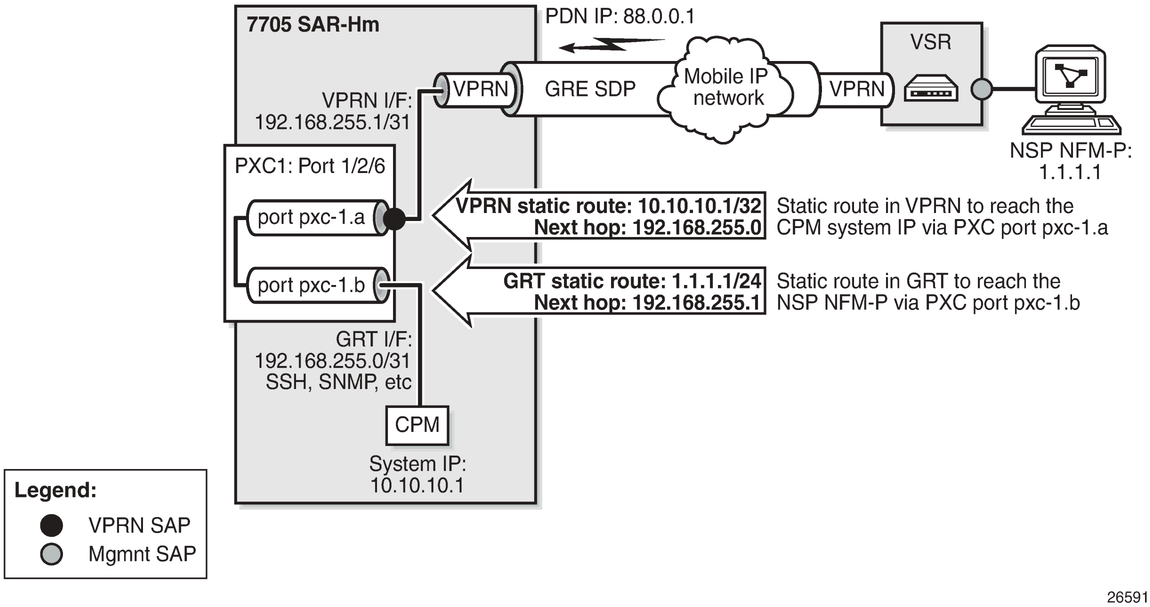
```
                    enable-grt
                        allow-local-management
                    exit
                    export-grt "NSP-leak"
                exit
                no shutdown
            exit
        exit
```

4.6.2 Port cross-connect (PXC)

For information about PXC, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*, "Port Cross-connect".

Figure 3: In-band management using a VPRN service and PXC shows an example of the operation of in-band management using a VPRN and PXC.

Figure 3: In-band management using a VPRN service and PXC



The following CLI example shows the configuration of the PXC based on the example shown in Figure 3: In-band management using a VPRN service and PXC.

Example:

```
A:DUT>config>port 1/2/6 shutdown
A:DUT>config>port-xc
A:DUT>config>port-xc# pxc 1 create
A:DUT>config>port-xc>pxc# port 1/2/6
A:DUT>config>port-xc>pxc# no shutdown
A:DUT>config>port-xc>pxc# exit all
A:DUT>>configure
A:DUT>>config# port pxc-1.a no shutdown
A:DUT>>config# port pxc-1.b no shutdown
A:DUT>>config# port 1/2/6 no shutdown
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

To ensure management traffic from the CPM can reach the NSP NFM-P over the VPRN, an interface in the Global Routing Table (GRT) is configured on one of the PXC ports. In the example shown in Figure 3: In-band management using a VPRN service and PXC, the GRT PXC port is port pxc-1.b. This port is looped internally together with PXC port pxc-1.a, the SAP of the in-band management VPRN. A router interface is required on port pxc-1.b:1 (VLAN 1) and used to route management traffic from the CPM toward the in-band management VPRN. A static route is configured in the GRT for the NSP NFM-P address, 1.1.1.1, with a next hop of the VPRN SAP, or port pxc-1.a:1. The following CLI output shows configuration examples in the GRT.

```
*A:DUT>config>service>vprn# info
----------------------------------------------
    interface "pxc"
        address 192.168.255.0/31
        port pxc-1.b:1
        no shutdown
    exit
...
    static-route-entry 1.1.1.1/24
        next-hop 192.168.255.1
            no shutdown
        exit
    exit
...
----------------------------------------------
*A:DUT>config>router#
```

A SAP interface on the other PXC port is required by the in-band management VPRN to route management traffic toward the CPM. A static route is configured in the VPRN for the CPM system IP address 10.10.10.1, with a next hop of the GRT interface port pxc-1.b:1. The following CLI output shows configuration examples for the VPRN.

```
*A:ALU-1>config>service# info
----------------------------------------------
...
    vprn 1 customer 1 create
        autonomous-system 65200
        route-distinguisher 65200:1
        auto-bind-tunnel
            resolution-filter
                gre
                exit
            exit
        vrf-target target:65200:1
        interface "pxc" create
                address 192.168.255.1/31
                sap pxc-1.a:1 create
                exit
        exit
        static-route-entry 10.10.10.1/32 next-hop 192.168.255.0
        no shutdown
    exit
...
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5 Secure Boot

The SR OS Secure Boot ensures that the software executed by the system is trusted and originated from Nokia IP Routing.

At every boot of the system, each step in the boot process verifies the digital signature of the next software element to boot for integrity and authenticity up to the SR OS operating system images. This boot sequence forms the chain of trust for Secure Boot.

Software image signatures use RSA-4096 keys and SHA-384 hashes.

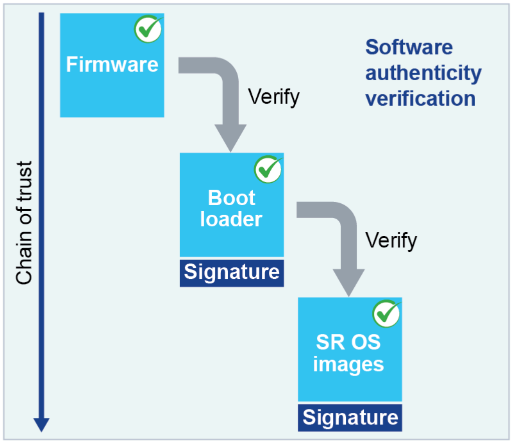
The Secure Boot chain is rooted in the platform CPM firmware based on UEFI specifications. As such, the Nokia Platform Key, Key Exchange Key, allowed and disallowed databases are provisioned when Secure Boot is activated to perform the required signature verification.

Firmware updates are also digitally signed and verified using the same principle. The signature verification of a firmware update is performed at boot time by the existing firmware before the firmware update can proceed.

5.1 Secure Boot chain

The Secure Boot chain of trust for SR OS platforms can be visualized with the following diagram.

Figure 4: Secure boot chain of trust



sw1396

The software images part of the Secure Boot chain varies among SR OS platforms. This list of software images per platform includes the Boot Loader, `boot.ldr` or `/EFI/BOOT/` and installer images, and the SR OS `*.tim` software images.

The software images part of the Secure Boot chain vary between SR OS platforms. This list of software images per platform includes the Boot Loader, `boot.ldr` or `/EFI/BOOT/` and installer images, and the SR OS `*.tim` software images.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.2 Activate Secure Boot

Secure Boot is enabled on the CPM card by providing the card slot, card serial number, and confirmation code command options.

Use the following command to activate Secure Boot.

```
admin system security secure-boot activate card "A" serial-number NS123456789 confirmation-code
 secure-boot-permanent
```

```
admin system security secure-boot activate
```

The following example shows the warning messages and a prompt for proceeding with Secure Boot activation.

Example

```
WARNING: CLI This operation will permanently activate secure boot on card A and cannot be
 reversed.
WARNING: CLI After activation, the system will only accept digitally signed software and
 will not boot using un-signed software.
WARNING: CLI This operation will immediately reset card A.
WARNING: CLI Configuration and/or Boot options may have changed since the last save.
Are you sure you want to continue (y/n)?
```

The card serial number and Secure Boot confirmation code are required to avoid activating Secure Boot by mistake in the network. The confirmation code is *secure-boot-permanent*.

The Secure Boot **activate** command verifies that the BOF primary image uses the same software release as the currently running software and automatically reboots the designated CPM card if the software release matches. Otherwise, an error is generated in the CLI.

Note: The system also verifies the boot.ldr version against the running software version on applicable platforms. These verifications are made to ensure that the entire boot chain up to the primary image supports Secure Boot before activating Secure Boot and rebooting the CPM.

WARNING: After Secure Boot is activated on the CPM, the capability is permanently enabled and cannot be disabled. The CPM permanently refuses to execute unsigned software for security reasons. As a result, it is not possible to downgrade to a software release published before the release that introduced Secure Boot for a specific platform.

WARNING: After Secure Boot is activated on the CPM, the capability is permanently enabled and cannot be disabled. The CPM permanently refuses to execute unsigned software for security reasons. As a result, it is not possible to downgrade to a software release published before the release that introduced Secure Boot for a specific platform.

5.3 Operational commands and logs

This section describes the following:

- Secure boot state

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

- Software update process
- Update Secure Boot variables

5.3.1 Secure Boot state

Secure Boot and UEFI variables Secure Boot keys status is available on the CPM.

Use the following command to display Secure Boot state information.

```
show card A detail
```

Output example

```
Hardware Data
    Secure boot status            : enabled
    UEFI variables status         : ok
```

where

- Secure Boot status — indicates if Secure Boot is enabled or disabled
- UEFI variables status — indicates if Secure Boot variables need updating

The system records at every boot in the security log if Secure Boot is enabled or disabled on the CPM. The following is an example of such a log message.

```
24 2023/05/17 06:09:03.140 EDT MAJOR: SECURITY #2241 Base Card A
"CPM A has booted with a secure-boot status of enabled"
```

Secure Boot UEFI variables can be obtained on the CPM card using the following command:

Secure Boot and UEFI variables Secure Boot keys status is available on the CPM.

Use the following command to display Secure Boot state information.

```
show card A detail
```

Output example

```
Hardware Data
    Secure boot status            : enabled
    UEFI variables status         : ok
```

where

- Secure Boot status — indicates if Secure Boot is enabled or disabled
- UEFI variables status — indicates if Secure Boot variables need updating

The system records at every boot in the security log if Secure Boot is enabled or disabled on the CPM. The following is an example of such a log message.

```
24 2023/05/17 06:09:03.140 EDT MAJOR: SECURITY #2241 Base Card A
"CPM A has booted with a secure-boot status of enabled"
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Secure Boot UEFI variables can be obtained on the CPM card using the following command:

```
tools dump system security secure-boot uefi-var card
```

The command displays the following x509 certificates and SHA-256 hash UEFI variables:

- Platform Key (PK)
- Key Exchange Key (KEK)
- Allowed Database (DB)
- Disallowed Database (DBx)

The command displays the following x509 certificates and SHA-256 hash UEFI variables:

- Platform Key (PK)
- Key Exchange Key (KEK)
- Allowed Database (DB)
- Disallowed Database (DBx)

5.3.2 Software update

After Secure Boot is enabled, and before upgrading to a new software release, the user must validate that the new software image is properly signed. The main reason for this additional verification on systems with Secure Boot enabled is because the system only boots Nokia-signed software images and does not boot unsigned or improperly signed images.

Use the following command to validate the signature of the TiMOS *.tim images contained in the **software-image** *url* location referenced in the command. This verification includes `cpm.tim`, `iom.tim`, `support.tim`, `both.tim`, `kernel.tim`, as well as the `boot.ldr` if present in CF3 directory.

```
admin system security secure-boot validate software-image url
```

5.3.3 Update Secure Boot variables

The system supports Secure Boot UEFI key updates and revocation using the following commands.

```
admin system security secure-boot update-key
admin system security secure-boot revoke-key
```

6 Router configuration

The 7705 SAR-Hm series of routers supports standard IP routing as covered in the following topics:

- IP router configuration
- Filter policy support

6.1 IP router configuration

This section describes the following functionality on 7705 SAR-Hm series nodes:

- PDN router interfaces
  - IPv4 PDN router interface
  - IPv6 PDN router interface
  - Static cellular system IPv4 mode
  - Static cellular interface IPv4 mode
  - Dynamic cellular interface IPv4 mode
  - Static cellular interface IPv6 mode
  - Dynamic cellular interface IPv6 mode
- DHCP client
  - Restrictions on configuring a router interface with DHCP client enabled
  - Route policy option for DHCP client
  - GRE termination for services over a DHCP client
- Router interface command reference
  - PDN router interface configuration and show command hierarchies
  - DHCP client configuration, show, tools, debug, and clear command hierarchies
  - PDN router interface command descriptions
  - DHCP client command descriptions

For general information about IP router configuration support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*, "IP router configuration":

- Configuring IP router command options
  - Interfaces
    - Network interface
    - Network domains
    - System interface
  - Router ID

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

  - Autonomous systems
  - Confederations
  - Exporting an inactive BGP route from a VPRN
  - DHCP relay
  - Internet protocol versions
- Aggregate next hop
- Invalidate next-hop based on ARP/neighbor cache state
- Router interface encryption with NGE
- Process overview
- Configuration notes
- Configuring an IP router with CLI
- System management tasks

For descriptions of IP router commands, see 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*.

6.1.1 PDN router interfaces

A packet data network (PDN) router interface is a type of router interface specific to a cellular port. PDN router interfaces are network-facing only and provide the main routing function over a cellular port. Each PDN connection that operates on a cellular port requires a PDN router interface.

A specific PDN router interface is associated with a specific SIM. Port 1/1/1 is always associated with SIM 1 and port 1/1/2 is always associated with SIM2. Therefore, a PDN router interface configured against port 1/1/1 is associated with SIM 1 and a PDN router interface configured against port 1/1/2 is associated with SIM 2. For information about configuring cellular ports, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*.

A PDN router interface is configured using the command **config>router>interface** *interface-name* **pdn**. A PDN router interface supports either IPv4 or IPv6 operation. The address type is determined by the protocol, either IPv4 or IPv6, configured for the PDN profile. A PDN profile must be configured and associated with the PDN router interface in order for a cellular port to attach to a cellular network. The address type is learned by the router interface during the PDN attachment process. For information about configuring a PDN profile, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*.

6.1.1.1 IPv4 PDN router interface

When a cellular port is configured for IPv4 operation, the associated PDN router interface is always an unnumbered interface; therefore, it cannot be directly configured with an IPv4 address. The IPv4 address assigned to a PDN interface must be specified from a loopback interface or learned directly from the cellular network during the cellular network attachment process. An IPv4 address specified from a loopback interface is used in the following ways:

- as the source IPv4 address for GRE-MPLS packets that are sent over a cellular port
- as the BGP **local-address** for BGP sessions over a cellular port

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- as the T-LDP **local-lsr-id** for T-LDP signaling sessions

An IPv4 PDN router interface can operate in one of three modes:

- static cellular system IPv4 mode
- static cellular interface IPv4 mode
- dynamic cellular interface IPv4 mode

The mode of operation dictates the way in which the IPv4 address is assigned to the PDN router interface and how it is used in conjunction with services.

For information about the types of services supported on an IPv4 PDN router interface and how an IPv4 PDN interface IP addresses is used by services, see Services over the cellular PDN interface.

An IPv4 PDN router interface supports Network Group Encryption (NGE). For information about NGE, see Network group encryption .

An IPv4 PDN router interface supports IPSec secure interfaces. For information about IPSec secure interfaces, see IPSec secured interface over cellular .

6.1.1.2 IPv6 PDN router interface

When a cellular port is configured for IPv6 operation, the associated PDN router interface is always a numbered interface.

An IPv6 PDN router interface can operate in one of two modes:

- static cellular interface IPv6 mode
- dynamic cellular interface IPv6 mode

The **ipv6>address** command is used to determine the mode of operation of the PDN router interface. When the address is specified, the IPv6 PDN router interface is operating in static cellular interface IPv6 mode. When the address is not specified, then it is operating in the dynamic cellular interface IPv6 mode.

For information about the types of services supported on an IPv6 PDN router interface, see Services over the cellular PDN interface.

An IPv6 PDN router interface supports IPSec secure interfaces. For information about IPSec secure interfaces, see IPSec secured interface over cellular .

An IPv6 PDN router interface does not support NGE.

6.1.1.2.1 Static routing on an IPv6 PDN router interface

When IPv6 is enabled on the PDN router interface, any static routes configured to use the PDN interface name as the next hop do not require the explicit configuration of the link-local address. This is because cellular networks do not require a next hop.

The following CLI output shows an example of a static route configuration on an IPv6-enabled PDN router interface.

```
*A:DUT# config# router
                interface "pdn-itf" pdn
                   port 1/1/1
                   ipv6
                        address 1::1/64
                   exit
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                exit
                static-route-entry ::/0
                   next-hop "pdn-itf"
                exit
           exit
     exit
```

6.1.1.3 Static cellular system IPv4 mode

In the static cellular system IPv4 mode of operation, the unnumbered interface under the PDN router interface is configured as the system interface. When the cellular port associated with the PDN interface attaches to the cellular network, the cellular network statically assigns an IP address to the node for the Access Point Name (APN) and associated installed Subscriber Identity Module (SIM). The system interface is then configured with the IP address that matches the cellular network-assigned IP address. The result is that the IP address provided by the cellular network for the PDN router interface and the system IP address of the node are identical.

A PDN router interface is considered operationally up only when the associated cellular port attaches to the network and an IP address is learned from the cellular attachment. The system checks whether the cellular network-assigned IP address matches the system IP address configured on the PDN interface. If it does not match, the PDN router interface is considered down and an alarm is raised.

The following CLI output shows an example of a PDN interface configured for static cellular system IPv4 mode.

```
*A:DUT# config# router
                interface "system"
                   address 88.0.0.1/32
                   no shutdown
                exit
                interface "pdn1-sim1" pdn
                   port 1/1/1
                   unnumbered "system"
                   no shutdown
                exit
           exit
      exit
```

When operating in static cellular system IPv4 mode, the following points apply.

- Only one cellular IP address can be used on the node. This affects dual SIM operation. If the PDN router interface of one of the dual SIM cellular ports is operating in static cellular system IPv4 mode, then the other PDN router interface must also operate in static cellular system IPv4 mode. The cellular network for each SIM must allocate the same system IP address when the node attaches to the cellular network over either cellular port.
- Some wireless service providers require that all packets entering their network from user equipment (UE) attached to their network have a source IP address that matches the IP address that the cellular network assigned to the UE. When this is a requirement and the node is using static cellular system IP mode, the PDN interface must be configured with an IP filter that allows only egress packets with a source IP address that matches the system IP address.
- The NSP NFM-P does not require an in-band management VPRN service to manage the node. Instead, the NSP NFM-P uses the system IP address to reach the node.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.1.1.4 Static cellular interface IPv4 mode

In the static cellular interface IPv4 mode of operation, the unnumbered interface configured under the PDN router interface is a loopback interface that is assigned a static address on the associated cellular port. This statically assigned IP address does not match the system IP address, which is a private address. When the cellular port associated with the PDN interface attaches to the cellular network, the cellular network assigns the same static IP address to the cellular port as the address assigned to the loopback address under the PDN router interface.

The cellular IP address assigned to the PDN router interface never changes after each subsequent cellular attachment. The static address assigned during the PDN attachment process is then used as the PDN router interface IP address for services operation. The PDN router interface is declared operationally up only when the PDN attachment completes and the IP address assigned by the cellular network matches the PDN router interface loopback address. If the address is not the same, the PDN interface stays operationally down and an alarm is raised.

The following CLI output shows an example of a PDN interface configured for static cellular interface IPv4 mode.

```
*A:DUT# config# router
                interface "pdn-loopback"
                   address 88.0.0.1/32
                   loopback
                   no shutdown
                exit
                interface "pdn1-sim1" pdn
                   port 1/1/1
                   unnumbered "pdn-loopback"
                   no shutdown
                exit
           exit
      exit
```

When operating in static cellular interface IPv4 mode, consider the following points.

- Some wireless service providers require that all packets entering their network from UE attached to their network have a source IP address that matches the IP address that the cellular network assigned to the UE. When this is a requirement and the node is using static cellular interface IPv4 mode, the PDN interface must be configured with an IP filter that allows only egress packets that have a source IP address that matches the IP address that was assigned during the PDN attachment. A filter must be configured on each PDN router interface that requires filtering.
- The system IP address used by the NSP NFM-P to manage the node is a private IP address. An in-band management VPRN service is required for the NSP NFM-P to reach the node.

6.1.1.5 Dynamic cellular interface IPv4 mode

In the dynamic cellular interface IPv4 mode of operation, the unnumbered interface configured under the PDN router interface is a loopback interface that has no IP address assigned to it. When the cellular port associated with the PDN interface attaches to the cellular network, the cellular network assigns a dynamic IP address to the cellular port, which is then used as the IP address for the loopback interface under the PDN router interface.

Because cellular IP address allocation is dynamic, the address changes during every PDN attachment. Because the loopback interface associated with the PDN router interface is not configured with any IP

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

address, this allows the node to learn the IP address assigned during the PDN attachment process and then assign that address to the loopback interface. The PDN router interface remains fixed to that address until the cellular port goes down and another PDN attachment is performed. This mode of operation is useful in applications where using dynamic address pools simplifies management and deployment of large numbers of nodes.

In this mode, the PDN router interface is operationally up when the system verifies that the IP address assigned to the interface does not conflict with any other IP address configured on the system. If there is a conflict, the PDN router interface is kept down.

The following CLI output shows an example of a PDN router interface configured for dynamic cellular interface IPv4 mode.

```
*A:DUT# config# router
                interface "pdn1-loopback"
                   loopback
                   no shutdown
                exit
                interface "pdn1-sim1" pdn
                   port 1/1/1
                   unnumbered "pdn-loopback"
                   no shutdown
                exit
           exit
      exit
```

When using dynamic cellular interface IPv4 mode, consider the following points:

- IP/MPLS services cannot be anchored to a fixed address on the node. Instead, only those IP/MPLS services that support dynamic IP address learning and behaviors are supported, such as VPRNs with auto-bind or Layer 2 services using pseudowire templates configured with **auto-gre-sdp**. See Services overview for more information.
- Some wireless service providers require that all packets entering their network from UE attached to their network have a source IP address that matches the IP address that the cellular network assigned to the UE. When this is a requirement, dynamic cellular interface IPv4 mode should not be used; instead, static cellular interface IPv4 mode should be used. When dynamic cellular interface IPv4 mode is used, there is no way to ensure all packets will meet the source IP address requirement as the node cannot filter a dynamically changing source IP address.
- The system IP address used by the NSP NFM-P to manage the node is a private IP address. An in-band management VPRN service is required for the NSP NFM-P to reach the node.

6.1.1.6 Static cellular interface IPv6 mode

In the static cellular interface IPv6 mode of operation, the PDN router interface IPv6 address is configured using the **config>router>interface** *interface-name* **pdn>ipv6>address** command. The cellular IP address assigned to the PDN router interface is never expected to change after each subsequent attachment to the cellular network. The address configured for the PDN router interface must be within the subnet of the network-assigned static IPv6 address upon PDN attachment, and the configured address cannot be the exact address assigned during the attachment. If the configured address is not within the subnet of the network-assigned IPv6 address or matches the network-assigned IPv6 address, then an alarm is raised and the PDN router interface is kept down.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The following CLI output shows an example of a PDN interface configured for static cellular interface IPv6 mode.

```
A:DUT# config# router
        interface "pdn1-sim1" pdn
            port 1/1/1
            ipv6
                address fd00:1:1:1::1/64
            exit
            no shutodwn
        exit
    exit
exit
```

When operating in static cellular interface IPv6 mode, consider the following points:

- GRE-MPLS based services are not supported as those packets use IPv4 addresses.
- IPSec secure interfaces are supported.
- Some wireless service providers require that all packets entering their network from UE attached to their network have a source IP address that is within the IPv6 subnet assigned during the PDN attachment process. When this is a requirement and the node is using static cellular interface IPv6 mode, the PDN interface must be configured with an IP filter that allows only egress packets that have a source IP address that is within the subnet that was assigned during the PDN attachment. A filter must be configured on each PDN router interface that requires filtering.
- The system IP address used by the NSP NFM-P to manage the node is a private IPv4 address. An in-band management VPRN service is required for the NSP NFM-P to reach the node.

6.1.1.7 Dynamic cellular interface IPv6 mode

In the dynamic cellular interface IPv6 mode of operation, the PDN router interface is not configured with an IPv6 address using the **config>router>interface** *interface-name* **pdn>ipv6>address** command. Instead, the IP address and subnet is learned by the PDN router interface each time the cellular interface attaches to the network. The IP address can change with each attachment. This mode of operation is useful in applications where using a dynamic address pool simplifies the management and deployment of large numbers of nodes.

Upon PDN attachment, the system dynamically allocates an IPv6 address that exists within the subnet of the IPv6 address assigned by the network during the cellular attachment. The PDN router interface remains fixed to that address until the cellular port goes down and another cellular attachment is performed.

In this mode, the PDN router interface is operationally up when the system verifies that the IP address and subnet assigned to the interface does not conflict with any other IP address and subnet configured on the system. If there is a conflict, the PDN router interface is kept down.

The following CLI output shows an example of a PDN router interface configured for dynamic cellular interface IPv6 mode.

```
*A:DUT# config# router
          interface "pdn1-sim1" pdn
             port 1/1/1
             ipv6
             exit
             no shutdown
         exit
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
    exit
exit
```

When using dynamic cellular interface IPv6 mode, the following points apply.

- GRE-MPLS based services are not supported as those packets use IPv4 addresses.
- IPSec secure interfaces are supported.
- Some wireless service providers require that all packets entering their network from UE attached to their network have a source IP address that is within the subnet -assigned IPv6 address and the subnet assigned to the UE during the cellular network attachment. When this is a requirement, dynamic cellular interface IPv6 mode should not be used; instead, static cellular interface IPv6 mode should be used. When dynamic cellular interface IPv6 mode is used there is no way to ensure that all packets will meet the source IP address requirement as the node cannot filter a dynamically changing source IP address.
- The system IP address used by the NSP NFM-P to manage the node is a private IPv4 address. An in-band management VPRN service is required for the NSP NFM-P to reach the node.

6.1.2 DHCP client

In the base router context, Ethernet ports and the WLAN station port can be configured with a router interface that supports a DHCP client. When the node operates as a DHCP client, it learns the IP address of the interface via dynamic IP address assignment. The DHCP client functionality is enabled by issuing the **no shutdown** command on the DHCP client in the **config>router>interface>autoconfigure>dhcp-client** context. The following output shows an example of a router interface enabled as a DHCP client.

```
*A:DUT# config# router interface "station-wlan-ifc"
          port 1/4/4
          autoconfigure dhcp-client
                no shutdown
            exit
          exit
```

The 7705 SAR-Hm supports up to three DHCP clients per node, one on the WLAN station port and two on Ethernet ports. The 7705 SAR-Hmc supports up to three DHCP clients on Ethernet ports.

When the DHCP client is enabled, changes to the DHCP client configuration take effect when the **shutdown** command is issued followed by the **no shutdown** command.

If DHCP relay configurations exist on the node, the DHCP client cannot be enabled until the DHCP relay configurations are removed. Similarly, if DHCP client configurations exist on the node, DHCP relay cannot be enabled until the DHCP client configurations are removed.

The DHCP client only supports IPv4.

When the DHCP client first becomes operational, learns an IP address from a remote DHCP server using a DHCP DISCOVER message.

The node will only send a DHCP DISCOVER message if:

- the DHCP client is enabled and the router interface is operationally up. Shutting down the DHCP client forces the release of the IP address.
- a DHCP NAK message is received from the DHCP server that invalidates the previous DHCP DISCOVER message or any existing lease

When a DHCP client is shut down, all cached values (such as IP addresses and DHCP options) are cleared. They are rediscovered by issuing the **no shutdown** command.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

If the port comes operationally up while the DHCP client is enabled and a DHCP discovery was not previously completed or a DHCP release was previously issued, then DHCP discovery is performed. If the port comes operationally up while the DHCP client is enabled and there was a previously completed DHCP discovery, then the DHCP client performs a DHCP REQUEST using the previously cached DHCP information from the discovery.

The operator can force a rediscovery procedure by executing the **restart** command in the **tools>perform>router>autoconfigure>dhcp-client interface** context.

The requested DHCP lease time can be configured using the CLI; however, the DHCP server can override this value. The node tracks the DHCP lease time and sends a DHCP REQUEST when half the lease time has elapsed. An IP address lease can be renewed manually using the **tools>perform>router>autoconfigure>dhcp-client interface lease-renew** command.

If the router interface goes down, the DHCP client parameters are cached for the interface. When the interface comes back up, if an IP address has been allocated and the lease time has not expired, the DHCP router interface will send a DHCP REQUEST to confirm that it can continue to use the IP address associated with the lease.

DHCP options must be configured in the CLI to make use of options received by the DHCP server. Any options received from the DHCP server are ignored if the corresponding options are not specified in the CLI. The DHCP client options are **router**, **static-route**, and **dns-server**. They are configured in the **config>router> interface>autoconfigure>dhcp-client>request-options** context.

The operator can use the **show>router>route-table protocol dhcp-client** command to view the active routes in the routing table that have been learned by the DHCP client. If the same route is received from more than one DHCP client, the route received from the DHCP server with the lowest ID (option 54) is installed in the route table.

The operator can use the **show>router>dns** command to view whether the DNS server has been configured to send request messages to the DHCP server. The node supports up to six DNS server entries learned by the DHCP clients. Only the first six DNS servers are stored by the node; any subsequent DNS servers that are learned will be ignored.

The CLI provides the option to use the router from the DHCP OFFER as the default gateway. In some scenarios, the router that is reachable via the WLAN port or an Ethernet port will be the default gateway. In other scenarios, the cellular interface will have reachability to the default gateway. The DHCP client **router** CLI option (under **request-options**) enables the router request option in the DHCP OFFER message. If the **router** option is enabled, the default gateway is assigned by the DHCP server.

The DHCP DISCOVER message sent from the node to the DHCP server contains the following options:

- chaddr—the MAC address of the client, either the WLAN or Ethernet port
- Option 51—the configured IP address lease time
- Option 53—the DHCP message type (DISCOVER)
- Option 60—a user-configurable vendor class identifier, either a hexadecimal string or an ASCII string
- Option 61—a user-defined client identifier: a hexadecimal string, an ASCII string, an interface name, or the client MAC address
- Option 55—the parameter request list:
  - Option 1—the subnet mask value
  - Option 3—the router option, a list of IP addresses for routers on the client subnet (unused if not enabled in the CLI)
  - Option 54—the DHCP server address

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The DHCP OFFER message from the DHCP server must contain the following options at a minimum:

- yiaddr—the DHCP router interface IP address
- Option 1—the subnet mask value
- Option 3—the router option, a list of IP addresses for routers on the client subnet
- Option 51—the configured IP address lease time
- Option 53—the DHCP message type (OFFER)
- Option 54—the DHCP server address

When responding to the server DHCP OFFER or when extending the time of an existing lease, the DHCP REQUEST message sent from the node to the DHCP server contains the following options:

- chaddr—the client MAC address
- Option 50—the requested IP address; this address is the same as the address contained in the yiaddr field that was received in the DHCP OFFER message
- Option 53—the DHCP message type (REQUEST)
- Option 54—the DHCP server address; this address is the same as the address received in the OFFER message
- Option 51—the IP address lease time; this value is the same as the lease time received in the OFFER message
- Option 60—the vendor class identifier; this value is the same as the vendor class identifier in the DISCOVER message
- Option 61—the client identifier; this value is the same as the client identifier in the DISCOVER message
- Option 55—the parameter request list:
  - Option 1—the subnet mask value
  - Option 3—the router option (unused if not enabled in the CLI)
  - Option 6—the DNS server option (unused if not enabled in the CLI)
  - Option 54—the DHCP server address
  - Option 121—the static-route option (unused if not enabled in the CLI)

When the DHCP client is shut down, a DHCP RELEASE message is sent to the DHCP server.

For BGP peers to other nodes behind the WLAN AP, the BGP local address can be set using the router interface name where the DHCP client is configured so that changes in the interface address because of DHCP messages are reflected in the local address of BGP sessions using this interface as the local address. For information about configuring services over a router interface enabled as a DHCP client, see Services over Ethernet with DHCP client.

6.1.2.1 Restrictions on configuring a router interface with DHCP client enabled

When a DHCP client is enabled on a router interface, the following protocol and services are supported on this interface:

- BGP with local-address set to this interface name
- Layer 3 VPRN services using mp-BGP
- Layer 2 VPLS/VPWS services using BGP-VPLS and BGP-VPWS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- Static routing using this interface as the next-hop
- IPsec secured interface

Note: Other routing protocols, unicast and multicast-based services, and other functionality not specified in the preceding list may be configurable, but are not supported on a DHCP client-enabled interface.

When a DHCP client is enabled on a router interface, the following commands cannot be configured in the **config>router>interface** context:

- **address**
- **secondary**
- **dhcp**
- **unnumbered**
- **loopback**

If any of the commands listed above are enabled, the **no shutdown** command is not available for the DHCP client until the commands are removed.

6.1.2.2 Route policy option for DHCP client

Routes can be imported from the DHCP client to other routing protocols with the **config>router>policy-options>policy-statement>entry>from>protocol dhcp-client** command.

6.1.2.3 GRE termination for services over a DHCP client

A router interface configured as a DHCP client supports the following service types: VLL, VPLS, and VPRN. These services use a GRE SDP as a transport tunnel.

When a DHCP client is enabled on a router interface and an address is learned by the client, there is no configuration required in order to terminate GRE SDPs on that interface IP address. GRE termination is enabled on a DHCP client address when the client learns the address. For information about configuring services over a router interface enabled as a DHCP client, see Services over Ethernet with DHCP client.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.1.3 Router interface command reference

- PDN router interface configuration and show command hierarchies
- DHCP client configuration, show, tools, debug, and clear command hierarchies
- PDN router interface command descriptions
- DHCP client command descriptions

6.1.3.1 PDN router interface configuration and show command hierarchies

The following PDN router interface commands are supported on the 7705 SAR-Hm series of routers.

For a description of the commands shown in black text, see 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*.

The commands shown in red text apply specifically to the PDN interface on the 7705 SAR-Hm series and are described in this guide.

```
config
    - router [router-name]
        - [no] interface interface-name pdn
            - cpu-protection policy-id
            - no cpu-protection
            - description description-string
            - no description
            - [no] enable-ingress-stats
            - group-encryption
            - no group-encryption
                - encryption-keygroup keygroup-id direction {inbound | outbound}
                - no encryption-keygroup direction {inbound | outbound}
                - ip-exception filter-id direction {inbound | outbound}
                - no ip-exception direction {inbound | outbound}
            - hold-time
                - up ip seconds
                - no up ip
                - down ip seconds [init-only]
                - no down
            - icmp
                - [no] mask-reply
                - param-problem [number seconds]
                - no param-problem
                - redirects [number seconds]
                - no redirects
                - ttl-expired [number seconds]
                - no ttl-expired
                - unreachables [number seconds]
                - no unreachables
            - if-attribute
                - [no] admin-group group-name [group-name...(up to 5 max)]
                - no admin-group
                - [no] srlg-group group-name [group-name...(up to 5 max)]
                - no srlg-group
            - ingress
                - filter ip ip-filter-id
                - no filter ip ip-filter-id
            - ip-mtu octets
            - no ip-mtu
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
             - [no] ipv6
                 - address ipv6-address/prefix-length [eui-64] [track-srrp srrp-instance]
 [modifier cga-modifier] [dad-disable] [primary-preference primary-reference]
                 - no address ipv6-address/prefix-length
             - [no] ntp-broadcast
             - port port-id
             - no port
             - qos network-policy-id [egress-port-redirect-group queue-group-name] [egress-
instance instance-id]] [ingress-fp-redirect-group queue-group-name ingress-instance instance-
id]
             - no qos
             - [no] shutdown
             - tos-marking-state {trusted | untrusted}
             - no tos-marking-state
             - unnumbered [ip-addr | ip-int-name]
             - no unnumbered
```

```
show
    - router interface interface-name
```

6.1.3.2 DHCP client configuration, show, tools, debug, and clear command hierarchies

The following router interface commands are supported on the 7705 SAR-Hm series of routers for a DHCP client in the IPv4 mode of operation.

The commands shown in red text apply specifically to a DHCP client on the 7705 SAR-Hm series and are described in this guide.

For a description of the commands shown in black text, see 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*.

```
config
    - router [router-name]
        - [no] interface interface-name
            - autoconfigure
                - dhcp-client
                    - class-id [hex hex-string] [string ascii-string]
                    - no class-id
                    - client-id [hex hex-string] [interface] [string ascii-string] [use-mac]
                    - no client-id
                    - lease-time [days days] [hrs hours] [min minutes] [sec seconds] [infinite]
                    - request-options
                        - [no] dns-server
                        - [no] router
                        - [no] static-route
                    - [no] shutdown
```

```
show
    - router
        - autoconfigure
            - dhcp-client interface ip-int-name
            - dhcp-client interface ip-int-name routes
            - dhcp-client interface ip-int-name statistics
        - interface interface-name detail
        - dns
        - route-table [family] [ip-prefix[/prefix-length] [longer | exact | protocol protocol-
name] [instance instance-id] [all] [next-hop-type type] [qos] [alternative]
        - route-table [family] summary
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
        - route-table family [ip-prefix[/prefix-length]] [longer | exact | protocol protocol-
name] [instance instance-id] extensive [all]
```

```
tools
    - dump
        - router
            - autoconfigure
                    - dhcp-client interface ip-int-name offer
                    - dhcp-client interface ip-int-name offer config-apply-status
                    - dhcp-client interface ip-int-name offer raw
```

```
tools
    - perform
        - router
            - autoconfigure
                - dhcp-client interface ip-int-name lease-renew
                - dhcp-client interface ip-int-name restart
```

```
debug
    - router
            - autoconfigure
                - dhcp-client interface ip-int-name
                    - [no] events
                    - [no] packet
                        - detail-level {low | medium | high}
                        - no detail-level
                        - mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
                        - no mode
                    - [no] rtm
```

```
clear
    - router
        - autoconfigure
            - dhcp-client interface ip-int-name statistics
```

6.1.3.3 PDN router interface command descriptions

The commands and parameters described in this section apply specifically to the PDN router interface on the 7705 SAR-Hm series of routers. All other applicable commands, as listed in PDN router interface configuration and show command hierarchies , are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

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* are supported on the 7705 SAR-Hm series of routers.

interface

Syntax

interface *interface-name* **pdn**

no interface pdn

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Context

config>router

Description

This command creates a logical IP router interface for the packet data network (PDN). PDN router interfaces are always network-facing interfaces. When created, attributes such as IP address, port, or system can be associated with the IP interface.

A PDN router interface can be configured for each cellular port.

The **no** form of the command removes the interface.

Parameters

interface-name

an alphanumeric character string describing the interface name, up to a maximum of 32 characters. The interface name must begin with a letter.

pdn

a mandatory keyword specifying that the interface represents a PDN

port

Syntax

port *port-id*

no port

Context

config>router>interface

Description

This command binds the PDN router interface to a physical port. The default value is the only supported port identifier.

Default

1/1/1

Parameters

port-id

a value equal to the cellular port identifier on the 7705 SAR-Hm series, configured in the **config>port** context and in the format *slot/mda/port*

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

router

Syntax

router interface *interface-name*

Context

show

Description

This command displays PDN router interface information.

Output

The following output is an example of PDN router interface information.

Output example

```
*A:Dut# show router interface "pdntest"
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm       Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                  PfxState
-------------------------------------------------------------------------------
pdntest                          Up        Down/Down   Pdn     n/a
   -                                                           -
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:Dut#
```

6.1.3.4 DHCP client command descriptions

The commands and parameters described in this section apply specifically to a DHCP client operating in IPv4 mode on the 7705 SAR-Hm series of routers. All other applicable commands, as listed in DHCP client configuration, show, tools, debug, and clear command hierarchies, are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

autoconfigure

Syntax

autoconfigure

Context

config>router>interface

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Description

This command enables the context to autoconfigure a DHCP client.

dhcp-client

Syntax

dhcp-client

Context

config>router>interface>autoconfigure

Description

This command enables the context to configure DHCP client parameters.

class-id

Syntax

class-id [**hex** *hex-string*][**string** *ascii-string*]

no class-id

Context

config>router>interface>autoconfigure>dhcp-client

Description

This command configures the vendor class identifier (option 60) for the DHCP client.

The **no** form of the command deletes the vendor class identifier configuration.

Default

n/a

Parameters

hex-string

specifies the vendor class identifier for the DHCP client as a hexadecimal string

Values 0x0 to 0xFFFFFFFF (maximum of 254 hex nibbles)

ascii-string

specifies the vendor class identifier for the DHCP client as an ASCII string

Values 127 characters maximum

client-id

Syntax

client-id [**hex** *hex-string*][**interface**][**string** *ascii-string*][**use-mac**]

no client-id

Context

config>router>interface>autoconfigure>dhcp-client

Description

This command configures the identifier for the DHCP client (option 61).

The **no** form of the command deletes the client identifier configuration.

Default

use-mac

Parameters

hex-string

specifies the client identifier as a hexadecimal string

Values 0x0 to 0xFFFFFFFF (maximum of 254 hex nibbles)

interface

specifies the IPv4 interface name as the client identifier

ascii-string

specifies the client identifier as an ASCII string

Values 127 characters maximum

use-mac

specifies the IPv4 MAC address of the associated port as the client identifier

lease-time

Syntax

lease-time [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**infinite**]

Context

config>router>interface>autoconfigure>dhcp-client

Description

This command configures the lease time granted by the DHCP server to the DHCP client.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Default

1 day

Parameters

days

specifies the lease time in days

Values 0 to 3650

hours

specifies the lease time in hours

Values 0 to 23

minutes

specifies the lease time in minutes

Values 0 to 59

seconds

specifies the lease time in seconds

Values 0 to 59

infinite

specifies that the lease never expires

request-options

Syntax

request-options

Context

config>router>interface>autoconfigure>dhcp-client

Description

This command configures the DHCP options for the request messages sent to the DHCP server.

Default

n/a

dns-server

Syntax

[**no**] **dns-server**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Context

config>router>interface>autoconfigure>dhcp-client>request-options

Description

This command enables the DNS server request option in the DHCP OFFER message from the DHCP server if the server supports it. If this option is enabled, it specifies a list of DNS servers available to the client.

The **no** form of the command disables DNS server as a request option.

Default

n/a

router

Syntax

[**no**] **router**

Context

config>router>interface>autoconfigure>dhcp-client>request-options

Description

This command enables the router request option in the DHCP OFFER message from the DHCP server if the server supports it. If this option is enabled, the default gateway is assigned by the DHCP server.

The **no** form of the command disables router as a request option.

Default

n/a

static-route

Syntax

[**no**] **static-route**

Context

config>router>interface>autoconfigure>dhcp-client>request-options

Description

This command enables the static route request option in the DHCP OFFER message from the DHCP server if the server supports it. If this option is enabled, it specifies a list of classless static routes (that is, the destination network addresses in these static routes include subnet masks) that a client should add to its routing table.

The **no** form of the command disables static route as a request option.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Default

n/a

shutdown

Syntax

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

Context

config>router>interface>autoconfigure>dhcp-client

Description

This command administratively disables the DHCP client.

The **no** form of the command enables the DHCP client.

Default

n/a

dhcp-client

Syntax

dhcp-client interface *ip-int-name*

dhcp-client interface *ip-int-name* **routes**

dhcp-client interface *ip-int-name* **statistics**

Context

show>router>autoconfigure

Description

This command displays DHCP client information.

Parameters

ip-int-name

displays DHCP client information associated with the specified IP interface name

routes

displays routing table information for routes received by the DHCP protocol

statistics

displays DHCP client statistics

Output

The following outputs are examples of DHCP client information:

Use subject to Terms available at: www.nokia.com/terms.

- DHCP client information associated with the specified interface name (**Output example (for the specified interface name)**)
- DHCP client routing table information for routes received by the DHCP protocol (**Output example (for DHCP client routing table information)**)
- DHCP client statistics (**Output example (for DHCP client statistics)**)

Output example

Output example (for the specified interface name)

```
*A:Dut-B# show router autoconfigure dhcp-client interface "to-dhcp"
===============================================================================
DHCP Client state
===============================================================================
Client IP address                 : 51.53.2.17/24
Client MAC address                : 90:3a:a0:f0:ba:d5
Server Identifier                 : 51.54.2.1
Router IP address                 : (Not Specified)
Primary DNS                       : 138.120.252.55
Secondary DNS                     : 138.120.252.57
Tertiary DNS                      : (Not Specified)
Lease acquired time               : 2021/05/06 23:09:46
Lease renew time                  : 2021/05/07 05:09:46
Lease rebind time                 : 2021/05/07 09:39:46
Lease end time                    : 2021/05/07 11:09:46
DHCP RFC protocol state           : bound
DHCP client user status           : established
Description                       : nexthop 51.53.2.1 is reachable (for
                                    routes 135.0.0.0/8)
===============================================================================
```

Output example (for DHCP client routing table information)

```
*A:Dut-B# show router autoconfigure dhcp-client interface "to-dhcp" routes
===============================================================================
DHCP client interface route table
===============================================================================
Prefix                                                  Status
  Next-hop
    (Reason)
-------------------------------------------------------------------------------
135.0.0.0/8                                             installed
  51.53.2.1
-------------------------------------------------------------------------------
No. of routes: 1
===============================================================================
```

Output example (for DHCP client statistics)

```
*A:Dut-B# show router autoconfigure dhcp-client interface "to-dhcp" statistics
===============================================================================
DHCP Client statistics
===============================================================================
DHCPDISCOVER messages                                    : 10
DHCPREQUEST messages                                     : 8
DHCPRELEASE messages                                     : 7
DHCPDECLINE messages                                     : 0
DHCPOFFER messages                                       : 8
DHCPACK messages                                         : 8
DHCPNAK messages                                         : 0
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
messages dropped                                         : 0
Statistics last cleared time                             : N/A
===============================================================================
```

autoconfigure

Syntax

autoconfigure

Context

tools>dump>router

Description

This command enables the context to display autoconfiguration information for debugging purposes.

dhcp-client

Syntax

dhcp-client interface *ip-int-name* **offer**

dhcp-client interface *ip-int-name* **offer config-apply-status**

dhcp-client interface *ip-int-name* **offer raw**

Context

tools>dump>router>autoconfigure

Description

This command displays IPv4 DHCP client information for debugging purposes.

Parameters

ip-int-name

the IP interface name associated with the DHCP client

offer

displays the contents of the OFFER message

config-apply-status

displays the configured DHCP options from the DHCP server OFFER message that are applied to the DHCP client and the status of these options

offer raw

displays the contents of the OFFER message in hexadecimal format

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

autoconfigure

Syntax

autoconfigure

Context

tools>perform>router

Description

This command enables the context to perform autoconfiguration operations.

dhcp-client

Syntax

dhcp-client interface *ip-int-name* **lease-renew**

dhcp-client interface *ip-int-name* **restart**

Context

tools>perform>router>autoconfigure

Description

This command performs IPv4 DHCP client lease operations.

Parameters

ip-int-name

the IP interface name associated with the DHCP client

lease-renew

performs DHCP client operations associated with lease renewals

restart

performs DHCP client operations associated with lease restarts

autoconfigure

Syntax

autoconfigure

Context

debug>router

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Description

This command enables the context to perform autoconfiguration debugging operations.

dhcp-client

Syntax

dhcp-client interface *ip-int-name*

Context

debug>router>autoconfigure

Description

This command enables debugging for an IPv4 DHCP client.

Parameters

ip-int-name

the IP interface name associated with the DHCP client

events

Syntax

[**no**] **events**

Context

debug>router>autoconfigure>dhcp-client

Description

This command enables or disables debugging for all DHCP client events.

packet

Syntax

[**no**] **packet**

Context

debug>router>autoconfigure>dhcp-client

Description

This command enables or disables debugging for all DHCP client packets.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

detail-level

Syntax

detail-level {**low** | **medium** | **high**}

no detail-level

Context

debug>router>autoconfigure>dhcp-client>packet

Description

This command sets the level of detail for packet tracing.

Parameters

low

specifies a low tracing detail level

medium

specifies a medium tracing detail level

high

specifies a high tracing detail level

mode

Syntax

mode {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}

no mode

Context

debug>router>autoconfigure>dhcp-client>packet

Description

This command specifies the types of packets to be debugged.

Parameters

dropped-only

specifies to debug dropped packets only

ingr-and-dropped

specifies to debug ingress packets and dropped packets

egr-ingr-and-dropped

specifies to debug egress packets, ingress packets, and dropped packets

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

rtm

Syntax

[**no**] **rtm**

Context

debug>router>autoconfigure>dhcp-client

Description

This command enables or disables debugging for the addition, removal, and modification of DHCP client routes to the system Route Table Manager.

autoconfigure

Syntax

autoconfigure

Context

clear>router

Description

This command enables the context to clear autoconfigured DHCP client information.

dhcp-client

Syntax

dhcp-client interface *ip-int-name* **statistics**

Context

clear>router>autoconfigure

Description

This command clears IPv4 DHCP client statistics.

Parameters

ip-int-name

the IP interface name associated with the DHCP client

statistics

clears DHCP client statistics

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.2 Filter policy support

For general information about filter policy support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*, "Filter Policies":

- ACL filter policy overview
  - Filter policy basics
    - Filter policy packet match criteria
    - IPv4/IPv6 filter policy entry match criteria
    - IP exception filters
    - Filter policy actions
    - Viewing filter policy actions
    - Filter policy statistics
    - Filter policy logging
    - Filter policy management
  - Filter policy advanced topics
    - Match list for filter policies
    - Filter policy scope and embedded filters
    - IP exception filters
- Configuring filter policies with CLI
  - Common configuration tasks
    - Creating an IPv4 filter policy
    - Creating an IPv6 filter policy
    - Creating an IPv4 exception filter policy
    - Creating an IPv6 exception filter policy
    - Creating a match list for filter policies
    - Applying filter policies
    - Creating a redirect policy
- Filter management tasks

For descriptions of filter commands, see 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*.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

7 Routing protocols

The 7705 SAR-Hm series of routers support routing protocols and routing functionality as covered in the following topics:

- BGP
- RIP
- OSPF
- Route policies

7.1 BGP

This section describes the following functionality:

- Using a router interface address as the BGP local address

For general information about BGP support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*, "BGP" :

- BGP overview
- BGP sessions
  - BGP session state
  - Detecting BGP session failures
    - Peer tracking
    - Bidirectional Forwarding Detection
  - High availability BGP sessions (BGP graceful restart only)
  - BGP session security
  - BGP address family support for different session types
  - BGP groups
- BGP design concepts
- BGP messages
- BGP path attributes
  - Origins
  - AS path
  - Next-hop
    - Unlabeled IPv4 unicast routes
    - Unlabeled IPv6 unicast routes
    - VPN-IPv4 routes
    - VPN-IPv6 routes

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

        - Next-hop resolution
        - Next-hop tracking
    - Local preference
    - Route aggregation path attributes
    - Community attributes
    - Route reflection attributes
    - 4-Octet AS attributes
    - AIGP metric
- BGP routing information base (RIB)
- BGP applications
    - BGP prefix origin validation
    - BGP route leaking
    - BGP optimal route reflection
- BGP configuration process overview
- Configuration notes
- Configuring BGP with CLI
- BGP configuration management tasks

For descriptions of BGP commands, see 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 Using a router interface address as the BGP local address

In cellular and WLAN networks, the router interface IP address can be assigned statically or dynamically. A cellular port supports different modes of operation depending on whether the IP address must be assigned statically or dynamically. See PDN router interfaces for information about the supported modes of operation on the PDN router interface.

When the PDN router interface is operating in dynamic cellular interface IP mode, the dynamically changing interface IP address must be reflected in BGP advertisements. Neighbor peers that are originating services that rely on BGP routing information to reach the local node must use the IP address of the PDN router interface on the local node in order to reach it. The local address for BGP sessions from the local node to neighbor peers must therefore match the IP address of the PDN router interface at all times, even after the IP address changes.

To facilitate a dynamically changing router interface IP address, the BGP **local-address** command must be configured with the name of the loopback interface used by the unnumbered interface under the PDN router interface instead of a fixed IP address. Using the loopback interface name, the SR OS will automatically assign the current IP address of the PDN router interface as the BGP **local-address** when the PDN router interface comes up (for example, when the cellular PDN interface learns the IP address during the cellular attachment procedure). This means that the BGP local address will inherit the loopback interface's dynamic address information and when routes are being advertised to peers, those peers will be able to route traffic toward this router's PDN router interface.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Configuring the loopback interface name used by the PDN router interface as the local address is available in both the **config>router>bgp>group** context and the **config>router>bgp>group>neighbor** context. For complete command syntax, description, and parameter information, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*, "configure router bgp commands".

When BGP sessions are using the loopback interface name that is used PDN router interface as the local address, the remote neighbor peer must use the **dynamic-neighbor** command in order to accept BGP sessions from 7705 SAR-Hm nodes that have dynamically changing router interface IP addresses.

When dual SIM operation is required, there are two PDN interfaces, one per cellular port associated with each SIM. At a minimum, two BGP sessions are required, one for each PDN interface. Each BGP session must be configured with the **local-address** using the loopback interface associated with each PDN router interface.

7.2 RIP

The 7705 SAR-Hm series of routers support RIP on Ethernet interfaces only.

For general information about RIP support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*, "RIP":

- RIP overview
- RIPng
- Common attributes
- RIP configuration process overview
- Configuration notes
- Configuring RIP with CLI
- RIP configuration management tasks

For descriptions of RIP commands, see 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*.

7.3 OSPF

The 7705 SAR-Hm series of routers support OSPF on Ethernet interfaces only.

For general information about OSPF support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*, "OSPF":

- Configuring OSPF
  - OSPF areas
  - OSPFv3 authentication
  - OSPF graceful restart helper
  - Virtual links
  - Neighbors and adjacencies
  - Link-state advertisements

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

  - Metrics
  - Authentication
  - IP subnets
  - Preconfiguration recommendations
  - Multiple OSPF instances
  - Multi-address support for OSPFv3
- SPF LSA filtering
- FIB prioritization
- Extended LSA support in OSPFv3
- Support of multiple instances of router information LSA in OSPFv2 and OSPFv3
- OSPF configuration process overview
- Configuration notes
- Configuring OSPF with CLI
- OSPF configuration management tasks

For descriptions of OSPF commands, see 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*.

7.4 Route policies

For general information about route policy support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*, "Route policies":

- Configuring route policies
- Route policy configuration process overview
- Configuration notes
- Configuring route policies with CLI
- Route policy configuration management tasks

For descriptions of route policy commands, see 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*.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

8 MPLS

The 7705 SAR-Hm series of routers support MPLS as described in Label Distribution Protocol .

T-LDP is required for VPLS and Epipe services that depend on T-LDP signaling for label distribution and control. See the Layer 2 and Layer 3 services chapter for more information about services supported on the 7705 SAR-Hm series.

8.1 Label Distribution Protocol

For general information about Label Distribution Protocol (LDP) support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide*, "Label Distribution Protocol":

- Label Distribution Protocol
  - Execution flow
  - Label exchange
  - Global LDP filters
  - Configuring multiple LDP LSR ID
  - T-LDP hello reduction
- TTL security for BGP and LDP
- Unnumbered interface support in LDP
  - Feature configuration
  - Operation of LDP over an unnumbered IP interface
    - Targeted LDP
- LDP graceful handling of resource exhaustion
  - User guidelines and troubleshooting procedures
- LDP process overview
- Configuring LDP with CLI
- LDP configuration management tasks

For descriptions of LDP commands, see 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*.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9 Services overview

Topics in this chapter include:

- Overview
- Service types
- Nokia service model
- Service entities
- Services over the cellular PDN interface
- Services over Ethernet with DHCP client
- Services with the WLAN interface

9.1 Overview

A service is a type of communication connection from one place to another. These communication connections have particular attributes and characteristics that are needed to provide a specific communications link through which an information flow or exchange can occur. The 7705 SAR-Hm series of routers support the following services:

- Layer 2 Virtual Leased Line (VLL) and BGP virtual private wire services (VPWS)
- Layer 2 virtual private LAN services (VPLS) and BGP VPLS services
- Layer 3 IP VPN services (VPRN)
- serial transport using raw socket and IP transport services
- transporting WLAN interface traffic over a service

The service model uses (logical) service entities to construct a service. These logical entities provide a uniform, service-centric configuration and management model for service provisioning (see Nokia service model for more information). Different services can be created on the same node at the same time, and each service is uniquely identified by a service ID.

The supported services provide connectivity between a service access point (SAP) on one node and a SAP on a remote node. A SAP is a logical point where data traffic enters and exits a service. SAPs on the node are associated with Ethernet ports, VLANs, access router interfaces, serial ports, or the WLAN interface.

A connection between two SAPs on the same router is known as a local service. A connection between SAPs on a local and a remote router is known as a distributed service. SAP-to-SAP local services are supported for Ethernet and WLAN-based services. SAP-to-SAP local services are not supported for serial port and raw socket IP transport services.

Distributed services use service destination points (SDPs) to direct traffic from a local router to a remote router through a service tunnel. An SDP is created on the local router and identifies the endpoint of a logical unidirectional service tunnel. Traffic enters the tunnel at the SDP on the local router and exits the tunnel at the remote router. Hence, a service tunnel provides a path from one service router to another.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Because an SDP is unidirectional, two service tunnels are needed for bidirectional communication between two service routers (one SDP on each router). The only supported SDP tunnel type is GRE-MPLS tunnels.

SDPs are configured on each participating service router or are auto-bound to the far-end router depending on the requirements and type of service. When configuring SDPs on the source router, the address of the destination router must be specified. When using the auto-bind function for SDPs, configuring individual SDPs between service routers is not required. The node uses BGP advertised information to perform the auto-bind SDP function to the far-end routers. For more information about auto-bind, see SDP binding.

After SDPs are created, they are bound to a specific service, or the service is enabled with auto-bind SDPs, to create a binding to the transport tunnels. In both cases, the SAPs that are part of the service use the bound SDPs as the transport for data traffic between nodes. The binding process is needed to associate the far-end devices to the service; otherwise, far-end devices are not able to participate in the service.

9.2 Service types

The 7705 SAR-Hm series of routers offers the following types of services:

- Virtual Leased Line (VLL) services
  - Ethernet VLL (Epipe)—a PWE3 Ethernet service over MPLS or GRE tunnels for Ethernet frames on 7705 SAR-Hm nodes.
- BGP Virtual Private Wire Services (VPWS)
  - BGP VPWS is a point-to-point Layer 2 VPN service based on RFC 6624 (Layer 2 Virtual Private Networks using BGP for Auto-Discovery and Signaling) which in turn uses the BGP pseudowire signaling concepts from RFC 4761, Virtual Private LAN Services Using BGP for Auto-Discovery and Signaling.
- Internet Enhanced Service (IES)
  - IES is a direct Internet access service where the SAP is assigned an IP interface for routed connectivity.
- Virtual Private LAN Service (VPLS)
  - VPLS provides a Layer 2 multipoint VPN service to end customers. Sites in a VPLS instance appear to be on the same LAN regardless of their location. The 7705 SAR-Hm series nodes can participate in BGP VPLS-based services and traditional T-LDP signaled services.
- Virtual Private Routed Network Service (VPRN)
  - VPRN provides a Layer 3 VPN service to end customers. VPRN services provide MP-BGP peering with other PEs, configurable QoS policy and filtering, and VRF import and export policies.

Table 3: Pseudowire service types lists the supported pseudowire (PW) service types. The values are as defined in RFC 4446.

Table 3: Pseudowire service types

PW service type (Ethertype)	Value
Ethernet tagged mode	0x0004
Ethernet raw	0x0005

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9.3 Nokia service model

The 7705 SAR-Hm series of routers is deployed at the customer provider edge (PE). Services are provisioned on the router in order to facilitate the transport of communications data across an IP/MPLS network using the Ethernet or wireless interfaces available on the node. The data is formatted so that it can be transported in encapsulation tunnels created using Layer 3 generic routing encapsulation (GRE) MPLS.

The Nokia service model has four main logical components, referred to as (logical) service entities. The entities are: applications, service types, service access points (SAPs), and service destination points (SDPs) (see Service entities). In accordance with the service model, the operator uses the (logical) service entities to construct an end-to-end service. The service entities are designed to provide a uniform, service-centric model for service provisioning. This service-centric design implies the following characteristics.

- Multiple services can be bound to a single application.
- Multiple service types can be bound to a single tunnel.
- Tunnel configurations are independent of the services they carry.
- Changes are made to a single service entity rather than to multiple ports on multiple devices. It is easier to change one tunnel rather than several services.
- The operational integrity of a service entity (such as a service tunnel or service endpoint) can be verified by one operation rather than through the verification of dozens of parameters, thereby simplifying management operations, network scalability, and performance.
- A failure in the network core can be correlated to specific subscribers and services.
- The following policies are applied to various services:
  - QoS policies
  - filter policies (IP and MAC)

Additional properties can be configured for bandwidth assignments and class of service on the appropriate entity.

9.4 Service entities

The basic (logical) service entities in the service model used to construct an end-to-end service are:

- Applications
- Service types
- Service access points (SAPs)
- Service Destination Points (SDPs)

Figure 5: Service entities and the service model shows an example of how the service entities relate to the service model. An application attachment point (for example, an Ethernet port, VLAN, or serial port) connects to a SAP. The SDPs define the entrance and exit points of service tunnels, which carry one-way traffic between the two routers (NOK-A and NOK-B). Configured SDPs are bound to a service or the service is auto-bound which automatically creates tunnels to far-end nodes. The binding of the service to SDPs is the final step in enabling the end-to-end service. In Figure 5: Service entities and the service model, the entrance and exit points are over the wireless interface.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

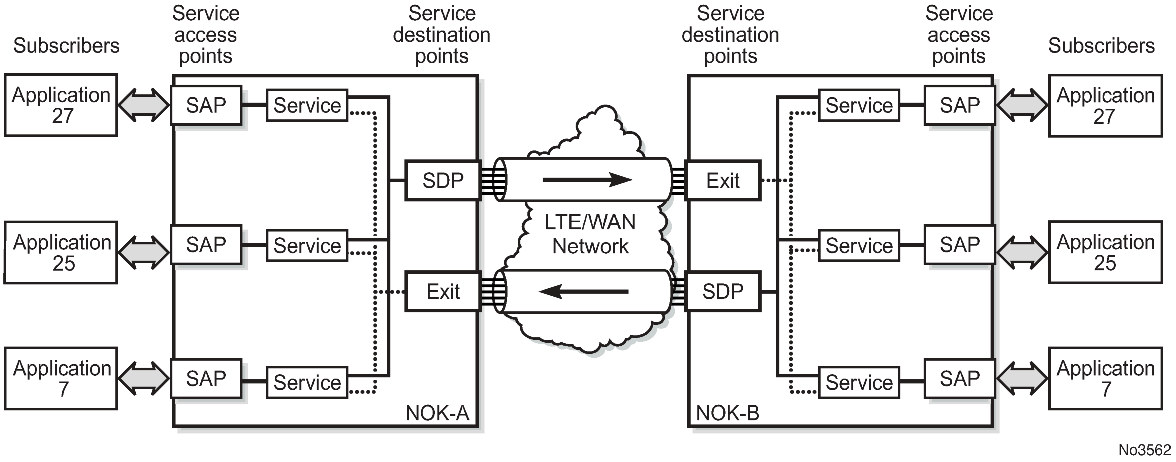
Traffic encapsulation occurs at the SAP and SDP. The 7705 SAR-Hm series supports the following SAP encapsulation types:

- Ethernet untagged or tagged
- IP
- raw serial character data on the serial ports

The 7705 SAR-Hm series supports GRE-MPLS encapsulation for SDPs.

For information about SAP encapsulation types, see SAP encapsulation types and identifiers. For information about SDP encapsulation types, see SDP encapsulation types.

Figure 5: Service entities and the service model



9.4.1 Applications

Every application must have a customer ID, which is assigned when the application service is created. To provision a service, a customer ID must be associated with the service at the time of service creation.

Note: The terms application, customers, and subscribers are used synonymously in this manual. When referring to SR OS manuals for more information, these terms may appear and are interchangeable.

9.4.2 Service types

Service types provide the traffic adaptation needed by customer attachment circuits (ACs). This (logical) service entity adapts customer traffic to service tunnel requirements. A VLL service is a point-to-point MPLS-based emulation service, also called Virtual Private Wire Service (VPWS). The 7705 SAR-Hm series provides Ethernet VLL (Epipe) service and BGP VPLS-based Layer 2 service.

The series also provides Ethernet layer (MAC-based) VPLS service (including management VPLS), raw socket IP transport service, as well as IP layer VPRN and IES services, that offer any-to-any connectivity within a Virtual Routing Domain or Generic Routing Domain, respectively.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9.4.2.1 Service names

A service ID number must be associated with a service at the time of service creation. When the service is created, an optional service name can be assigned to the service for use by commands that reference the service.

9.4.3 Service access points (SAPs)

Topics in this section include:

- SAP encapsulation types and identifiers
- SAP configuration considerations

A service access point (SAP) is the point at which a service begins (ingress) or ends (egress) and represents the access point associated with a service. A SAP may be a physical port or a logical entity within a physical port. For example, a SAP may be an Ethernet port or a VLAN that is identified by an Ethernet port and a VLAN tag. Each application service connection is configured to use only one SAP.

A SAP identifies the application interface point for a service on a service router. Figure 6: Service access point (SAP) shows two applications connected to the same service via two different SAPs. The SAP identifiers are 1/2/5 and 1/2/6, which represent the physical ports associated with these SAPs. The physical port information should be configured before provisioning a service. For more information about configuring a port, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*.

The 7705 SAR-Hm series supports VLL, VPWS, VPLS, and VPRN services. For each service type, the SAP has slightly different parameters; see Layer 2 and Layer 3 services for information.

In general, SAPs are logical endpoints that are local to the node and are uniquely identified by:

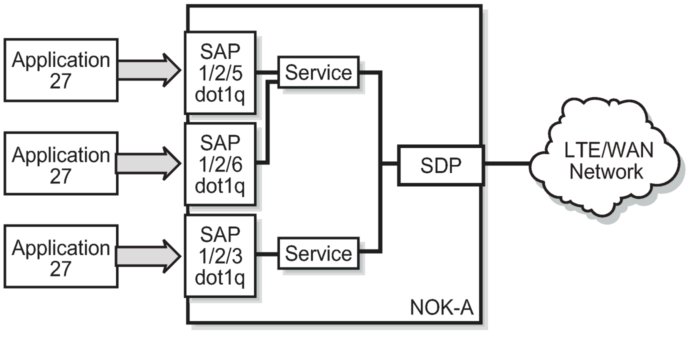
- the physical Ethernet port
- the physical serial port
- the encapsulation type for the service
- the encapsulation identifier (ID), which is the optional VLAN ID for Epipes

Depending on the encapsulation, a physical port can have more than one SAP associated with it (for example, a port may have several VLANs, where each VLAN has an associated SAP). SAPs can only be created on ports designated as "access" in the physical port configuration.

SAPs cannot be created on ports designated as core-facing "network" ports because these ports have a different set of features enabled in software.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Figure 6: Service access point (SAP)



9.4.3.1 SAP encapsulation types and identifiers

The SAP encapsulation type is an access property of the Ethernet port used for the service. It identifies the protocol that is used to provide the service.

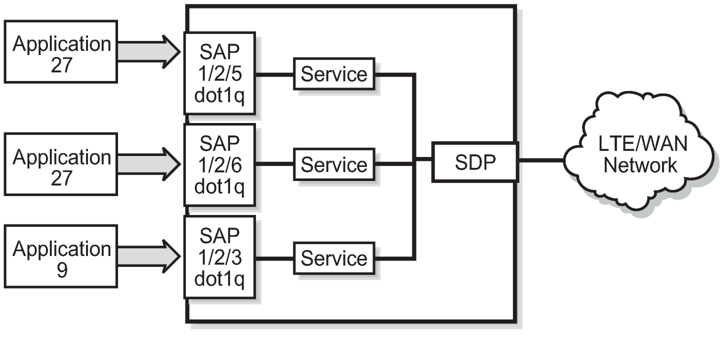
The encapsulation ID for Ethernet ports is an optional suffix that is appended to a *port-id* to specify a logical sub-element for a SAP. For example, *port-id:qtag1* represents a port that can be tagged to use IEEE 802.1Q encapsulation (referred to as dot1q), where each individual tag can identify with an individual service.

9.4.3.1.1 Ethernet encapsulations

The following encapsulation service options are available on Ethernet ports:

- null—supports a single service on the port; for example, where a single customer with a single service customer edge (CE) device is attached to the port.
- dot1q—supports multiple services for one customer or services for multiple customers (see Figure 7: Multiple SAPs on a single port). For example, dot1q could be used when the Ethernet port is connected to a multi-tenant unit device with multiple downstream customers. The encapsulation ID used to distinguish an individual service is the VLAN ID in the IEEE 802.1Q header.

Figure 7: Multiple SAPs on a single port



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9.4.3.1.1.1 Default SAP on a dot1q port

The 7705 SAR-Hm series of routers supports default SAP functionality on dot1q- encapsulated ports. On dot1q-encapsulated ports where a default SAP is configured, all packets with Q-tags not matching any other explicitly defined SAPs are assigned to the default SAP for transport. A default SAP is defined in the CLI using the character "*" as a Q-tag, where the "*" means "all".

One of the applications where the default SAP feature can be used is for an access connection of an application that uses the whole port to access Layer 2 services. The internal VLAN tags are transparent to the service. This (the use of a whole port) can be provided by a null-encapsulated port. A dedicated VLAN (not used by the user) can be used to provide management to this application.

In this type of environment, two SAPs logically exist, a management SAP and a service SAP. The management SAP can be created by specifying a VLAN tag that is reserved to manage the application. The service SAP covers all other VLANs and behaves as a SAP on a null-encapsulated port.

There are a few constraints related to the use of a default SAP on a dot1q-encapsulated port:

- The default SAP is supported only on VPLS, and Epipe VLL and VPWS services and cannot be created in IES and VPRN services because IES and VPRN services cannot preserve VLAN tag markings.
- For VPLS SAPs with STP enabled, STP listens to untagged and null-tagged BPDUs only. All other tagged BPDUs are forwarded like other customer packets. This is the same behavior as null-encapsulated ports.
- IGMP snooping is not supported on a default SAP. By not allowing IGMP snooping of a default SAP, all IGMP packets will be transparently forwarded.
- The default SAP and the SAP defined by explicit null encapsulation are mutually exclusive (for example, 1/1/1:* and 1/1/1:0 are mutually exclusive). This avoids conflict as to which SAP untagged frames should be associated with.

9.4.3.2 SAP configuration considerations

In addition to being an entry or exit point for service traffic, a SAP has to be configured for a service and, therefore, has properties. When configuring a SAP, consider the following.

- A SAP is a local entity and is only locally unique to a specific device. The same SAP ID value can be used on another service router.
- There are no default SAPs. All subscriber service SAPs must be created.
- The default administrative state for a SAP at creation time is administratively enabled.
- When a SAP is deleted, all configuration parameters for the SAP are also deleted.
- A SAP is owned by and associated with the service in which it is created.
- An Ethernet port with a dot1q encapsulation type means that the traffic for the SAP is identified based on a specific IEEE 802.1Q VLAN ID value. The VLAN ID is stripped off at SAP ingress and the appropriate VLAN ID is placed on at SAP egress. As a result, VLAN IDs only have local significance, so the VLAN IDs for the SAPs for a service need not be the same at each SAP.
- If a port is administratively shut down, all SAPs on that port will be operationally out of service.
- A SAP cannot be deleted until it has been administratively disabled (shut down).
- Each SAP can have one of the following policies assigned to it:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- Ingress QoS policy
- Egress QoS policy
- Ingress filter policy (for Epipe VLL and VPWS SAPs, VPLS SAPs, VPRN SAPs, IES SAPs, and IES in-band management SAPs)
- Egress filter policy (for VPRN and IES SAPs, and for VPLS SAPs (Ethernet SAPs only))

9.4.4 Service Destination Points (SDPs)

Topics in this section include:

- SDP binding
- Spoke and mesh SDPs
- SDP encapsulation types
- SDP ping

An SDP identifies the endpoint of a logical unidirectional service tunnel. The service tunnel provides a path from one service router to another.

In more general terms, SDP refers to the service tunnel itself. The SDP terminates at the far-end router, which is responsible for directing the flow of packets to the correct service egress SAPs on that device.

Note: In this document and in command line interface (CLI) usage, SDP is defined as Service Destination Point. However, it is not uncommon to find the term SDP defined in several different ways, as in the following list. All variations of SDP have the same meaning:

- Service Destination Point
- Service Distribution Point
- Service Destination Path
- Service Distribution Path
- Service Delivery Path

When an SDP is bound to a service, the service is referred to as a distributed service. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP binding that binds the service to the service tunnel. Multiple SDPs to different far-end nodes are bound to a service to provide transport for SAPs to other nodes participating in that service.

When configured, an SDP has the following characteristics.

- An SDP is locally unique to a participating service router. The same SDP ID can appear on other service routers.
- An SDP uses either the system IP address or the cellular PDN interface IP address of the far-end edge router to locate its destination.
- An SDP is not specific to any one service or to any type of service. When an SDP is created, services are bound to the SDP. An SDP can also have more than one service type associated with it.
- All services bound to an SDP use the same SDP (transport) encapsulation type defined for the SDP (for example, GRE-MPLS).
- An SDP is a service entity used for service management. Even though the SDP configuration and the services carried within it are independent, they are related objects. Operations on the SDP affect all

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

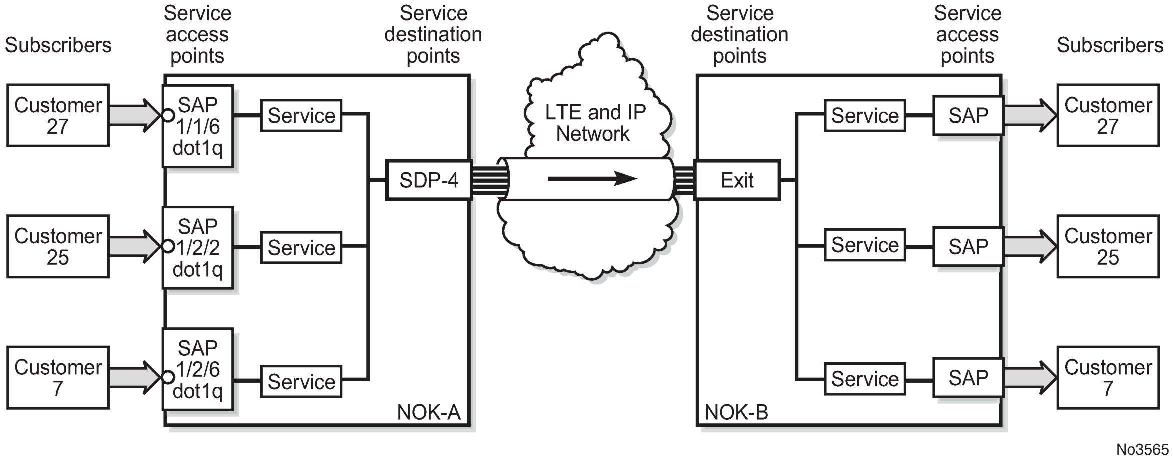
the services associated with the SDP. For example, the operational and administrative state of an SDP controls the state of services bound to the SDP.

- An SDP tunnel from a local device to the far-end device (router) requires a return SDP tunnel from the far end back to the local device. Each device must have an SDP defined for every remote router to which it wants to provide service. The SDP must be created before a distributed service can be configured.
- An SDP can be used to provide PW redundancy, where up to four spoke SDPs can be assigned to a service endpoint that acts as the managing entity to ensure service connection. For information about pseudowire redundancy, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide*, "Pseudo-wire redundancy".

9.4.4.1 SDP binding

To configure a distributed service pointing from NOK-A to NOK-B, the SDP ID on the NOK-A side (see Figure 8: SDP tunnel pointing from NOK-A to NOK-B) must be specified during service creation in order to bind the service to the tunnel (the SDP). Otherwise, service traffic is not directed to a far-end point and the far-end devices cannot participate in the service (there is no service). To configure a distributed service pointing from NOK-B to NOK-A, a return SDP on the NOK-B side must similarly be specified.

Figure 8: SDP tunnel pointing from NOK-A to NOK-B



SDP configuration and binding is required for:

- Layer 2 services that use T-LDP signaling
- Layer 3 services that do not use multi-protocol BGP(MP-BGP) to advertise routes with auto-bind

For Layer 3 VPRN services that use MP-BGP to advertise routes, auto-bind can be configured on the service to automatically bind that service to SDPs with reachability to remote nodes that are participating in MP-BGP.

The VPRN auto-bind function has the following characteristics.

- SDPs can be configured while auto-bind is enabled.
- Configuring SDPs when auto-bind is enabled is not required to transport VPRN services between nodes participating in the same VPRN.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- Configured SDPs have higher precedence and the node will select the configured SDP and its attributes to tunnel traffic to the far-end node.
- Auto-bind does not require a return path SDP from a far-end router as long as auto-bind is enabled on that far-end router for the service. If auto-bind is not enabled on the far-end router, then a return path SDP to the local 7705 SAR-Hm series node is required.
- For Layer 2 services that use BGP signaling (BGP-VPLS and BGP-VPWS) to exchange label information for the service, **auto-gre** can be configured on the pseudowire template of the service to automatically bind that service to SDPs with reachability to remote nodes that are participating in the BGP-signaled Layer 2 service. For information about the auto-GRE function available for BGP-VPLS and BGP-VPWS, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide*.

9.4.4.2 Spoke and mesh SDPs

There are two types of SDPs: spoke and mesh. The type of SDP defines how flooded traffic (or broadcast traffic, such as an ARP request) is propagated. For point-to-point PW/VLL services, spoke SDPs are the only way to bind services to the far-end router. For VPLS, mesh and spoke SDP bindings are allowed.

A spoke SDP that is bound to a service operates like a traditional bridge port. Flooded traffic that is received on the spoke SDP is transmitted to all the spoke SDPs, mesh SDPs, and SAPs to which it is connected. Flooded traffic is not transmitted back toward the port from which it was received.

In contrast, a mesh SDP that is bound to a service operates like a single bridge port. Flooded traffic received on a mesh SDP is transmitted to all spoke SDPs and SAPs to which it is connected. Flooded traffic is not transmitted to any other mesh SDPs or back toward the port from which it was received. This property of mesh SDPs is important for multi-node networks; mesh SDPs are used to prevent the creation of routing loops.

9.4.4.3 SDP encapsulation types

The Nokia service model uses encapsulation tunnels (also referred to as service tunnels) through the core to interconnect service routers. An SDP is a logical way of referencing the entrance to an encapsulation tunnel.

The 7705 SAR-Hm series supports Layer 2 or Layer 3 services within generic routing encapsulation (GRE-MPLS encapsulation).

An SDP has an implicit maximum transmission unit (MTU) value because services are carried in encapsulation tunnels and an SDP is an entrance to the tunnel. The MTU is configurable (in octets), where the transmitted frame can be no larger than the MTU.

9.4.4.3.1 GRE encapsulation

Generic routing encapsulation (GRE) tunnels are used to transport network layer packets over a Layer 3 network such as a cellular or WLAN interface.

GRE-MPLS SDPs are supported on network interfaces.

9.4.4.3.1.1 GRE format

In accordance with RFC 2784, a GRE encapsulated packet has the following format:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- delivery header
- GRE header
- payload packet

Delivery header

The delivery header is always an IPv4 header.

GRE header

The GRE header format is shown in Figure 9: GRE header and described in Table 4: GRE header descriptions.

Figure 9: GRE header

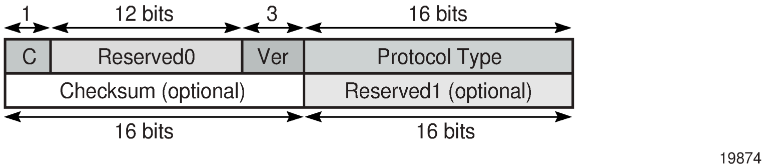


Table 4: GRE header descriptions

Field	Description
C	Specifies whether there is a checksum in the header If set to 1, both the checksum and reserved1 fields must be present In the network egress (transmit) direction, the C bit is always set to 0; therefore, the checksum and reserved1 fields are omitted from the header. The GRE header is therefore always 4 bytes (32 bits) in the network egress direction. In the network ingress direction, the C bit validity is checked. If it is set to a non-zero value, the GRE packet is discarded and the IP discards counter is increased.
Reserved0	Indicates whether the header contains optional fields The first 5 bits of the field are always set to 0 and bits 6 to 12 are reserved for future use and also set to 0
Ver	Always set to 000 for GRE At network ingress, if a GRE packet is received with the version field set to any value other than 000, the packet is discarded and the IP discards counter is increased
Protocol type	Specifies the protocol type of the original payload packet—identical to Ethertype with the only supported option being MPLS unicast (0x8847)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Field	Description
Checksum (optional)	Not applicable
Reserved1 (optional)	Not applicable

Payload packet

The payload encapsulation format depends on the type of service that is being carried over GRE-MPLS. The payload encapsulation format for GRE services is shown in Figure 10: GRE service payload packet over Ethernet and described in Table 5: GRE service payload packet descriptions.

Figure 10: GRE service payload packet over Ethernet

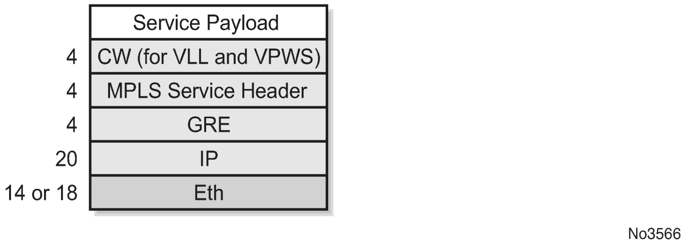


Table 5: GRE service payload packet descriptions

Field	Description
Eth	The Layer 2 transport header The only Layer 2 protocol supported is Ethernet MTU size depends on the encapsulation type (14 bytes for null encapsulation and 18 bytes for dot1q encapsulation) The Ethertype is always set to IP (0x800)
IP	Indicates the transport protocol IPv4 is the transport protocol for GRE-MPLS
GRE	Indicates the encapsulation protocol
MPLS service header	The MPLS service label identifies the service and the specific service element being transported For VLL and VPWS services, the label references the pseudowire that was statically configured, or signaled via T-LDP or BGP signaling For VPLS services, the label references a particular VPLS pseudowire that was signaled via T-LDP or BGP signaling to allow the end-to-end VPLS service For VPRN services, the label references either a spoke SDP pseudowire associated with the VPRN, or an MP-BGP

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Field	Description
	advertised route that has been signaled via BGP to allow the end-to-end VPRN service
CW for VLL and VPWS	The pseudowire Control word (CW) is a 32-bit (4-byte) field that is inserted between the VC label and the Layer 2 frame For more information about the Control word, see "Pseudo-wire Control word" in the 7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide.
Services payload	The services payload is the payload of the service being encapsulated For VLL, VPWS, and VPLS, this is a Layer 2 frame with either null or with dot.1q encapsulation For VPRN, this is a Layer 3 IPv4 or IPv6 packet without Layer 2 information

At network egress over a cellular port, the destination IP address of the GRE-MPLS IP header is always the far-end IP address that was either configured for the SDP, or learned through BGP routing. If the far-end address is for a cellular port on another 7705 SAR-Hm series node, then that address could be either the system IP address or the cellular PDN interface IP address, depending on the mode of operation deployed at that far-end location. The source IP address of the GRE-MPLS IP header is always set to the cellular PDN interface IP address. This address may be statically configured or dynamically assigned to a cellular port. For information about the PDN router interface modes of operation and how the PDN router interface IP address is assigned, see PDN router interfaces.

At the cellular port network ingress, the destination IP address in the IP header is the same as the cellular PDN interface IP address, because this IP address is the only address reachable over the cellular network. The source IP address of the IP header matches the far-end IP address associated with the GRE-MPLS tunnel. If the packet originates from another cellular port over the cellular network, the source IP address matches the cellular IP address used by the remote node. If the packet originates from another node that is Ethernet connected, then the source IP address is typically the system IP address of those nodes.

At network egress over an Ethernet interface, the source IP address is always set to the node system IP address; the destination IP address is set to one of the following:

- the system IP address of the service router on which the GRE SDP is configured
- the far-end interface address
- a loopback address

9.4.4.3.2 GRE SDP tunnel fragmentation and reassembly

It is possible to transport services over GRE-MPLS tunnels when the service MTU is larger than the cellular interface MTU. This requires the GRE-MPLS packets to be fragmented and reassembled using GRE SDP fragmentation and reassembly operations. For information, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide*, "GRE SDP tunnel fragmentation and reassembly".

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9.4.4.3.3 GRE SDP termination on router interface IP address

In some applications, an Ethernet interface is required to operate as a network interface and originate and terminate GRE-MPLS packets. If the application requires that GRE-MPLS packets terminate on the interface IP address instead of on the system IP address, then GRE SDP termination on the router interface IP address functionality is available. For information, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide*, "GRE SDP termination on router interface IP address".

9.4.4.4 SDP ping

For general information about SDP ping support, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide*, "SDP ping".

9.5 Services over the cellular PDN interface

When configuring services to and from the node over the cellular PDN interface, the following points should be considered:

- The mode of operation that is required for the cellular PDN interface, either static cellular system IPv4, static cellular interface IPv4, dynamic cellular interface IPv4, static cellular interface IPv6, or dynamic cellular interface IPv6. See PDN router interfaces for information about each mode of operation.
- The service type that is required; for example, a VLL, VPLS, or VPRN. See Layer 2 and Layer 3 services for information about supported service types.
- The signaling type that is required, either T-LDP, BGP, or both. See MPLS and Router configuration for information about configuring signaling and routing.
- The routing and reachability of the node for each configured service type when the node is operating with two SIMs. For information about dual SIM deployment, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*, "Dual SIM Deployment".

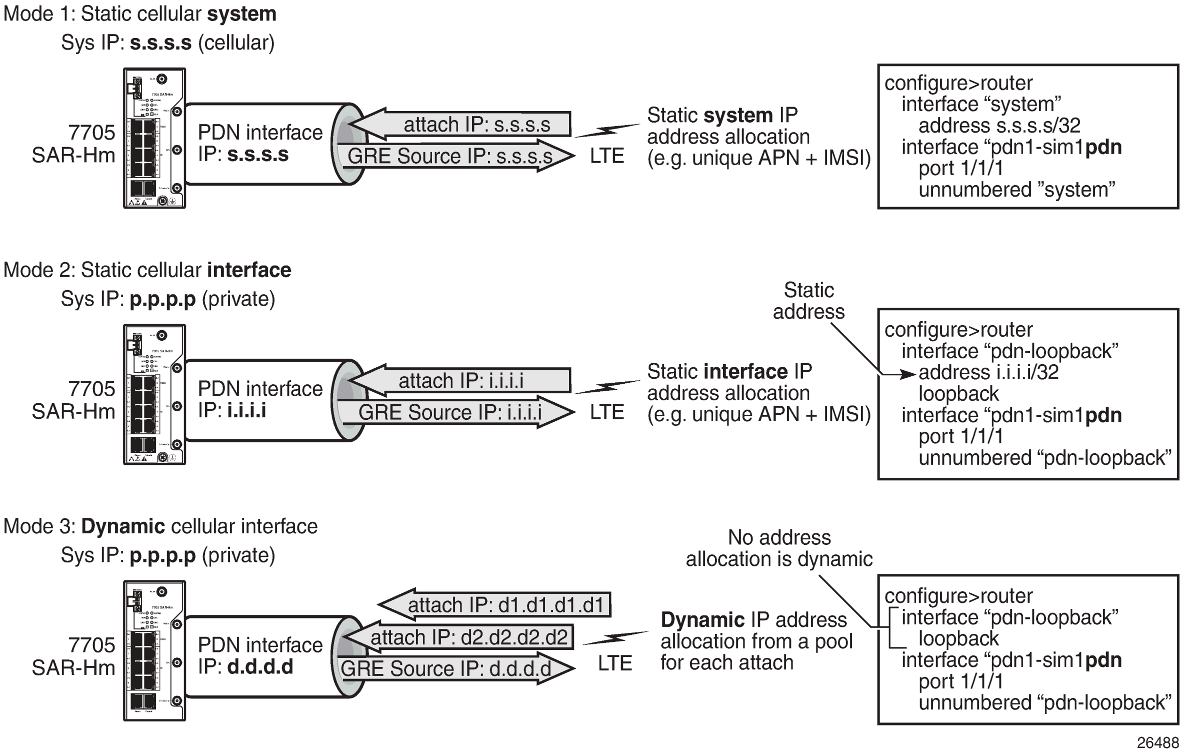
The combinations of points from the list above will result in different configuration requirements when enabling services over a cellular port.

The mode of operation of the cellular port for each enabled SIM is the main consideration when enabling services over cellular. Figure 11: IPv4 modes of operation on the cellular PDN interface shows an example of the IPv4 modes of operation. The points to consider for enabling services over cellular for each mode of operation are described below.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Figure 11: IPv4 modes of operation on the cellular PDN interface


Mode 1: Static cellular **system**
Sys IP: **s.s.s.s** (cellular)
7705 SAR-Hm
PDN interface IP: **s.s.s.s**
attach IP: s.s.s.s
GRE Source IP: s.s.s.s
LTE
Static **system** IP address allocation (e.g. unique APN + IMSI)
configure>router
interface “system”
address s.s.s.s/32
interface “pdn1-sim1**pdn**
port 1/1/1
unnumbered ”system”
Mode 2: Static cellular **interface**
Sys IP: **p.p.p.p** (private)
7705 SAR-Hm
PDN interface IP: **i.i.i.i**
attach IP: i.i.i.i
GRE Source IP: i.i.i.i
LTE
Static address
Static **interface** IP address allocation (e.g. unique APN + IMSI)
configure>router
interface “pdn-loopback”
address i.i.i.i/32
loopback
interface “pdn1-sim1**pdn**
port 1/1/1
unnumbered “pdn-loopback”
Mode 3: **Dynamic** cellular interface
Sys IP: **p.p.p.p** (private)
7705 SAR-Hm
PDN interface IP: **d.d.d.d**
attach IP: d1.d1.d1.d1
attach IP: d2.d2.d2.d2
GRE Source IP: d.d.d.d
LTE
No address allocation is dynamic
Dynamic IP address allocation from a pool for each attach
configure>router
interface “pdn-loopback”
loopback
interface “pdn1-sim1**pdn**
port 1/1/1
unnumbered “pdn-loopback”
26488

9.5.1 Static cellular system IPv4 mode

When a PDN router interface is configured for static cellular system IPv4 mode, consider the following points when setting up a service over a PDN router interface and its associated cellular port:

- The system IP address used to manage the node is the same as the cellular PDN interface IP address that gets assigned during the cellular attachment procedure.
- SDPs that are destined for the local node from other nodes must be configured to use the system IP address (identical to the cellular IP address) of the local node as the far-end address.
- T-LDP signaling sessions from the local node to peers use the system IP address as the local address for these sessions. This is the default behavior of the SR OS. The T-LDP sessions from peer nodes to the local node must be established to the system IP address.
- BGP sessions from the local node to peers where BGP VPWS, BGP VPLS, MP-BGP, or BGP routing is required for services use the system IP address as the local address for sessions. This is the default behavior of the SR OS. BGP sessions from peer nodes to the local node must be established to the system IP address.
- Static cellular system IPv4 mode supports all service types.
- In a dual SIM deployment, static cellular system IPv4 mode requires that the same IP address be allocated for both SIMs. The single system IP address allocation depends on this requirement being met. This requirement can be challenging to meet in most deployment models. Static cellular interface

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

IP mode or dynamic cellular interface IP mode should be considered when dual SIM is required, as these modes allow different IP addresses to be allocated for each SIM.

9.5.2 Static cellular interface IPv4 mode

When a PDN router interface is configured for static cellular interface IPv4 mode, consider the following points when setting up a service over a PDN router interface and its associated cellular port:

- The system IP address used to manage the node is not the same as one of the cellular PDN interface IP addresses assigned during the cellular attachment procedure.
- SDPs that are destined for the local node from other nodes must be configured to use the PDN interface IP address of the local node as the far-end address. They must not use the system IP address of the local node as the far-end address.
- T-LDP signaling sessions from the local node to peers must use the PDN interface IP address as the source IP address for these sessions; otherwise, GRE-MPLS services will not function properly. Operators must use the **local-lsr-id** LDP command to specify that the PDN router interface address is the local LSR ID on this 7705 SAR-Hm for these T-LDP sessions. For information about configuring the **local-lsr-id** command, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*. When the **local-lsr-id** is configured, T-LDP sets the source IP address of session packets to the PDN interface IP address.
- BGP sessions from the local node to peers where BGP VPWS, BGP VPLS, MP-BGP, and BGP routing is required for services must use the PDN interface IP address as the source IP address for these sessions. If these sessions do not use the PDN interface IP address as the source IP address, then GRE-MPLS services that require BGP-advertised information will not function properly.

  Operators must configure the BGP **local-address** command to specify that the PDN router interface is the local address on the local 7705 SAR-Hm series node for these BGP sessions. For information about configuring the BGP local address, see Using a router interface address as the BGP local address. When the **local-address** is configured, BGP sets the source IP address of session packets to the PDN interface IP address.
- Static cellular interface IPv4 mode supports all service types.

When dual SIM operation is required, the points listed above must be considered for each PDN router interface configured for each SIM.

9.5.3 Dynamic cellular interface IPv4 mode

When a PDN router interface is configured for dynamic cellular interface IPv4 mode, consider the following points when setting up a service a over PDN router interface and its associated cellular port:

- The system IP address used to manage the node is not the same as the cellular PDN interface IP address assigned during the cellular attachment procedure.
- The PDN interface IP address changes every time the PDN reattaches to the cellular network
- SDP configurations cannot be made from other nodes to the local node. The changing IP address of the PDN interface during each PDN attachment procedure inhibits the static configuration needed to manually configure SDPs.
- T-LDP signaling sessions cannot be established toward the local node because the changing PDN interface IP address inhibits the static configuration of T-LDP sessions toward the PDN interface.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- BGP sessions cannot be established toward the local node because the changing PDN interface IP address inhibits the static configuration of BGP sessions toward the PDN interface.
- BGP sessions from the local node to peers where MP-BGP and BGP routing is required for services must use the PDN interface IP address as the source IP address for these sessions. Operators must specify the loopback interface of the PDN router interface when configuring the BGP **local-address** command. For information about configuring the BGP local address, see Using a router interface address as the BGP local address. When the **local-address** command is configured with the loopback interface of the PDN router interface, BGP sets the source IP address of session packets to the PDN interface IP address.
- BGP far-end peering nodes to the local node must be configured with the **dynamic-neighbor** command using an IP address range that matches the possible PDN router interface attachment IP addresses on the local node. This allows the PDN interface IP address to dynamically change and re-establish BGP sessions to the same far-end peering node. For information about the **dynamic-neighbor** command, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.
- Only services that use **auto-bind** or **auto-gre-sdp** can operate with dynamic cellular interface IP mode. The 7705 SAR-Hm series supports MP-BGP-based VPRN services with **auto-bind**, and BGP-VPLS and BGP-VPWS with **auto-gre-sdp**.
- Dynamic cellular interface IP mode does not support the following services:
  - Layer 2 services that use T-LDP signaling
  - Layer 3 services that do not use **auto-bind**

When dual SIM operation is required, the points listed above must be considered for each PDN router interface configured for each SIM.

9.5.4 Static cellular interface IPv6 mode

When a PDN router interface is configured for static cellular interface IPv6 mode, consider the following points when setting up a service over a PDN router interface and its associated cellular port:

- GRE-MPLS based services are not supported with static cellular interface IPv6 mode.
- Services that are supported using IPSec secure interfaces are supported with static cellular interface IPv6 mode.

In a dual SIM deployment, the points listed above must be considered for each PDN router interface configured for each SIM.

9.5.5 Dynamic cellular interface IPv6 mode

When a PDN router interface is configured for dynamic cellular interface IPv6 mode, consider the following points when setting up a service over a PDN router interface and its associated cellular port:

- GRE-MPLS based services are not supported with dynamic cellular interface IPv6 mode.
- Services that are supported using IPSec secure interfaces are supported with dynamic cellular interface IPv6 mode.

In a dual SIM deployment, the points listed above must be considered for each PDN router interface configured for each SIM.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

9.6 Services over Ethernet with DHCP client

When configuring services over an Ethernet-based router interface that is enabled as a DHCP client, the IP address is dynamically allocated by the DHCP server that the DHCP client communicates with. See DHCP client and Router interface command reference for information about configuring the DHCP client on a router interface.

The IP address allocated by the DHCP server may not be the same address each time the DHCP client issues a DHCP discovery or request message. In any case, the value of the address is not typically known and establishing services over the interface needs to account for this discovered IP address.

Consider the following points when setting up a service over an Ethernet-based router interface.

- SDP configurations cannot be made from other nodes to the local node. The potentially changing and unknown IP address inhibits the static configuration that is needed to manually configure SDPs.
- T-LDP signaling sessions cannot be established toward the local node because the potentially changing and unknown IP address inhibits the static configuration of T-LDP sessions toward the interface.
- BGP sessions cannot be established toward the local node because the potentially changing and unknown IP address inhibits the static configuration of BGP sessions toward the interface.
- BGP sessions from the local node to peers where MP-BGP and BGP routing is required for services must use the DHCP client IP address as the source IP address for these sessions. Operators must use the router interface name when configuring the BGP local address. For information about configuring the BGP local address, see Using a router interface address as the BGP local address. When the **local-address** command is configured with the DHCP client interface, BGP sets the source IP address of session packets to the IP address learned by the DHCP client from the DHCP server.
- BGP far-end peering nodes to the local node must be configured with the **dynamic-neighbor** command using an IP address range that matches the possible DHCP client addresses on the local node. This allows the IP address assigned by the DHCP server to the DHCP client to dynamically change and re-establish BGP sessions to the same far-end peering node. For information about the **dynamic-neighbor** command, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.
- Only services that use **auto-bind** or **auto-gre-sdp** can operate over a router interface enabled as a DHCP client. The 7705 SAR-Hm series supports MP-BGP-based VPRN services with **auto-bind** and BGP-VPLS and BGP-VPWS with **auto-gre-sdp**.
- Router interfaces that are enabled as DHCP clients enabled do not support the following services:
  - Layer 2 services that use T-LDP signaling
  - Layer 3 services that do not use **auto-bind**

9.7 Services with the WLAN interface

The WLAN interface can be configured as either an access point (AP) or as a station. For information about the AP and station and how to configure them, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide* .

When configured as an AP, the WLAN interface provides SAP-level connectivity to the traffic it sends and receives over the interface from devices that are connected to it. The WLAN AP traffic can be transported over a service to remote locations; for example, to a remote WLAN gateway.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

When configured as a station, the WLAN interface operates as a network interface to transport services over WLAN toward a remote AP. The node uses GRE-MPLS encapsulated SDPs to provide Layer 3 transport over the WLAN station interface.

9.7.1 Transporting WLAN access point traffic over services

The WLAN interface can be used as an access point to provide connectivity to other devices. As an access point, the WLAN interface brings device traffic into a service SAP, which is then carried over an SDP and ultimately over a network WAN interface such as an Ethernet port or a cellular port. The port ID of the WLAN interface is used as the SAP ID that binds the WLAN interface to the service. For information about configuring the WLAN MDA and WLAN port parameters to enable the WLAN interface, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*.

To provide services from the WLAN AP to other nodes and devices in the network, a Layer 2 Epipe service is required. The Epipe either connects the WLAN AP to the Nokia WLAN gateway (WLAN-GW) enabled on the VSR or 7750 SR, or back hauls the WLAN AP traffic to other nodes in the network. For information about configuring the WLAN-GW, see the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide* .

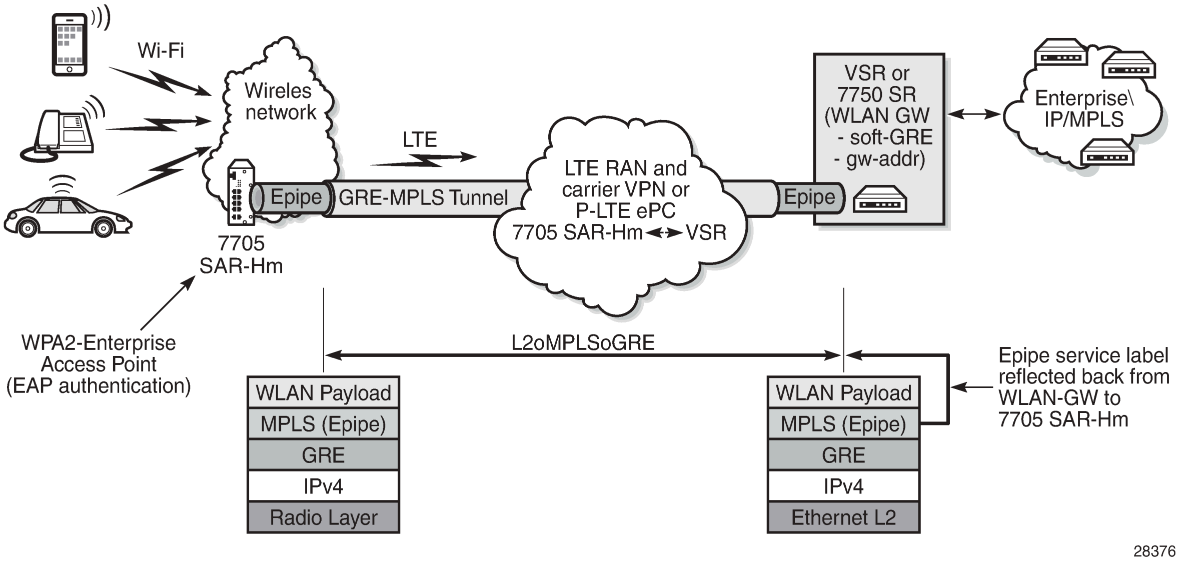
WLAN clients can be optionally authenticated by an AAA server before being allowed access to the WLAN AP and before their traffic can be carried over the transport service.

9.7.2 Layer 2 Epipe service to the WLAN-GW

The WLAN interface AP can connect directly to the WLAN Gateway (WLAN-GW) over a Layer 2 Epipe service. For information about the WLAN-GW, see the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*, "WiFi aggregation and offload".

Figure 12: Using an Epipe to connect a WLAN AP to a WLAN-GW illustrates the use of an Epipe service to connect the WLAN AP on a 7705 SAR-Hm to the WLAN-GW.

Figure 12: Using an Epipe to connect a WLAN AP to a WLAN-GW



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

In Figure 12: Using an Epipe to connect a WLAN AP to a WLAN-GW , to connect to the WLAN-GW, the WLAN interface AP port ID must be configured as the L2 SAP of an Epipe service. The Epipe service is configured with a spoke SDP where the far-end address of the SDP (GRE) is configured to reach the gateway address of the WLAN-GW.

There is no signaling required to establish the Epipe service because a static ingress and egress VC label must be configured with the same value. The VC label received by the WLAN-GW from the WLAN AP node (the egress VC label) is reflected back from the WLAN-GW for traffic destined for the WLAN AP node. The 7705 SAR-Hm uses the received VC label (the ingress VC label) to determine that the received traffic is for the Epipe service associated with the WLAN AP SAP.

If the same SSID is used for multiple WLAN APs in the network (for example, an enterprise SSID for a campus-wide WLAN network), the same VC label should be used for each WLAN AP Epipe participating in the same SSID network WLAN service. Using a unique VC label per SSID allows WLAN clients connecting to the SSID to roam between WLAN APs that are broadcasting the same SSID.

The following output shows a configuration example of the SDP and Epipe SAP.

```
A:ALA-1>config>service# info
----------------------------------------------
...
    epipe 5500 customer 5 vpn 5500 create
        description "WLAN AP mySSIDname to WLAN GW"
        sap 1/4/1 create
            no shutdown
        exit
        spoke-sdp 1:123 create
            description "SDP 1 binding to WLAN GW gw-address"
            ingress
                vc-label 5500
            exit
            egress
                vc-label 5500
            exit
        exit
        no shutdown
    exit
```

The WLAN AP authenticates users before forwarding their traffic over the Epipe. See the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide* for information about security parameters and supported authentication protocols.

DHCP snooping and DHCP relay must be enabled on the WLAN AP so that attached clients can successfully acquire an IP address from the WLAN GW when they issue DHCP requests. The WLAN AP snoops for DHCP requests and modifies them to include DHCP option 82, specifically the circuit ID sub-option that includes the MAC address of the AP, the SSID of the AP, and the SSID type of either open or secured. The DHCP request is then relayed to the WLAN GW over the Epipe service. To enable DHCP snooping and DHCP relay on the WLAN port, the command **config>port>wlan>access-point>dhcp>no shutdown** must be executed in the CLI. For more information, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*.

9.7.3 Services over the WLAN station port

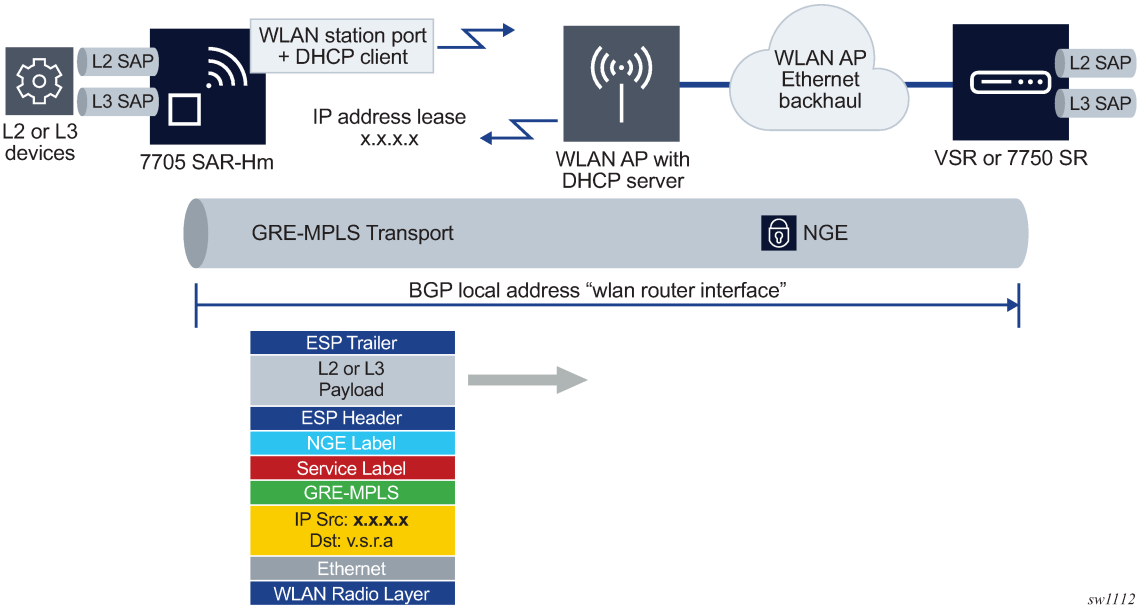
The WLAN station port provides network-level connectivity to a WLAN AP to provide end-to-end services between the node and another Nokia router. A network interface configured on the WLAN station acts in a similar fashion to network interfaces configured on Ethernet ports. BGP routing and GRE-MPLS-based

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

SDPs can traverse the network interface on the WLAN station port. The remote AP that the WLAN station port connects to must provide the necessary reachability to another Nokia router that can terminate the services from the node.

Figure 13: Services transport over the WLAN station port illustrates how the WLAN station port connected to an AP can provide end-to-end services between the node and another Nokia router.

Figure 13: Services transport over the WLAN station port



When configuring services over the WLAN station port, the router interface IP address can be configured manually on the router interface or it can be automatically discovered by the DHCP client configured on the router interface.

When the IP address is configured manually, services are established using standard methods to set up services over Ethernet ports because the WLAN station operates as a standard Ethernet port when it is operationally up.

For information about an automatically discovered IP addresses using the DHCP client, see Services over Ethernet with DHCP client.

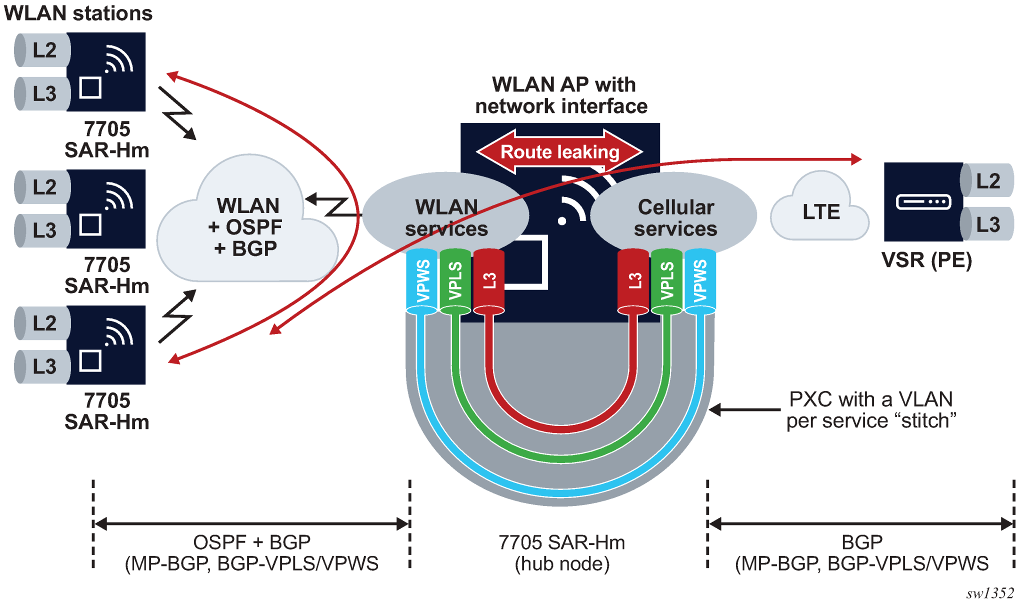
9.7.3.1 Stitching services between the cellular interface and a WLAN AP

When extending IP/MPLS services over WLAN from the cellular interface, services can be stitched together from the cellular interface to the WLAN AP interface. Service stitching allows operators to create a hub-and-spoke topology from the stitching node to other WLAN stations over the WLAN AP using the same WLAN network.

Figure 14: Stitching services from a cellular interface to a WLAN AP is an example of stitching services from a cellular interface to the WLAN AP.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Figure 14: Stitching services from a cellular interface to a WLAN AP



With a hub-and-spoke WLAN topology, Layer 2 or Layer 3 services can be established between the WLAN stations over the same WLAN network. An OSPF and BGP control plane is configured over the WLAN network from each station to the AP, so that each WLAN station learns routing information from the other stations or from the WLAN AP. The control plane also distributes routing information learned from the cellular interface allowing WLAN stations to learn routes to PE nodes reachable over the cellular interface.

When services from a station need to reach a destination over the cellular interface, the services must terminate on the PXC port of the hub 7705 SAR-Hm. The other end of the PXC port then re-originates the traffic over a dedicated service over the cellular interface toward other PEs reachable over the cellular interface.

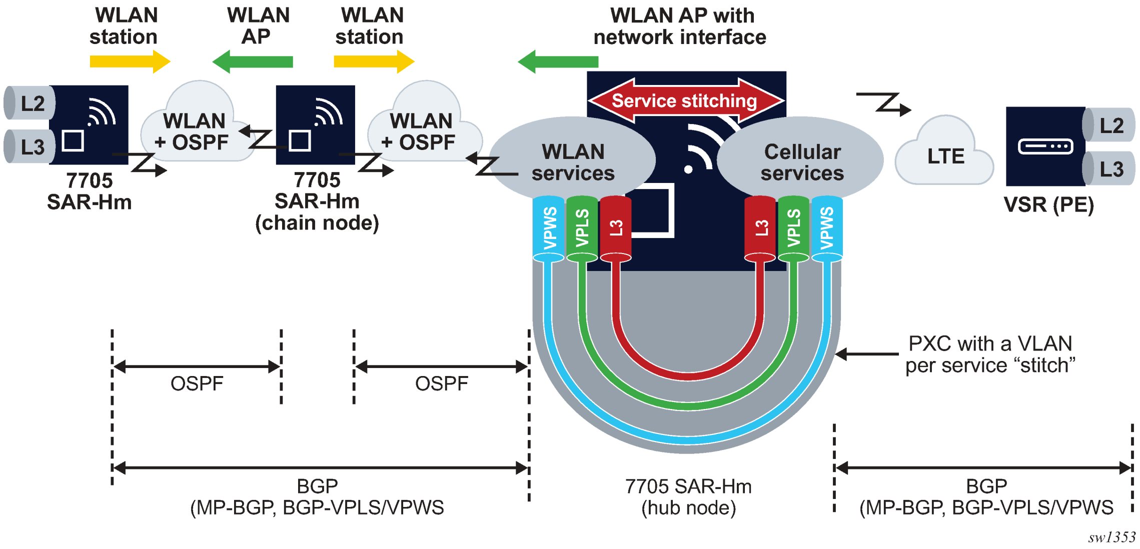
For Layer 3 VPRN services, routes need to be leaked from the WLAN-side VPRN to the cellular-side VPRN. For VPLS, MAC addresses are learned across the PXC port as needed and re-advertised in BGP-VPLS. For VPWS, the stitch is achieved by extending the Epipe service from WLAN to over cellular.

9.7.3.2 Daisy chaining

When stitching services between the cellular interface and the WLAN interface, it is possible to create a daisy chain topology; see Figure 15: Daisy chain topology for stitched services.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Figure 15: Daisy chain topology for stitched services



In a daisy chain topology, a hub node is configured as described in section Stitching services between the cellular interface and a WLAN AP and a chain node is introduced to further extend the WLAN network by creating multiple hops between the hub node and the last node in the chain. The OSPF control plane is configured on all WLAN interfaces and BGP is configured from the hub node to the last node in the chain. If services terminate on the chain node, a BGP session is configured between the chain node and the hub node.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

10 Layer 2 and Layer 3 services

The 7705 SAR-Hm series of routers support the following services:

- Layer 2 services:
  - Virtual Leased Line (VLL) services
  - Virtual private LAN Service (VPLS)
- Layer 3 services:
  - Internet Enhanced Service (IES)
  - Virtual Private Routed Network (VPRN) service
  - IP transport services

10.1 Virtual Leased Line (VLL) services

For general information about VLL support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide*, "VLL services":

- Ethernet Pipe (Epipe) services
  - Epipe service overview
  - Epipe service pseudowire VLAN tag processing
  - Epipe up operational state configuration option
- Pseudowire redundancy service models
- BGP VPWS
  - Single-homed BGP VPWS
  - Dual-homed BGP VPWS
- VLL service considerations
- Configuring a VLL service with CLI
- Service management tasks

For descriptions of VLL services commands, see 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*.

10.2 Virtual private LAN Service (VPLS)

For general information about VPLS support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide*, "Virtual Private LAN Service":

- VPLS service overview

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- VPLS features
  - VPLS service pseudowire VLAN tag processing
  - VPLS MAC learning and packet forwarding
  - Pseudowire control word
  - Table management
  - Split horizon SAP groups and split horizon spoke SDP groups
  - VPLS and spanning tree protocol
  - VPLS access redundancy
  - Object grouping and state monitoring
  - MAC flush message processing
  - ACL next-hop for VPLS
  - SDP statistics for VPLS and VLL services
  - BGP VPLS
  - BGP multi-homing for VPLS
- Routed VPLS and I-VPLS
  - IES or VPRN IP interface binding
  - IP interface MTU and fragmentation
  - ARP and VPLS FDB interactions
  - The allow-ip-int-bind VPLS flag
  - R-VPLS restrictions
- VPLS service considerations
- Configuring a VPLS service with CLI
- Service management tasks

See 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* for descriptions of VPLS service commands.

10.3 Internet Enhanced Service (IES)

For general information about IES support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN*, "Internet Enhanced Service":

- IES service overview
- IES features
  - IP interfaces
    - Object grouping and state monitoring
  - SAPs
    - Encapsulations

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

    - Shaping and bandwidth control
  - Routing protocols
  - QoS policies
  - Filter policies

For descriptions of IES commands, see 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*.

On the 7705 SAR-Hm series of routers, IES services are supported on Ethernet ports. IES services are not supported over cellular ports or the WLAN interface.

10.4 Virtual Private Routed Network (VPRN) service

The 7705 SAR-Hm series of routers support a filter action that adjusts the maximum segment size of TCP packets traversing VPRN SAP interfaces. For information, see TCP MSS adjustment filter on VPRN SAP interfaces.

For general information about VPRN support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN*, "Virtual Private Routed Network":

- VPRN service overview
  - Routing prerequisites
  - Core MP-BGP support
  - Route distinguishers
  - Route reflector
  - CE-to-CE route exchange
  - Constrained route distribution
  - Export of inactive VPRN BGP routes
- VPRN features
  - IP interfaces
    - Traffic differentiation based on route characteristics
    - Associating an FC and priority with a route
    - Displaying QoS information associated with routes
    - Object grouping and state monitoring
    - VPRN IP interface applicability
  - SAPs
    - SAP encapsulations
    - Pseudowire SAPs
  - QoS policies
  - Filter policies
  - DSCP marking

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

  - Configuration of TTL propagation for VPRN routes
  - CE to PE routing protocols
  - Spoke SDPs
  - IP-VPNs
  - Traffic leaking to GRT
  - Traffic leaking from VPRN to GRT for IPv6
  - RIP metric propagation in VPRNs
  - NTP within a VPRN service
  - VPN route label allocation
- QoS on ingress binding
- FIB prioritization
- Configuring a VPRN service using CLI
- Service management tasks

For descriptions of VPRN commands, see 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*.

10.4.1 TCP MSS adjustment filter on VPRN SAP interfaces

The 7705 SAR-Hm series of routers support a configurable filter that adjusts the maximum segment size (MSS) of TCP packets marked with a SYN flag that traverse VPRN SAP interfaces. The MSS adjustment filter prevents upstream and downstream TCP packets from being fragmented.

MSS adjustment is performed by the virtualized integrated BB ISA MDA when an IP filter is enabled with the **action tcp-mss-adjust** command. The filter can be applied on a VPRN SAP interface in the ingress direction, egress direction, or both directions. Both IPv4 and IPv6 filters are supported. For information about the virtualized BB ISA MDA, see the *7705 SAR-Hm Interface Configuration Guide*, "Chassis IOM and MDAs".

To configure a TCP MSS adjustment filter on a VPRN SAP interface:

1. Create a NAT group that will be used for MSS adjustment.

   The following CLI output is an example of the creation of a NAT group on the virtualized integrated BB ISA MDA in slot 1/6.

```
config
   card 1
        mda 6
            mda-type isa-bb-v
            no shutdown
        exit
        no shutdown
    exit
```

```
configure
    isa
        nat-group 1 create
            active-mda-limit 1
            mda 1/6
            no shutdown
        exit
```

2. Associate the NAT group with a routing instance and configure the MSS value as shown in the following example.

```
config
    service
        vprn services-id
            mss-adjust-group 1 segment-size 1352
```

3. Create ingress or egress IP filters that perform TCP MSS adjustment.

   The following example shows the configuration of IPv4 filters and IPv6 filters that perform TCP MSS adjustment at ingress and egress.

```
configure
    filter
        ip-filter 1 name "1" create
            default-action forward
            description "Ingress"
            entry 1 create
                match protocol tcp
                    tcp-syn true
                exit
                action
                    tcp-mss-adjust
                exit
            exit
        exit
        ip-filter 2 name "2" create
            default-action forward
            description "Egress"
            entry 1 create
                match protocol tcp
                    tcp-syn true
                exit
                action
                    tcp-mss-adjust
                exit
                egress-pbr default-load-balancing
            exit
        exit
        ipv6-filter 1 name "3" create
            default-action forward
            description "Ingress"
            entry 1 create
                match next-header tcp
                    tcp-syn true
                exit
                action
                    tcp-mss-adjust
                exit
            exit
        exit
        ipv6-filter 2 name "4" create
            default-action forward
            description "Egress"
            entry 1 create
                match next-header tcp
                    tcp-syn true
                exit
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                action
                    tcp-mss-adjust
                exit
                egress-pbr default-load-balancing
            exit
        exit
    exit
```

4. Apply the filters that perform TCP MSS adjustment to the VPRN SAP interface. The filters can be applied in the ingress direction, egress direction, or both directions. In the following example, the filters are applied in both the ingress and egress directions.

```
config
    service
        vprn service-id
            interface "int1_vprn1" create
                address 10.10.1.1/24
                sap 1/2/3 create
                    ingress
                        filter ip 1
                    exit
                    egress
                        filter ip 2
                    exit
                exit
            exit
        exit
        vprn service-id2
            interface "int1_vprn2" create
                ipv6
                    address 10:1::1/32
                    neighbor 10:1::2 00:02:01:00:00:01
                exit
                sap 1/2/3:1 create
                    ingress
                        filter ipv6 3
                    exit
                    egress
                        filter ipv6 4
                    exit
                exit
            exit
        exit
```

10.5 IP transport services

This section describes about the following topics:

- Raw socket IP transport service
- GNSS NMEA data IP transport service
- Serial raw socket IP transport configuration commands hierarchy
- IP transport show commands hierarchy
- IP transport clear commands hierarchy

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

10.5.1 Raw socket IP transport service

Serial data transport using raw sockets over IP transport services is a method of transporting serial data, in character form, over an IP network using Layer 3-based services. This feature can help transport Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs) to Front-End Processors (FEPs), or SCADA masters.

The functionality provided by the IP transport service feature for serial raw sockets is summarized as follows:

- IP transport local host server function, to listen and open raw socket sessions from remote hosts
- IP transport remote host client function, to initiate and open new raw socket sessions to remote hosts
- Both local host and remote host functions support either TCP or UDP IP transport services
- IP transport over a VPRN service
- Enhanced QoS and queuing of sessions to ensure collisions between sessions do not cause serial data to impact RTUs and end-user equipment

Figure 16: IP transport service illustrates a more detailed view of the local host (server) and remote host (client) functionality that enables multiple communication streams to and from a serial port using raw socket IP transport.

The figure shows a three-node network, a 7705 SAR-Hm (left), a 7705 SAR-8/7705 SAR-18 (top-right) and a 7750 SR/VSR (bottom right). There are two devices, RTU (1) and RTU (2) connected to the serial ports on the 7705 SAR-Hm. The FEP server [A] can reach the RTUs the via socket sessions that originate from the SDI card on the 7705 SAR-8/7705 SAR-18 node.

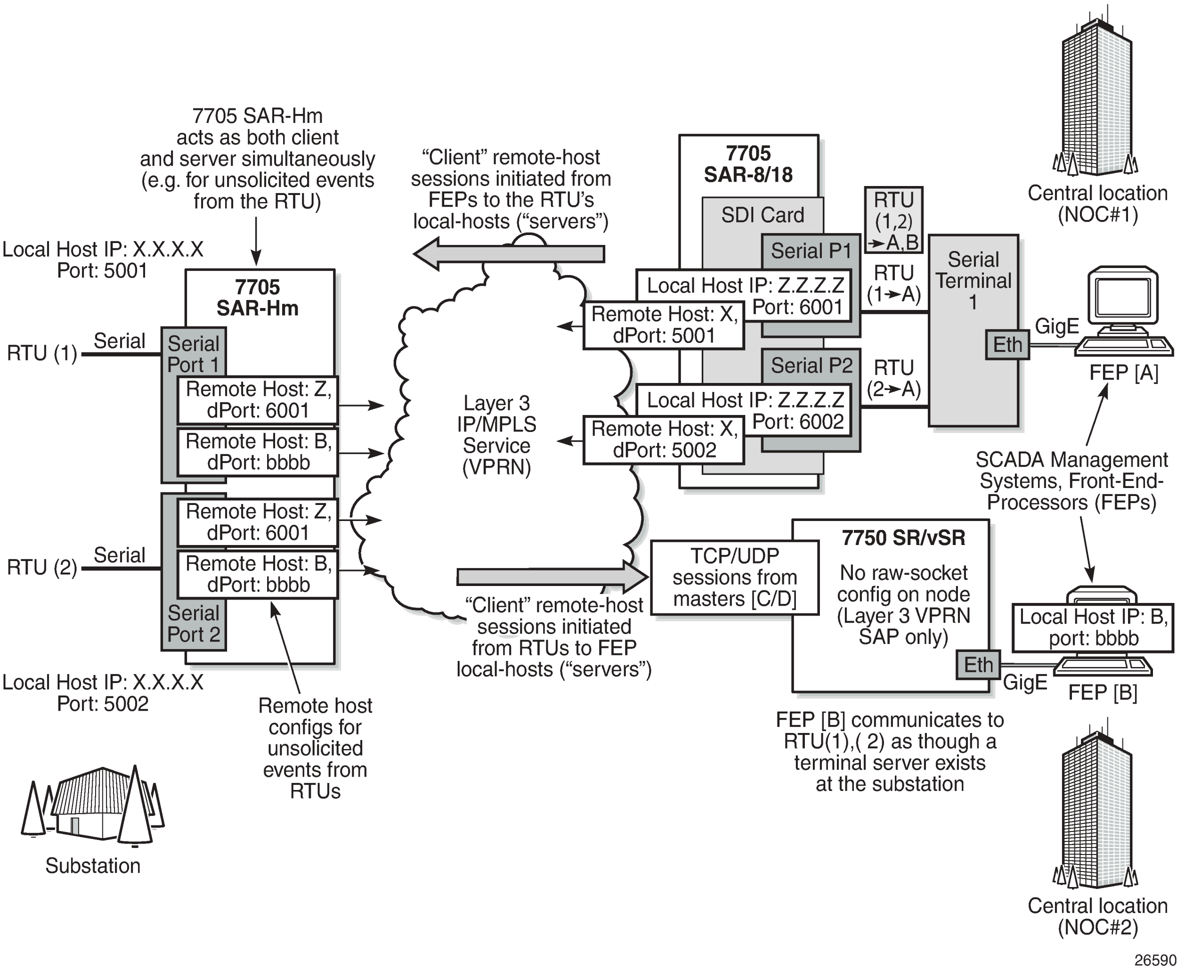
The bottom right 7750 SR or VSR node is connected to FEP server [B] directly using Ethernet. This FEP server reaches the RTUs via a Layer 3 VPRN service where TCP and UDP sessions originating from the FEP server [B] terminate on the 7705 SAR-Hm to deliver the raw socket serial data to the RTUs.

Through local host and remote host configurations on the 7705 SAR-Hm, 7705 SAR-8, or 7705 SAR-18, serial raw socket IP transport sessions are established to carry serial data over a wireless IP/MPLS network. The source and destination IP addresses and port numbers for these sessions are derived directly from the local/remote host configurations associated with each serial port or master head-end server. Further details are described in the subsequent sections.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Figure 16: IP transport service


7705 SAR-Hm acts as both client and server simultaneously (e.g. for unsolicited events from the RTU)
"Client" remote-host sessions initiated from FEPs to the RTU's local-hosts ("servers")
7705 SAR-8/18
SDI Card
Serial P1
Serial P2
RTU (1,2) ➔A,B
RTU (1➔A)
RTU (2➔A)
Serial Terminal 1
Eth
GigE
Central location (NOC#1)
FEP [A]
Local Host IP: X.X.X.X Port: 5001
7705 SAR-Hm
RTU (1)
Serial
Serial Port 1
Remote Host: Z, dPort: 6001
Remote Host: B, dPort: bbbb
Local Host IP: Z.Z.Z.Z Port: 6001
Remote Host: X, dPort: 5001
Local Host IP: Z.Z.Z.Z Port: 6002
Remote Host: X, dPort: 5002
Layer 3 IP/MPLS Service (VPRN)
SCADA Management Systems, Front-End-Processors (FEPs)
RTU (2)
Serial
Remote Host: Z, dPort: 6001
Remote Host: B, dPort: bbbb
Serial Port 2
TCP/UDP sessions from masters [C/D]
7750 SR/vSR
No raw-socket config on node (Layer 3 VPRN SAP only)
Eth
GigE
Local Host IP: B, port: bbbb
FEP [B]
"Client" remote-host sessions initiated from RTUs to FEP local-hosts ("servers")
Local Host IP: X.X.X.X Port: 5002
Remote host configs for unsolicited events from RTUs
FEP [B] communicates to RTU(1),(2) as though a terminal server exists at the substation
Substation
Central location (NOC#2)
26590

A raw socket IP transport interface can be configured for each serial port. This allows the raw socket IP transport to receive TCP or UDP session packets from multiple remote hosts when operating as a local host (server), or to create new multiple sessions to remote hosts to send and receive serial data when operating as a client.

There are two main configurations required for a serial raw socket IP transport service to be operational and support the sending and receiving of serial data:

1. Port-level socket configuration—this includes rudimentary serial link parameters such as baud rate, start/stop values, and bits.

   Also, socket-level configuration is required, such as end-of-packet checking parameters (idle-time, length, special character), and the inter-sessions delay for transmitting sessions data out the serial link. For information about the required port-level configuration, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*, "Serial raw socket interface commands".
2. IP transport service-level configuration—this includes creating an IP transport subservice to associate the serial port within a Layer 3 VPRN service, so that TCP/UDP encapsulated serial data can be routed within the corresponding Layer 3 service. The IP transport subservice ID is modeled and created identical to creating SAP IDs under the same service types. IP transport configuration includes IP

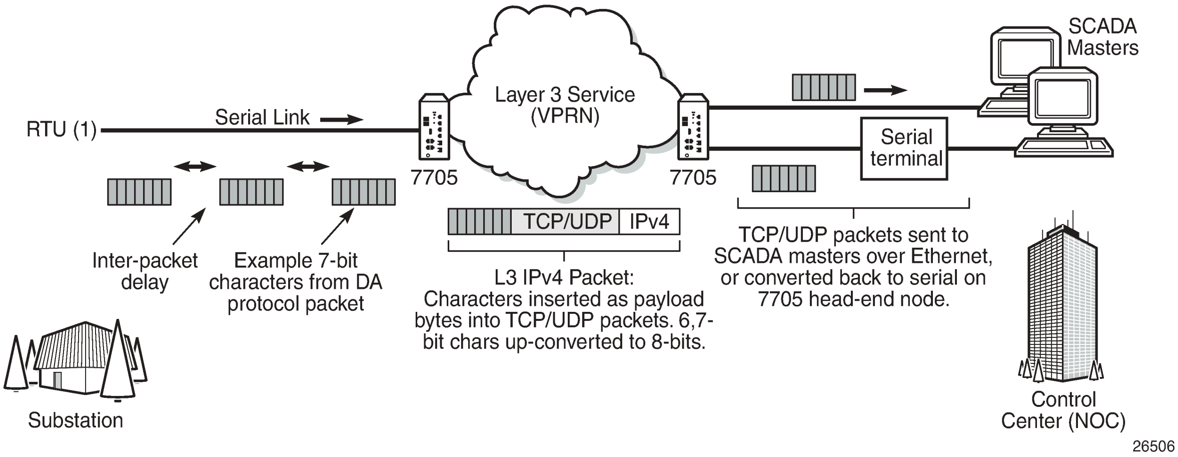
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

transport local host items and remote host items, such as TCP timers and sessions controls. These are described further in the sections that follow. Also, see Serial raw socket IP transport configuration commands hierarchy for the required information.

A raw socket IP transport service configured for a serial port allows the IP transport local host to listen to and open raw socket sessions from remote hosts that need to communicate over the serial port, and for each serial port's local host to initiate and open raw socket sessions to remote hosts when serial data needs to be sent to those remote hosts. The local and remote host functions support TCP or UDP sessions (but not both concurrently) over the VPRN service.

The serial data is received as characters that represent bytes in a packet. These bytes are packetized into Layer 3 TCP/UDP packets that are then transported or forwarded across the IP/MPLS network using the node's Layer 3 VPRN service constructs for routing. Figure 17: TCP/UDP packet transport over IP/MPLS illustrates how serial data is encapsulated into TCP/UDP packets and transported over IP/MPLS. When using a cellular port, GRE-MPLS and encapsulations for the service would be included, but this is not shown in the figure.

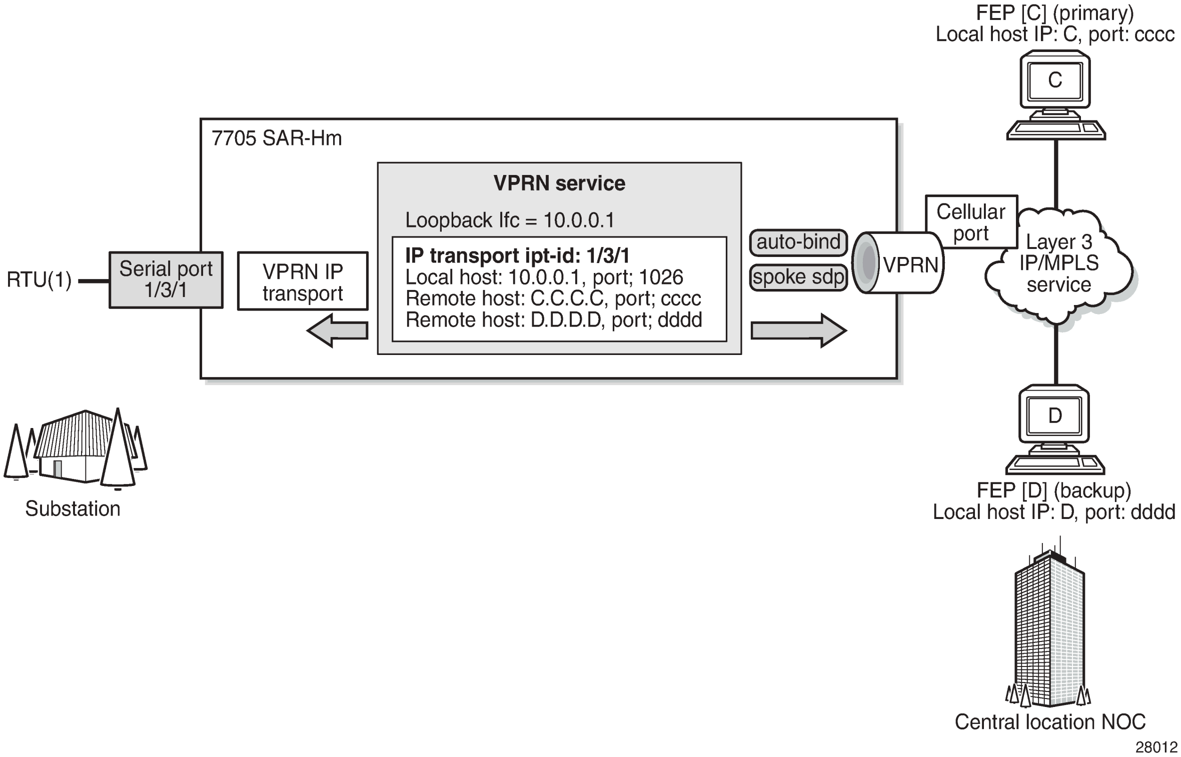
Figure 17: TCP/UDP packet transport over IP/MPLS


SCADA Masters
Layer 3 Service (VPRN)
RTU (1)
Serial Link
7705
7705
Serial terminal
TCP/UDP
IPv4
Inter-packet delay
Example 7-bit characters from DA protocol packet
L3 IPv4 Packet: Characters inserted as payload bytes into TCP/UDP packets. 6,7-bit chars up-converted to 8-bits.
TCP/UDP packets sent to SCADA masters over Ethernet, or converted back to serial on 7705 head-end node.
Substation
Control Center (NOC)
26506

For raw socket packets to be routed within a VPRN service, an IP transport subservice must be configured within a VPRN context. The IP transport subservice context is where users configure local host and remote host information, such as IP addresses and ports for establishing TCP/UDP sessions, and other per-session parameters. TCP/UDP encapsulated serial data is routed within the corresponding Layer 3 VPRN service. Figure 18: VPRN IP transport service illustrates this basic concept.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Figure 18: VPRN IP transport service



To create an IP transport subservice, the **ip-transport** command is used with the corresponding serial port as the *ipt-id* to bind the serial port SAP to the IP transport subservice. After the IP transport service is created, local host and remote host configurations can proceed. A local host must be configured before remote hosts can be configured.

Each local host uses a local address (from a loopback or local interface configured under the VPRN service context) as the local host IP address (that is, the source IP address in the raw socket packets leaving the node within the VPRN service) of the IP transport subservice associated with the serial port. The local host is used to terminate TCP/UDP sessions from remote hosts. The local host can select either the TCP or UDP protocol for raw socket sessions but not both concurrently.

Multiple remote hosts can be configured under the IP transport subservice associated with the serial port so that each remote host receives the serial data that is received on the serial port. Each remote host has its own remote destination IP address and port value for establishing sessions. The configured remote hosts use the TCP or UDP protocol configured for the IP transport subservice.

Note: It is not necessary to configure remote hosts when the IP transport service is not originating sessions. If sessions are only established toward the IP transport local host (for example, remote servers polling the local host), the remote host configuration is not necessary. Remote host configurations may still be desirable when using **filter-unknown-host**.

IP transport processing of TCP/UDP packets is performed by the CPM task. Filters configured for protecting the CPM need to take into account the raw socket IP transport packets and ensure the filter is not blocking associated IP transport sessions. For example, operators need to ensure interface IP

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

addresses and ports configured on the node are not blocked, and remote host IP/port combinations are not blocked.

Note: IP transport-to-IP transport raw socket data on the same node is not supported.

10.5.1.1 Remote host manual TCP connection check

A manual TCP connection check can be performed for each remote host configured for a raw socket IP transport subservice. When executed by an operator, the TCP connection check attempts to establish a TCP session toward the configured remote host. Only one TCP connection check attempt is made, with a fixed timeout of 5 seconds. If the attempt is successful, the session is torn down immediately without data being sent.

The TCP connection check is initiated in the CLI using the **tools>perform>service>ip-transport>remote-host>check-tcp** command. The result is displayed in the CLI using the **tools>dump>service>ip-transport>remote-host>check-tcp** command. Equivalent management is available via SNMP.

If a TCP connection to a remote host already exists because of serial traffic being transmitted, the check returns "successful" without impacting the existing TCP connection.

10.5.1.2 QoS requirements for IP transport

Serial raw socket data that is transported using an IP transport service can be DSCP marked at the source node. This allows the source node (local host) of the traffic to mark packets correctly so that downstream nodes prioritize them as needed, and to queue local traffic in the right egress queue based on the classification assigned to the IP transport service.

The node does not support FC classification; instead, it marks the DSCP in packets based on the IP transport subservice DSCP setting. This DSCP setting overrides the DSCP marking that would have otherwise been based on the egress network queue policy FC. These packets are queued on egress with all other control traffic and are considered high priority.

Additionally, the DSCP setting is assigned per IP transport subservice for all traffic from the local host and all traffic destined for each remote host. There is no per remote host control for the DSCP setting.

10.5.2 GNSS NMEA data IP transport service

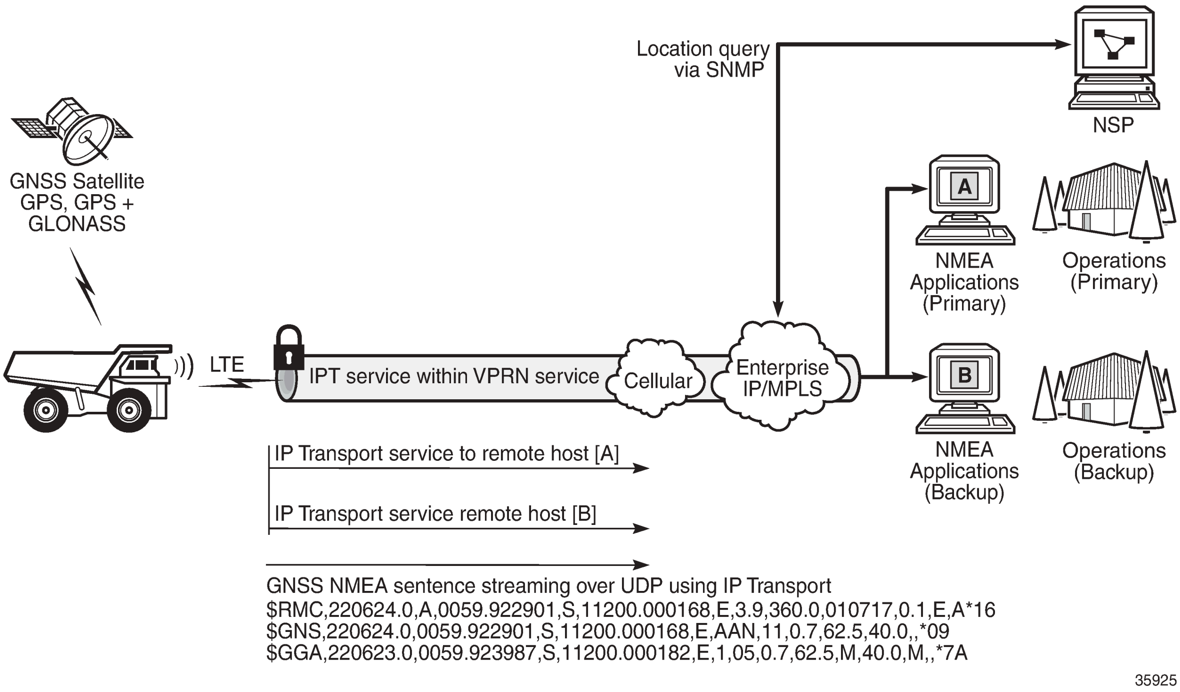
IP transport services are used to send GNSS National Marine Electronics Association (NMEA) data to remote hosts. All IP transport functionality supported for serial data over raw sockets is also available for NMEA data. See Raw socket IP transport service for information.

An IP transport subservice within a Layer 3 VPRN service can be configured to transmit GNSS NMEA data from the GNSS receiver (as the IP transport local host) to one or more remote hosts. See Figure 19: GNSS NMEA data over IP transport service. Any packets sent from remote hosts toward the local host of the IP transport subservice are dropped.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Figure 19: GNSS NMEA data over IP transport service



```
$RMC,220624.0,A,0059.922901,S,11200.000168,E,3.9,360.0,010717,0.1,E,A*16
$GNS,220624.0,0059.922901,S,11200.000168,E,AAN,11,0.7,62.5,40.0,,*09
$GGA,220623.0,0059.923987,S,11200.000182,E,1,05,0.7,62.5,M,40.0,M,,*7A
```

Use the following syntax to create an IP transport subservice within a VPRN service.

CLI syntax:

```
config>service
    vprn service-id [customer customer-id] [create]
        ip-transport ipt-id [create]
            description description-string
            filter-unknown-host
            local-host ip-addr ip-addr port-num port-num protocol {tcp
 | udp}
            remote-host host-id [ip-addr ip-addr] [port-num port-num]
 [create]
                description description-string
                name host-name
                exit
            shutdown
            tcp
                inactivity-timeout seconds
                max-retries number
                retry-interval seconds
            exit
        exit
    exit
exit
```

To enable the transport of NMEA data from the local host, configure the *ipt-id* as **gnss**. The following example is an IP transport subservice configuration output for the transport of NMEA data.

```
A:NOK-B>config>service>vprn# info
----------------------------------------------
        ip-transport gnss create
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                description "ip-transport to send NMEA data to multiple hosts"
                filter-unknown-host
                local-host ip-addr 192.0.2.1 port-num 2000 protocol tcp
                remote-host 1 create ip-addr 128.5.5.1 port-num 32000
                exit
                remote-host 2 create ip-addr 128.4.4.2 port-num 32000
                exit
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:NOK-B>config>service>vprn#
```

For information about configuring NMEA parameters on the GNSS receiver, see the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide*, "GNSS configuration".

10.5.3 Serial raw socket IP transport configuration commands hierarchy

```
config
    - service
        - vprn service-id [customer customer-id] [create]
            - ip-transport ipt-id [create]
            - no ip-transport ipt-id
                - description description-string
                - no description
                - dscp dscp-name
                - [no] filter-unknown-host
                - local-host ip-addr ip-addr port-num port-num protocol {tcp | udp}
                - no local-host
                - remote-host host-id [ip-addr ip-addr] [port-num port-num] [create]
                - no remote-host
                    - description description-string
                    - no description
                    - name host-name
                    - no name
                - [no] shutdown
                - tcp
                    - inactivity-timeout seconds
                    - max-retries number
                    - retry-interval seconds
```

10.5.3.1 IP transport configuration command descriptions

ip-transport

Syntax

ip-transport *ipt-id* [**create**]

no ip-transport *ipt-id*

Context

config>service>vprn

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Description

This command creates an IP transport subservice within a VPRN service. An IP transport subservice can be used to transmit serial raw socket data to and from a local host and remote host. An IP transport subservice can also be used to transmit GNSS NMEA data from the GNSS receiver to one or more remote hosts.

All IP transport subservices must be explicitly created using the **create** keyword. An IP transport subservice is owned by the service within which it is created. An IP transport subservice can only be associated with a single service. The **create** keyword is not needed when editing parameters for an existing IP transport subservice. An IP transport subservice must first be shut down before changes can be made to the configured parameters.

The **no** form of this command deletes the IP transport subservice with the specified *ipt-id*. When an IP transport subservice is deleted, all configured parameters for the IP transport subservice are also deleted.

Default

no ip-transport

Parameters

ipt-id

the physical port associated with the IP transport subservice

Values For serial raw sockets, the *ipt-id* must reference an RS-232 serial port that has been configured as a **socket** and be expressed in the format *slot*/*mda*/*port*

For a GNSS receiver, the *ipt-id* must be configured as **gnss**

create

creates this IP transport subservice

description

Syntax

description *description string*

no description

Context

config>service>vprn>ip-transport

config>service>vprn>ip-transport>remote-host

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.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Default

no description

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.

dscp

Syntax

dscp *dscp-name*

Context

config>service>vprn>ip-transport

Description

This command configures the DSCP name used to mark the DSCP field in IP transport packets originating from this node.

Default

ef

Parameters

dscp-name

the DSCP name used to mark the DSCP field in IP transport packets. Table 6: Valid DSCP names lists the valid DSCP names.

Table 6: Valid DSCP names

dscp-name
be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

filter-unknown-host

Syntax

[**no**] **filter-unknown-host**

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Context

config>service>vprn>ip-transport

Description

This command filters connections from unknown hosts. An unknown host is any host that is not configured as a remote host.

The **no** form of this command disables the filter.

Default

no filter-unknown-host

local-host

Syntax

local-host ip-addr *ip-addr***port-num** *port-num***protocol** {**tcp** | **udp**}

no local-host

Context

config>service>vprn>ip-transport

Description

This command creates the local host within the IP transport subservice.

The local host is required to accept TCP/UDP sessions initiated from far-end remote hosts, and for the node to initiate sessions toward the far-end remote hosts.

Note: When the IP transport ID is configured as **gnss**, any packets sent from remote hosts to the local host are dropped.

The local host must be created before a remote host is created.

The **no** form of this command deletes the local host.

Default

no local-host

Parameters

ip-addr

the IP address that is used for this local host. The IP address must be the same as a loopback or local interface IP address that is already configured within this service.

Values a.b.c.d (IPv4 address)

port-num

the port number that is used by remote hosts to establish TCP/UDP sessions to this local host

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Values 1026 to 49150

protocol {tcp | udp}

the protocol type that is used for all sessions to and from this local host, either tcp or udp

remote-host

Syntax

remote-host *host-id* **ip-addr** *ip-addr*] **port-num** *port-num* [**create**]

no remote-host *host-id*

Context

config>service>vprn>ip-transport

Description

This command creates a remote host within the IP transport subservice. Multiple remote hosts can be created in order to send serial raw socket data or GNSS NMEA data to remote destinations. The **create** keyword must be used for each remote host that is created.

The **no** form of this command deletes the remote host.

Default

no remote-host

Parameters

host-id

the remote host identifier

Values 1 to 2147483647or a name string up to 64 characters

ip-addr

the IP address that is used to reach the remote host in order to route IP transport packets to that remote host

Values a.b.c.d (IPv4 address)

port-num

the destination port number that is used to reach the serial port socket or the GNSS receiver on the remote host

Values 1 to 65535

create

creates this remote host

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

name

Syntax

name *host-name*

no name

Context

config>service>vprn>ip-transport>remote-host

Description

This command configures a unique name for this remote host.

The **no** form of this command deletes the remote host name.

Default

n/a

Parameters

host-name

a unique name for this remote host, up to 64 characters long

shutdown

Syntax

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

Context

config>service>vprn>ip-transport

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

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Special Cases

VPRN IP transport subservice

when an IP transport subservice within a VPRN service is shut down, all TCP/UDP packets received from remote hosts are dropped and any serial data received from the serial port is dropped. Any TCP connections that were up are closed and no new TCP connection requests are accepted.

It is not possible to make configuration changes to an IP transport subservice without performing a **shutdown** first.

The operational state of an IP transport subservice is relative to the operational state of the serial port or GNSS receiver for which the IP transport subservice is defined. When a serial port or GNSS receiver is shut down, the IP transport subservice associated with the serial port or GNSS receiver becomes operationally down.

When the **no shutdown** command is executed for an IP transport subservice, it becomes operationally up. Serial data from the serial port or NMEA sentence data from the GNSS receiver is encapsulated in TCP/UDP packets destined for remote hosts, and TCP/UDP packets can be received by the local host, where raw serial data is then sent out the serial port.

tcp

Syntax

tcp

Context

config>service>vprn>ip-transport

Description

This command creates the context to configure TCP parameters within this IP transport subservice.

Default

n/a

inactivity-timeout

Syntax

inactivity-timeout *seconds*

Context

config>service>vprn>ip-transport>tcp

Description

This command specifies how long to wait before disconnecting a TCP connection because of traffic inactivity over the connection.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Default

30 s

Parameters

seconds

how long to wait, in seconds, before disconnecting a TCP connection

Values 1 to 65535

max-retries

Syntax

max-retries *number*

Context

config>service>vprn>ip-transport>tcp

Description

This command specifies the number of times that a remote host, acting as a client, tries to establish a TCP connection after the initial attempt fails.

Default

5

Parameters

number

the number of attempts to establish a TCP connection after the initial attempt fails

Values 0 to 10

retry-interval

Syntax

retry-interval *seconds*

Context

config>service>vprn>ip-transport>tcp

Description

This command specifies how long to wait before each TCP **max-retries** attempt.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Default

5 s

Parameters

seconds

how long to wait, in seconds, before each TCP **max-retries** attempt

Values 1 to 300

10.5.4 IP transport show commands hierarchy

```
show
    - service
        - id service-id
            - ip-transport [ip-transport ipt-id]
                - remote-host host-id [detail | statistics]
        - ip-transport-using [ip-transport ipt-id]
```

10.5.4.1 IP transport show commands descriptions

id

Syntax

id *service-id*

Context

show>service

Description

This command displays information for a particular service ID

Parameters

service-id

identifies the service in the domain by service number or name

ip-transport

Syntax

ip-transport *ipt-id* [**detail** | **statistics**]

Context

show>service>id

Use subject to Terms available at: www.nokia.com/terms.

Description

This command displays information for a specified IP transport subservice within this service. If no IP transport subservice is specified, summary information is displayed for all IP transport subservices associated with the service.

Parameters

ipt-id

the physical port associated with the IP transport subservice

Values For serial raw sockets, the *ipt-id* must reference an RS-232 serial port that has been configured as a **socket** and must be expressed in the format *slot*/*mda*/*port*

For a GNSS receiver, the *ipt-id* must be configured as **gnss**

create

creates this IP transport subservice

detail

displays more information for the specified IP transport subservice

statistics

displays statistical information for the specified IP transport subservice

Output

The following outputs show examples of summary and detailed information for an IP transport subservice.

Output example

```
*A:Dut# show service id 100 ip-transport
=============================================================================
IP Transport (Summary), Service 100
=============================================================================
IptId     LocalIP         LocalPort Proto RemHost DSCP FltrUnkn Adm  Opr
-----------------------------------------------------------------------------
1/3/1     192.168.1.1     1026      udp   1       ef   enabled  Up   Down
-----------------------------------------------------------------------------
Entries found: 1
=============================================================================
*A:Dut#
```

```
*A:Dut# show service id 100 ip-transport 1/3/1 detail
===============================================================================
IP Transport
===============================================================================
Service Id         : 100 (VPRN)
IP Transport Id    : 1/2/4
Description        : (Not Specified)
Admin State        : Up                        Oper State          : Down
Oper Flags         : svcAdminDown portOperDown noIfAddress
Local IP Address   : 192.168.1.1               Local Port Number   : 1026
Local IP Protocol  : udp
DSCP               : ef                        Filter Unknown Host : enabled
TCP Inact Timeout  : 30
TCP Max Retries    : 5
TCP Retry Interval : 5
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
Num Remote Hosts   : 1
Last Mgmt Change   : 06/02/2017 11:15:50
Last Oper Change   : 06/02/2017 11:02:52
-------------------------------------------------------------------------------
IP Transport Accumulated Statistics
-------------------------------------------------------------------------------
Known Remote Hosts
  Packets sent                           : 0
  Characters sent                        : 0
  Packets received                       : 0
  Characters received                    : 0
  Connections                            : N/A
    To                                   : N/A
    From                                 : N/A
  Connection retries                     : N/A
  Connection failures                    : N/A
  Currently connected                    : N/A
Unknown Remote Hosts
  Packets sent                           : 0
  Characters sent                        : 0
  Packets received                       : 0
  Characters received                    : 0
  Successful connections from            : N/A
  Rejected due to unknown host filter    : 0
  Rejected due to out of resources       : 0
  Inactivity timeouts                    : N/A
  Last RemIp:RemPort                     : 0.0.0.0:0
  Currently connected                    : N/A
Dropped packets due to no remote hosts   : 0
===============================================================================
```

remote-host

Syntax

remote-host *host-id* [**detail** | **statistics**]

Context

show>service>id>ip-transport

Description

This command displays information for a specified remote host within this IP transport subservice within this service. If no remote host is specified, summary information is displayed for all remote hosts within this IP transport subservice.

Parameters

host-id

the remote host identifier

Values 1 to 2147483647or a name string up to 64 characters long

detail

displays more information for a specified remote host

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

statistics

displays summary information for a specified remote host

Output

The following outputs show examples of summary and detailed information for an IP transport subservice remote host.

Output example

```
*A:Dut# show service id 100 ip-transport remote-host
=============================================================================
IPT Remote Host (Summary), Service 100 IPT 1/3/1
=============================================================================
RemId      RemIp:RemPort         Rcvd Chars Sent Chars Drop Chars State
                                 Rcvd Pkts  Sent Pkts  Drop Pkts  Up Time
-----------------------------------------------------------------------------
2          192.168.1.1:1027      0          0          0          N/A
                                 0          0          0          N/A
-----------------------------------------------------------------------------
Number of known remote hosts: 1
Number of unknown remote hosts: N/A
Total entries found: 1
=============================================================================
*A:Dut#
```

```
*A:Dut#  show service id 100 ip-transport 1/3/1 remote-host 2 detail
===============================================================================
IPT Remote Host
===============================================================================
Service Id         : 100 (IES)
IP Transport Id    : 1/3/1
Remote Host Id     : 2
Name               : (Not Specified)
Description        : (Not Specified)
IP Address         : 192.168.1.6               Port Number         : 4000
Last Mgmt Change   : 12/07/2016 16:48:44
Session State      : connected                 Up Time             : 00h01m44s
Last Connect       : successful
-------------------------------------------------------------------------------
IPT Remote Host Statistics
-------------------------------------------------------------------------------
Sent Pkts       : 134                   Sent Chars      : 201000
Dropped Pkts    : 0                     Dropped Chars   : 0
Rcvd Pkts       : 267                   Rcvd Chars      : 201000
Session information
  Connections                            : 2
    To                                   : 1
    From                                 : 1
  Connection retries                     : 0
  Connection failures                    : 0
  Closed by far end                      : 1
  Inactivity timeouts                    : 0
===============================================================================
*A:Dut#
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

ip-transport-using

Syntax

ip-transport-using [**ip-transport** *ipt-id*]

Context

show>service

Description

This command displays IP transport subservice information for a specified port. If no port is specified, the command displays a summary of all IP transport subservices defined for this service.

Parameters

ipt-id

the physical port associated with the IP transport subservice

Values For serial raw sockets, the *ipt-id* must reference an RS-232 serial port that has been configured as a **socket** and must be expressed in the format *slot*/*mda*/*port*

For a GNSS receiver, the *ipt-id* must be configured as **gnss**

Output

The following output is an example of **ip-transport-using** information.

Output example

```
*A:Dut# show service ip-transport-using
=========================================
IP Transports
=========================================
IptId     SvcId      Type      Adm  Opr
-----------------------------------------
1/3/1     1          VPRN      Down Down
1/3/2     2          VPRN      Up   Down
-----------------------------------------
Entries found: 2
=========================================
*A:Dut#
```

10.5.5 IP transport clear commands hierarchy

```
clear
    - service
        - id service-id
            - ip-transport ipt-id
                - remote-host host-id
                    - statistics
                - statistics
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

10.5.5.1 IP transport clear commands descriptions

id

Syntax

id *service-id*

Context

clear>service

Description

This command clears commands for a specific service.

Parameters

service-id

uniquely identifies a service by service number or name

ip-transport

Syntax

ip-transport *ipt-id*

Context

clear>service>id

Description

This command clears IP transport statistics for this service.

Parameters

ipt-id

the physical port associated with the IP transport subservice

Values For serial raw sockets, the *ipt-id* must reference an RS-232 serial port that has been configured as a **socket** and must be expressed in the format *slot*/*mda*/*port*

For a GNSS receiver, the *ipt-id* must be configured as **gnss**

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

remote-host

Syntax

remote-host *host-id*

Context

clear>service>id>ip-transport

Description

This command clears statistics pertaining to a specified remote host assigned to this IP transport subservice.

Parameters

host-id

the remote host identifier

Values 1 to 2147483647or a name string up to 64 characters long

statistics

Syntax

statistics

Context

clear>service>id>ip-transport

clear>service>id>ip-transport>remote-host

Description

This command clears statistics-related information pertaining to all configured IP transport subservices or to all configured remote hosts for a specified IP transport subservice.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

11 Network group encryption

The 7705 SAR-Hm series of routers supports Network Group Encryption (NGE) for securing MPLS services and their related control plane. Supported NGE functions include the following:

- SDP encryption of Layer 2 and Layer 3 service
- VPRN encryption
- router interface and PDN interface encryption of control plane and data plane Layer 3 packets
- PW template encryption for BGP VPLS and BGP VPWS services

For information about router interface encryption commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*, **group-encryption** command descriptions.

For information about SDP, VPRN, and PW template encryption, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide*, "NGE".

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

12 Quality of Service

The 7705 SAR-Hm series of routers supports Quality of Service (QoS) as covered in the following topics:

- QoS policies
- Network QoS policies
- Network queue QoS policies
- Service ingress and egress QoS policies

12.1 QoS policies

For general information about QoS policies support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, "QoS policies":

- QoS overview
- Forwarding classes
- Queue parameters
- QoS policies overview
  – Service versus network QoS
  – QoS policy entities
  – Network QoS policies
  – Network queue QoS policies
  – Service ingress QoS policies
  – Service egress QoS policies
  – Configuration notes

12.2 Network QoS policies

This section describes Dedicated bearers functionality

For general information about network QoS policies support, see the following topics in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, "Network QoS Policies":

- Network QoS policies overview
- Network ingress
  – Network ingress tunnel QoS override
  – Network ingress IP match criteria
- Network egress
- Basic configurations

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- Service management tasks

For descriptions of network QoS policy commands, see 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*.

12.2.1 Dedicated bearers

A default bearer is established when the node first attaches to a cellular network for each cellular port that has an enabled SIM. An IP address is assigned for each default bearer and the node uses this IP address for the associated PDN router interface that is used to route traffic to and from the cellular network. See the PDN router interfaces section for information about PDN router interfaces and IP address assignment.

In addition to the default bearer, the node accepts network-initiated dedicated bearer establishment. The node does not initiate dedicated bearers toward the network.

Dedicated bearers provide a dedicated tunnel for specific types of traffic depending QoS requirements. Because they are established for the same cellular port as the default bearer, dedicated bearers use the same PDN router interface configured for the default bearer for sending and receiving traffic. Dedicated bearers can be a guaranteed bit rate (GBR) or non-GBR, whereas the default bearer can only be non-GBR. Dedicated bearers use traffic flow templates (TFTs) to provide special treatment to specific services that need to use the dedicated bearers.

The network programs TFTs on the cellular interface for each dedicated bearer. The TFTs contains at least one and up to eight packet filter items as follows:

- source address (with subnet mask)
- IP protocol number (TCP, UDP)
- destination port range
- source port range
- IPSec Security Parameter Index (SPI)
- type of Service (TOS) (IPv4)
- Flow-Label (IPv6 only)
- evaluation precedence index

The node expects only one TFT to be programmed by the network for each dedicated bearer. More than one TFT per dedicated bearer is not supported.

The node expects that the TFT programmed per dedicated bearer will contain only a TOS packet filter. Other TFT parameters, if they are specified and programmed, are not supported. The TOS packet filter enables mapping of egress packets that match the TOS settings to the corresponding dedicated bearer and provide GBR, or non-GBR, service for the traffic as required.

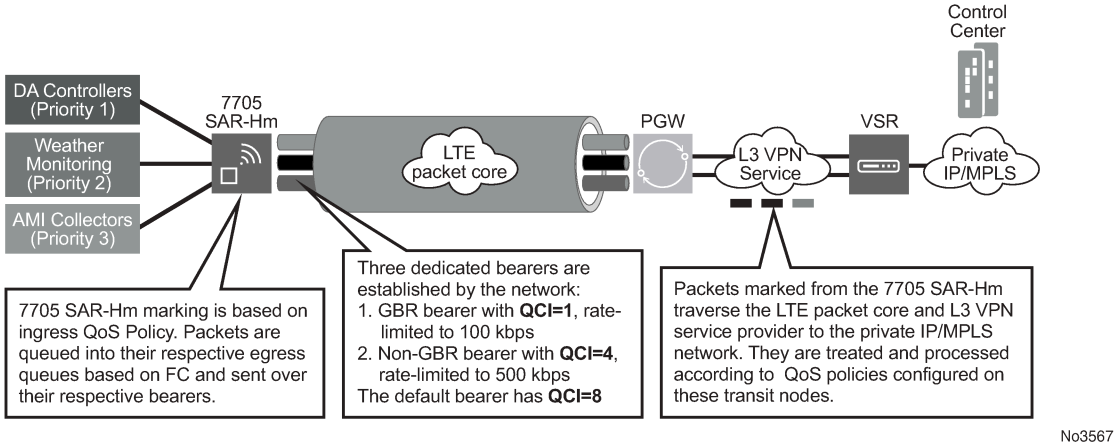
Operators must coordinate with their wireless service providers and subscribe for dedicated bearers with the specific TOS packet filter settings as required. Operators must then ensure that service ingress classification and marking for the respective traffic flows match the dedicated bearer TOS packet filter when services traffic must egress the radio interface on the dedicated bearer.

Figure 20: Dedicated bearer and differentiated services over a cellular network illustrates a typical use case for dedicated bearers to differentiate services over a cellular network.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Figure 20: Dedicated bearer and differentiated services over a cellular network


Control Center
DA Controllers (Priority 1)
Weather Monitoring (Priority 2)
AMI Collectors (Priority 3)
7705 SAR-Hm
LTE packet core
PGW
L3 VPN Service
VSR
Private IP/MPLS
No3567

7705 SAR-Hm marking is based on ingress QoS Policy. Packets are queued into their respective egress queues based on FC and sent over their respective bearers.

Three dedicated bearers are established by the network:
1. GBR bearer with **QCI=1**, rate-limited to 100 kbps
2. Non-GBR bearer with **QCI=4**, rate-limited to 500 kbps

The default bearer has **QCI=8**

Packets marked from the 7705 SAR-Hm traverse the LTE packet core and L3 VPN service provider to the private IP/MPLS network. They are treated and processed according to QoS policies configured on these transit nodes.

The following CLI output shows an example of bearer information configured on a cellular port.

```
*A:Dut-E# show port 1/1/1
===============================================================================
Cellular Interface
===============================================================================
...
==================================================================
Bearer Information
==================================================================
Bearer Id   Bearer Type   QCI   UL GBR   UL MBR   DL GBR   DL MBR
------------------------------------------------------------------
        5       default     5
        6     dedicated     1      100      200     1000    50000
        7     dedicated     9
==================================================================
==========================================================
Traffic Flow Template Packet Filters
==========================================================
Bearer Id   Filter Id   Precedence   Direction   TOS/Mask
----------------------------------------------------------
        6           1            1      uplink    0xc0/fc
        6           2            2    downlink    0x04/fc
        7           1          200        both
==========================================================
```

12.3 Network queue QoS policies

For general information about network queue QoS policies support, see the topics listed below in the*7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, "Network queue QoS policies":

- Basic configurations
  - Default network queue policy values

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

12.4 Service ingress and egress QoS policies

The 7705 SAR-Hm series of routers support the creation of SAP ingress QoS policies that filter on MAC criteria. For information, see MAC criteria filter.

For general information about service ingress and egress QoS policies support, see the topics listed below in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, "Network queue QoS policies":

- Basic configurations
- Service ingress QoS policy
  - Service ingress QoS queue
  - Ingress forwarding class (FC)
  - Ingress IP match criteria
  - Ingress IPv6 match criteria
- Service egress QoS policy
  - Service egress QoS queue
  - Egress percent-rate support
  - Egress SAP FC and FP overrides
  - Dot1p egress remarking
  - DSCP and IP precedence egress remarking
- Service management tasks

For descriptions of service ingress and egress QoS policy commands, see 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*.

12.4.1 MAC criteria filter

The 7705 SAR-Hm series of routers support the creation of ingress SAP QoS policies that filter on MAC information with the command **config>qos>sap-ingress>mac-criteria>entry>action fc**. Operators can filter packets based on Layer 2 MAC criteria to set the forwarding class (FC) for the packet when forwarding to the egress interface. MAC filtering is supported on all services.

The following CLI output shows an example of a MAC criteria filter configured on a VPLS SAP.

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/4
        ethernet
            mode access
        exit
        no shutdown
    exit
    port 1/1/9
        ethernet
            mode access
        exit
        no shutdown
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
    exit
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        sap-ingress 66 name "66" create
            queue 1 create
            exit
            queue 2 create
            exit
            queue 11 multipoint create
            exit
            fc "af" create
                queue 2
            exit
            fc "be" create
                queue 1
            exit
            mac-criteria
                entry 1 create
                    match frame-type ethernet-II
                        src-mac 00-14-14-14-00-02
                    exit
                    action fc "af"
                exit
            exit
        exit
        sap-ingress 67 name "67" create
            queue 1 create
            exit
            queue 2 create
            exit
            queue 11 multipoint create
            exit
            fc "af" create
                queue 2
            exit
            fc "be" create
                queue 1
            exit
            mac-criteria
                entry 1 create
                    match frame-type ethernet-II
                        src-mac 00-14-14-14-00-01
                    exit
                    action fc "af"
                exit
            exit
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 name "1" create
            description "Default customer"
        exit
        vpls 12 name "12" customer 1 vpn 12 create
            description "Default tls description for service id 12"
            stp
                shutdown
            exit
            sap 1/1/4 create
                description "Default sap description for service id 12"
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                static-mac 00:14:14:14:00:02 create
                ingress
                    qos 66
                exit
                no shutdown
            exit
            sap 1/1/9 create
                description "Default sap description for service id 12"
                static-mac 00:14:14:14:00:01 create
                ingress
                    qos 67
                exit
                no shutdown
            exit
            no shutdown
        exit
    exit
```

12.4.1.1 MAC criteria command reference

The 7705 SAR-Hm series of routers support the MAC criteria commands liststed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide* .

12.4.1.1.1 MAC criteria configuration commands

```
config qos sap-ingress
    mac-criteria
        entry entry-id [create]
        no entry entry-id
            [no] action [fc fc-name]
            description description
            no description
            match [frame-type {802dot3|802dot2-llc|802dot2-snap | ethernet-II}
            no match
                dot1p dot1p-value [dot1p-mask]
                no dot1p
                dsap dsap-value [dsap-mask]
                no dsap
                dst-mac ieee-address [ieee-address-mask]
                no dst-mac
                etype etype-value
                no etype
                inner-tag value [vid-mask]
                no inner-tag
                outer-tag value [vid-mask]
                no outer-tag
                snap-oui {zero | non-zero}
                no snap-oui
                snap-pid snap-pid
                no snap-pid
                src-mac ieee-address [ieee-address-mask]
                no src-mac
                ssap ssap-value [ssap-mask]
                no ssap
        renum old-entry-number new-entry-number
        type filter-type
        no type
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

13 OAM and diagnostics

The 7705 SAR-Hm series of routers supports OAM and diagnostics as described in OAM fault and performance tools and protocols.

13.1 OAM fault and performance tools and protocols

For general information about OAM, SAA, and OAM-PM support, see the topics listed below in the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide*, "OAM fault and performance tools and protocols":

- OAM overview
  - SDP diagnostics
    - SDP ping

For descriptions of OAM fault commands, see 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*.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

14 Multiservice Integrated Service Adapter and Extended Services Appliance

The 7705 SAR-Hm series of routers supports the Multiservice Integrated Adapter (MS-ISA) as covered in the following topics:

- IP tunnels
- Network Address Translation
- Application Assurance firewall

14.1 IP tunnels

This section describes IPSec secured interface over cellular functionality:

For general information about IP tunnel support, see the following topics in the *7450 ESS, 7750 SR, and VSR Multiservice ISA and ESA Guide*, "IP tunnels":

- IP tunnels overview
  - Tunnel ISAs
  - IPSec tunnel types
  - Operational conditions
  - QoS interactions
  - OAM interactions
  - Statistics collection
  - Security
  - IKEv2
  - SHA2 support
  - IPSec client lockout
  - IPSec tunnel CHILD_SA rekey
  - Multiple IKE/ESP transform support
  - Reverse routes for dynamic LAN-to-LAN IPsec tunnels
- Using certificates for IPSec tunnel authentication
- Trust-anchor profile
- Cert-profile
- IPSec deployment requirements
- IKEv2 remote-access tunnel
- Secured interface
- IPsec client database

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

- IPsec transport mode protected IP tunnel
- Configuring IPSec with CLI
- Quantum-safe IPSec
- IPSec troubleshooting guidelines

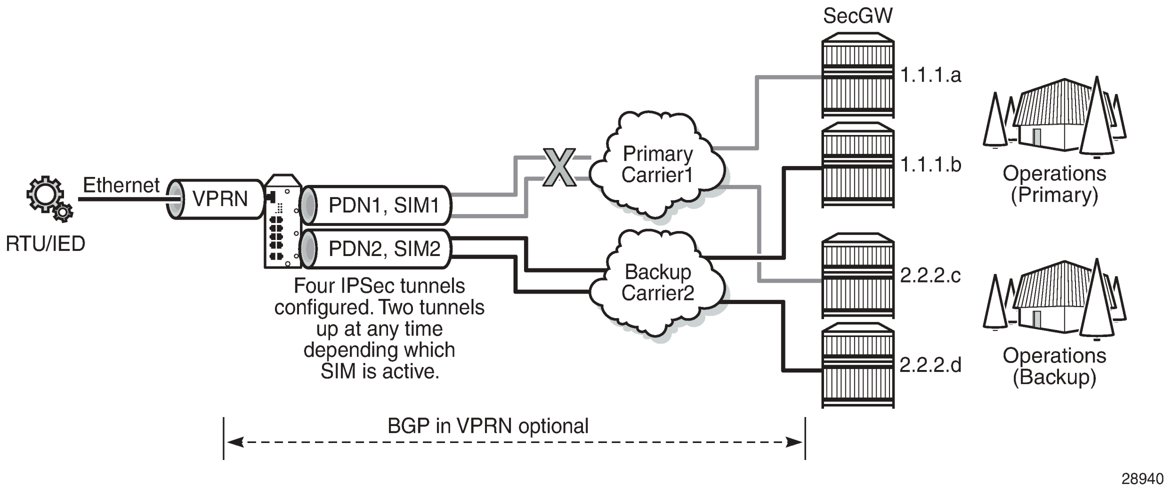
To configure and enable IP tunnels, the virtualized tunnel ISA MDA (isa-tunnel-v) must be configured in slot 5 or 6 on the router. See the *7705 SAR-Hm and SAR-Hmc Interface Configuration Guide* for information.

14.1.1 IPSec secured interface over cellular

The 7705 SAR-Hm series of routers supports IPSec secured interfaces over cellular interfaces.

Figure 21: IPSec secured interface over a cellular interface shows an example of an IPSec secured interface deployment over a cellular interface in a dual SIM environment.

Figure 21: IPSec secured interface over a cellular interface



With IPSec secured interfaces, static IPSec tunnels can be created under the PDN router interface associated for each SIM. When the SIM is active and the node attaches to the cellular network, the PDN router interface becomes operational. At that time, IPSec secured interface tunnels configured on the interface also begin to establish toward the security gateway they are configured to connect to. When the tunnel is established, data traffic traverses the IPSec secured interface. In Figure 21: IPSec secured interface over a cellular interface, only the pair of tunnels associated with the active SIM is operational.

The tunnel pair on the second PDN router interface is kept down and becomes operational when the second SIM becomes active.

Each IPSec secured interface tunnel is associated with one service. The supported service types are IES and VPRN.

Each service that needs to be secured over the PDN router interface must be configured with its own IPSec secured interface tunnel. For example if VPRN1, VPRN2, and VPRN3 all need to be secured, then three different IPSec secured interfaces are required, one for each service.

IPSec secured interface is supported on IPv4 and IPv6 PDN router interfaces.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

The following CLI output shows an example of IPSec secured interface configured on an IPv6 PDN router interface:

```
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        tunnel-group 1 isa-scale-mode tunnel-limit-32 create
            reassembly 2000
            multi-active
            mda 1/5
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router Base
        interface "lte-interface1" pdn
            port 1/1/1
            ip-mtu 1500
            ipv6
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "IPsec Configuration"
#--------------------------------------------------
    ipsec
        ike-transform 1 create
            dh-group 21
            ike-auth-algorithm sha384
            ike-encryption-algorithm des
        exit
        ike-policy 1 create
            ike-version 2
            dpd interval 10
            ike-transform 1
        exit
        ipsec-transform 1 create
            esp-auth-algorithm auth-encryption
            esp-encryption-algorithm aes256-gcm8
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        vprn 1 name "vprn1" customer 1 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-v6-ip 463c:f068:d815:e0ee:7ecf:5660::/96
                        remote-v6-ip c97e:a8fa:1785:52d7:9bb8:9b3b::/96
                    exit
                    entry 2 create
                        local-v6-ip 463c:f068:d815:e0ee:7ecf:5661::/96
                        remote-v6-ip c97e:a8fa:1785:52d7:9bb8:9b3c::/96
                    exit
                exit
            exit
            route-distinguisher 1.1.1.1:52
            static-route-entry c97e:a8fa:1785:52d7:9bb8::/80
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                ipsec-tunnel "tunnel1-vprn1"
                    no shutdown
                exit
            exit
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
    router Base
        interface "lte-interface1" pdn
            ipsec tunnel-group 1 public-sap 1
                ipsec-tunnel "tunnel1-vprn1" private-sap 1 private-service-
name "vprn1" create
                    encapsulated-ip-mtu 1300
                    remote-gateway-address 2001:90:10:3::2
                    security-policy 1
                    dynamic-keying
                        ike-policy 1
                        pre-shared-key "2KMbfx1sfSVdLxLEJsuVhs/
hfa42V3XyCZMLyubX" hash2
                        transform 1
                    exit
                    no shutdown
                exit
                no shutdown
            exit
        exit
    exit
```

14.2 Network Address Translation

This section describes the following Network Address Translation (NAT) functionality supported on the 7705 SAR-Hm series of routers:

- NAT with static port forwarding
- NAT on IPv4 interface
- NAT command reference

NAT runs on a single virtual ISA configured on the node. For general information about NAT support, see the topics listed below in the *7450 ESS, 7750 SR, and VSR Multiservice ISA and ESA Guide*, "Network Address Translation":

- Terminology
- Network Address Translation (NAT) overview
- Large scale NAT
- NAT pool addresses and ICMP Echo Request/Reply (ping)
- One-to-one (1:1) NAT
- NAT logging
  - Syslog, SNMP, local-file logging
  - SNMP trap logging
  - NAT syslog

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

- ISA feature interactions
  - MS-ISA use with service mirrors
- Configuring NAT

14.2.1 NAT with static port forwarding

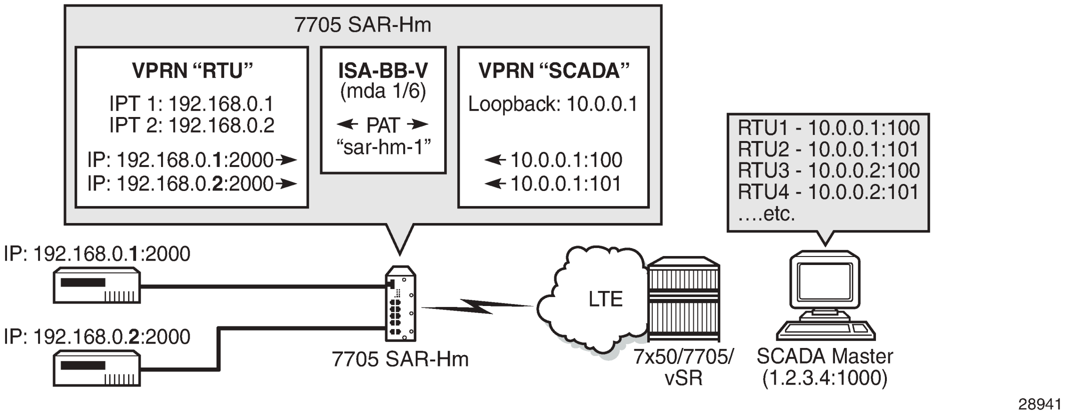
With NAT, the source IP address and the port of the host on the private side (inside) of the network are translated to an external IP address and port on the public side (outside) of the network. The IP address on the inside can be assigned to a raw socket IP host connected to an RS-232 serial interface or assigned to an IP interface associated with an Ethernet port.

Static port forwarding is configured on the CLI using the following parameters:

- inside IP address
- inside port
- outside IP address
- outside port
- protocol

Figure 22: NAT with static port forwarding shows an example of a network with a 7705 SAR-Hm series node configured to use NAT with static port forwarding.

Figure 22: NAT with static port forwarding



In the scenario shown above, the "RTU" VPRN service is inside and the "SCADA" VPRN service is outside. The "RTU" VPRN contains two IP transport services, one for each connected device. For information about IP transport services, see IP transport services and also see "Serial Transport over Raw Sockets" in the 7705 SAR-Hm and SAR-Hmc Interface Configuration Guide.

Figure 22: NAT with static port forwarding shows specific values for the inside IP address and port and outside IP address and port. The cellular interface of the node is used as the network-facing interface to transport the outside VPRN traffic.

When the SCADA master sends a packet to the node over the cellular network, it is carried within the outside "SCADA" VPRN service toward the node. The node sends the packet to the BB-ISA MDA to perform the required NAT function based on the configured NAT policy. NAT is applied to the packet as

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

needed. The packet is then processed by the inside "RTU" VPRN service, destined for the corresponding IP transport service.

When a packet is sent from the RTU toward the SCADA master, the inside "RTU" VPRN service sends the packet to the BB-ISA MDA where the NAT policy translates the IP address and port to the outside IP address and port, The BB-ISA MDA then sends the packet to the outside "SCADA" VPRN service where it is routed over the cellular interface using the "SCADA" VPRN service.

The following steps and CLI outputs show the configuration of NAT with static port forwarding based on Figure 22: NAT with static port forwarding.

1. Configure NAT on the BB-ISA MDA:

```
config
     isa
        nat-group 1
              mda 1/6
```

2. Configure the inside "RTU" VPRN (1) service for the inside static port forwarding NAT function:

```
config
     service
          vprn 1
             interface 'rtu1'
                 address 192.168.0.1/32
                 loopback
             interface 'rtu2'
                 address 192.168.0.2/32
                 loopback
             ip-transport 1/3/1
                 local-host ip-addr 192.168.0.1 port-num 2000 protocol udp
                 remote-host ip-addr 1.2.3.4 port-num 1000 protocol udp
             ip-transport 1/3/2
                 local-host ip-addr 192.168.0.2 port-num 2000 protocol udp
                 remote-host ip-addr 1.2.3.4 port-num 1000 protocol udp


config
     service
          vprn 1
             nat
                 inside
                     destination-prefix 1.2.3.4/24   .
                     nat-policy 'sar-hm-1'


config
     service
           nat
                nat-policy 'sar-hm-1
                     pool 'pool-name-1'  router 2
                port-forwarding
                    lsn router 1 ip 192.168.0.1 protocol udp port 2000 outside-
                                  ip 10.0.0.1 outside-port 100 nat-policy "sar-hm-1"
                    lsn router 1 ip 192.168.0.2 protocol udp port 2000 outside-
                                  ip 10.0.0.1 outside-port 101 nat-policy "sar-hm-1"
```

3. Configure the outside "SCADA" VPRN (2) service for the outside static port forwarding NAT function:

```
service vprn 2
     interface 'Outside_RTU'
        address 10.0.0.1/32
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
         loopback
      nat
         outside
                pool 'pool-name-1'nat-group 1 type large-scale
                          address-range 10.0.0.1 10.0.0.1 create
                          port-forwarding-range 30000
                          port-reservations ports 1000
```

14.2.2 NAT on IPv4 interface

This section provides information about NAT on IPv4 interfaces.

14.2.2.1 IPv4 interface as public NAT address

In addition to using dedicated IP address ranges in a NAT pool, which are completely disjoint from any local IPv4 interface, the 7705 SAR-Hm series of routers supports using the IPv4 address of an interface as the public IP address. The NAT pool adopts the interface IPv4 address as its public address. The interface address is either statically configured or learned dynamically from the cellular interface or from a DHCP server when a DHCP client is enabled on an Ethernet interface.

One NAT’d public interface is supported per routing context.

If an application on the public side initiates communication with a service expected to run on the public IP address (for example, SSH), a port-forward must be configured. This is necessary to allow a node on the public side to initiate an SSH connection to the 7705 SAR-Hm series of router over the NAT'd interface.

In this chapter, traffic that originates from or terminates on the public IPv4 address in the outside routing context, and traverses NAT toward the public side, is referred to as CPM traffic.

14.2.2.1.1 Access on the private side

NAT subscribers on the private side attach to the 7705 SAR-Hm series of router via the following:

- a network Layer 3 interface in the Base routing context or a service interface (IES or VPRN)
- an access Layer 3 interface tied to a spoke SDP
- R-VPLS

14.2.2.1.2 Public IPv4 address

The public IPv4 address used for NAT is one of the following:

- Obtained statically or dynamically on a cellular interface in Base (single SIM only)
- Statically configured on an interface in the Base routing context or on a SAP interface in an IES or VPRN service
- Dynamically obtained from a DHCP server when a DHCP client is configured on an interface in the Base routing context or on a SAP interface in an IES or VPRN service

Note:
When the public IPv4 address is obtained via DHCP on an IES SAP interface, the IES service requires an additional SAP interface with a statically configured IPv4 address for the DHCP client

to learn its IP address and transition to an operationally UP state. The address configured on the additional interface does not need to be routable or used in the network.

The following CLI output shows NAT configuration on a cellular interface:

```
A:node-2>config>router# info
----------------------------------------------
...
        interface "pdn1-loopback"
            loopback
            no shutdown
        exit
        interface "pdn1-sim1" pdn
            port 1/1/1
            unnumbered "pdn1-loopback"
            nat
                cpm-nat-policy <name>
                cpm-spf-nat-policy <name>
            exit
            no shutdown
        exit
----------------------------------------------
```

The following CLI output shows NAT configuration with DHCP client enabled on an IES SAP interface:

```
A:node-2>config>service# info
----------------------------------------------
...
        ies 1 name "demo" customer 1 create
            interface "public_interface_1" create
                autoconfigure
                    dhcp-client
                    no shutdown
                    client-id interface
                exit
            exit
            mac 00:10:01:00:00:01
            sap 1/2/1:1001 create
            exit
            nat
                cpm-nat-policy "cpm_policy_1"
            exit
        exit
        interface "any" create
            address 192.0.2.1/24
            sap 1/2/1:123 create
            exit
        exit
        no shutdown
    exit
----------------------------------------------
```

14.2.2.1.3 Source port allocation on NAT'd public interfaces

On a NAT'd public interface IP address, source ports are dynamically allocated individually, starting from the well-known range (greater than 1023) up to the end of the port range (65535). In other words, the NAT'd interface IPv4 address does not rely on port blocks.

Static port forwards can be allocated from the entire port range, including the well-known ports.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

14.2.2.1.3.1 Excluding ports from the public interface address

Certain UDP ports are reserved and excluded from allocation on the NAT'd public interface IPv4 address.

These ports are held in reserve to support the following applications, if configured:

- 68 – used by the DHCP client
- 500, 4500 – used by secure IPsec interfaces
- 3784, 3785, 4784 – used by BFD

14.2.2.1.4 Inbound access to local services over a NAT'd public interface

To enable external CPM traffic to reach the CPM over a NAT'd public interface, a CPM NAT policy must be associated with the public interface. Use the following commands to associate a CPM NAT policy:

```
configure router interface nat cpm-nat-policy
configure service ies interface nat cpm-nat-policy
configure service vprn interface nat cpm-nat-policy
```

Optionally, use the following commands to apply a CPM static port-forward NAT policy:

```
configure router interface nat cpm-spf-nat-policy
configure service ies interface nat cpm-spf-nat-policy
configure service vprn interface nat cpm-spf-nat-policy
```

Additionally, the listening port of the application must be explicitly opened by configuring a static port forward. This ensures that incoming traffic is correctly routed to the internal service behind NAT.

The following are examples of applications that require a static port-forward configuration:

- SSH, SCP, SFTP – TCP port 22
- BGP – TCP port 179
- NETCONF – TCP port 830 (over SSH) or TCP 22 (standard SSH)
- gNMI over TLS – TCP port 9339

14.2.2.1.5 Routing protocols over NAT'd interfaces

The public NAT interface can establish BGP and IGP peering, or neighbor relationships with external routing nodes.

14.2.2.1.6 Echo protocols over NAT'd interfaces

The public IPv4 address on the NAT'd interface responds to ICMP Echo Requests initiated from the public side. Conversely, it can also initiate ICMP Echo Requests toward nodes on the public side.

However, the NAT'd public interface IPv4 address does not respond to ICMP Echo Requests originating from the private side. Instead, users on the private side must direct Echo Requests to the IPv4 address configured on the private-facing interface.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Use the **configure router nat outside pool icmp-echo-reply** command to allow ICMP Echo Replies (ping responses) from a public IP interface:

14.2.2.1.7 Traceroute

The 7705 SAR-Hm series of routers supports traceroute initiated from the public side to a NAT'd public IPv4 address.

For ICMP-based traceroute, ICMP Echo Replies must be enabled (as noted in Echo protocols over NAT'd interfaces).

For UDP-based or TCP-based traceroute, port 33434 must be explicitly opened via static port forwards.

14.2.2.1.8 NAT policies using NAT'd interface address

A NAT policy defines the NAT pool selection for NAT subscribers on the private side and specifies applicable NAT behaviors, such as:

- Application Layer Gateway (ALG) support
- UDP/TCP session timeouts
- per-NAT subscriber session limits
- limits on the number of static port forwards allowed per-NAT subscriber

When a network interface is used as the public IP address, two distinct traffic paths, the transit path and local path, exist through the node.

The transit path is the traditional NAT path where subscriber traffic flows from the private side to the public side. The NAT policy is applied inside routing context, as shown in the following configuration example:

Note:
The NAT policy can also be associated with a **destination-profile** configuration or the **nat** IP filter action.

```
A:node-2>config>router>nat# info
---------------------------------------------
    inside
        nat-policy "demo-nat-policy"
    exit
---------------------------------------------
```

The local path handles CPM traffic that originates from or terminates on the node itself, such as SSH or FTP traffic. Because this traffic traverses the NAT'd interface, it also undergoes NAT processing. For such locally NAT'd traffic, a separate NAT policy is required, and the policy is applied directly under the public IP interface.

In this case, the source IP address for locally originated traffic may be one of the following:

- the interface public IPv4 address (that is, the NAT'd interface itself)
- a private IPv4 address behind NAT that is reachable in the outside routing context (via a directly configured interface or route leaking)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The NAT policy for this local path is configured using the **cpm-nat-policy** and **cpm-spf-nat-policy** commands under the interface, as shown in the following configuration example:

```
A:node-2>config>router>if# info
----------------------------------------------
    address 192.0.2.1/31
    port 1/2/1
    nat
        cpm-nat-policy "demo-cpm-nat-policy"
        cpm-spf-nat-policy "demo-cpm-spf-nat-policy"
    exit
    no shutdown
----------------------------------------------
```

The **cpm-nat-policy** is mandatory in cases where that traffic is locally originated or terminated on the NAT'd interface.

The **cpm-spf-nat-policy** is optional and is used to apply different NAT policy parameters specifically for static port-forwarded traffic. For example, a user can limit the number of sessions that an external host (from the public side) can establish on an open port via static port forwarding.

Note:
Neither of these two NAT policies is required if locally terminated traffic through NAT is not required. This includes scenarios such as ICMP ping requests sent to the NAT'd interface IP address from the public side. However, NAT must still enabled on the node for it to take effect on the public interface, as shown in the following configuration example:

The 7705 SAR-Hm series of routers supports traceroute initiated from the public side to a NAT'd public IPv4 address.

```
A:node-2>config>router>if# info
----------------------------------------------
    address 192.0.2.1/31
    port 1/1/c1/1
    nat
    exit
    no shutdown
----------------------------------------------
```

Both NAT'd transit traffic and local CPM traffic mapped to the same outside routing context share common NAT resources. Because local CPM traffic (originating from or destined for the node itself) is significantly smaller in scale than transit traffic, it is critical to protect NAT resources for local use, ensuring access to essential node functions such as SSH, FTP, or management protocols.

To guarantee availability for local traffic, the following NAT resources are afeguarded by the system:

- flows
- ports
- NAT subscribers

14.2.2.1.8.1 Excluding ports from the public interface address

The following measures are implemented to prevent local NAT traffic from being starved when the system reaches its flow capacity:

- 100 additional flows are reserved exclusively for local traffic once the node hits its maximum flow limit

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

- When the maximum flow scale is reached:
  - Only local flows are allowed to use the 100 reserved flows
  - The system removes the oldest transit flows to stay within the flow limit
  - Local traffic is also limited by the per-subscriber session limit defined in the NAT policy

While outbound local flows are under operator control, inbound local flows (for example, connections initiated from the public side to the 7705 SAR Gen 2) pose a higher security risk. Nokia recommends the following strategies to mitigate potential abuse:

- configure session limits in the NAT policy to cap the number of inbound flows per subscriber
- enable address and port-dependent filtering in the NAT policy to tighten access control
- use a dedicated NAT policy for static port forwards (**cpm-spf-nat-policy**) alongside the general **cpmnat-policy**. This allows the user to apply stricter parameters (such as session limits) specifically for port-forwarded traffic from the public side.

14.2.2.1.8.2 Local port protection

A configurable number of UDP/TCP ports are reserved exclusively for local traffic. Use the following commands to configure the number of reserved ports:

```
configure router nat outside pool cpm-reserved-ports
configure service vprn nat outside pool cpm-reserved-ports
```

The key behaviors for reserved and non-reserved ports include the following:

- Reserved ports are randomly selected from the available port range
- Non-reserved ports are shared between transit and local CPM traffic
- Reserved ports are only used when all shared ports are exhausted, ensuring that local applications always have access to a usable port range
- The number of reserved ports is configurable within the NAT pool

14.2.2.1.8.3 NAT subscriber protection

In the context of the NAT'd interface IP address, a NAT subscriber can be transit or local (private IPv4 address locally terminated on the 7705 SAR-Hm series router). The number of NAT subscriber resources is finite.

The following protections support local subscribers even when the system approaches its maximum NATsubscriber scale:

- An additional 8 NAT subscriber slots are reserved for local traffic
- When the maximum NAT subscriber count is reached, the system begins removing the oldest transit subscribers to ensure the total remains within system limits

14.2.2.1.9 NAT and IPsec secured interfaces

NAT and secure IP interfaces are supported on the same physical interface. See IPSec secured interface over cellular for information about configuring a secure IP interface.

© 2026 Nokia.

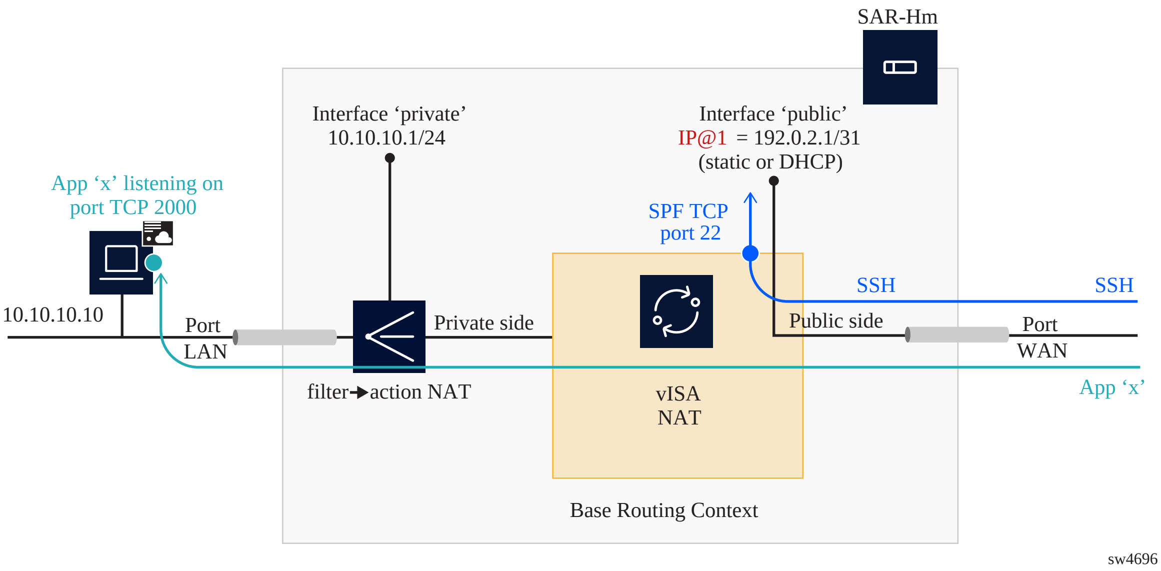
Use subject to Terms available at: www.nokia.com/terms.

14.2.2.1.10 NAT and IP configuration example

Procedure

The following figure shows a typical configuration example of NAT using a public interface IPv4 address. Both the private and public sides reside within the same routing context (Base router). Management access to the node is enabled from the public side via SSH using static port forwarding to the CPM. Additionally, a NAT subscriber on the private side runs application 'X', listening on TCP port 2000. This application is accessible from the public side through NAT using a transit port forward.

Figure 23: NAT with public IPv4 interface address



To configure NAT with a public IPv4 address:

Step 1. Configure the vISA in ‘broadband’ (bb) mode to enable NAT functionality with the **configure card mda mda-type** command.

```
A:node-2>config>card# info
----------------------------------------------
...
    mda 6
        mda-type isa-bb-v
        no shutdown
    exit
    no shutdown
----------------------------------------------
```

Step 2. Configure a NAT group that includes the broadband vISA with the **configure isa nat-group** command.

```
A:node-2>config>isa# info
----------------------------------------------
    nat-group 1 create
        active-mda-limit 1
        mda 1/3
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
        no shutdown
    exit
----------------------------------------------
```

Step 3. Configure NAT policies.

a. Configure a default transit NAT policy to associate with the inside routing context with the **configure service nat nat-policy** command. This NAT policy is required for transit traffic.

```
A:node-2>config>service>nat# info
----------------------------------------------
    nat-policy "demo-nat-policy" create
        pool "demo-pool" router Base
    exit
----------------------------------------------
```

b. Configure a CPM NAT policy to associate with the public NAT'd interface with the **configure service nat cpm-nat-policy** command. This policy is required only if there is NAT traffic that locally originates or terminates on the 7705 SAR SAR-Hm series router.

```
A:node-2>config>service>nat# info detail
----------------------------------------------
    nat-policy "demo-nat-policy" create
        alg
            ftp
        exit
...
----------------------------------------------
```

c. Optional: Configure another CPM NAT policy that can be used as an SPF-only NAT policy associated with the NAT'd public interface. This policy applies to port-forwarded traffic and is used to limit the number of sessions initiated by each external IPv4 host (in this example, to 20).

```
A:node-2>config>service>nat# info
----------------------------------------------
    cpm-nat-policy "demo-cpm-spf-nat-policy" create
...
        alg
            ftp
        exit
...
        session-limits
            max 20
            no watermarks
        exit
----------------------------------------------
```

Step 4. Associate the public NAT interface with CPM NAT policies to handle locally originated and terminated NAT traffic with the **configure router interface** command. A CPM NAT policy is mandatory if NAT traffic is initiated by, or destined for the local node. It is not required for transit traffic (that is, traffic passing through the node). Use the optional CPM SPF NAT policy if sessions initiated from the outside (for example, via static port forwards) require different NAT policy settings than locally originated traffic.

```
A:node-2>config>router# info
----------------------------------------------
…
    interface "pdn1-loopback"
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
        loopback
        no shutdown
    exit

    interface "pdn1-sim1" pdn
        port 1/1/1
        unnumbered "pdn1-loopback"
        nat
            cpm-nat-policy "demo-cpm-nat-policy"
            cpm-spf-nat-policy "demo-cpm-spf-nat-policy"
        exit
        no shutdown
    exit
…
----------------------------------------------
```

Step 5. Configure the NAT pool associated with the public (outside) interface with the **configure router nat outside pool** command.

```
A:node-2>config>router>nat>outside# info
----------------------------------------------
    pool "demo-pool" nat-group 1 type large-scale
    applications useinterface-ip create
        port-reservation ports 1
        port-forwarding-range 65535
        cpm-reserved-ports 20
        mode napt
        no shutdown
    exit
----------------------------------------------
```

Step 6. Configure a filter and apply it to the IPv4 interface to redirect traffic to NAT on the private side.

a. Configure the filter with the **configure filter ip-filter** command.

```
A:node-2>config>filter# info
----------------------------------------------
    ip-filter 1 name "demo-nat-filter" create
        entry 1 create
            action
                nat
            exit
        exit
    exit
----------------------------------------------
```

b. Apply the filter to the IPv4 interface with the **configure router interface ingress filter** command.

```
A:node-2>config>router# info
----------------------------------------------
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
...
    interface "demo-nat-private"
        address 10.10.10.1/24
        port 1/1/c2/1
        ingress
            filter ip 1
        exit
        no shutdown
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
    exit
...
----------------------------------------------
```

Step 7. Associate the default NAT policy on the private (inside) interface to handle transit traffic with the **configure router nat inside nat-policy** command.

```
A:node-2>config>router>nat# info
----------------------------------------------
    inside
        nat-policy "demo-nat-policy"
    exit
----------------------------------------------
```

Step 8. Configure port forwards for local SSH access through NAT (CPM port forwards) with the **configure service nat port-forwarding lsn** command. The CPM SPF NAT policy is optionally associated with a NAT public interface. If it is not configured, the user must explicitly reference the mandatory CPM NAT policy (in this case, "demo-cpm-nat-policy") in the static port-forward configuration.

Step 9. Enable persistence for the port forwards configured in step 8 using the **configure system persistence nat-port-forwarding location** command.

```
A:node-2>config>system>persistence>nat-fwd# info
----------------------------------------------
location cf2:
----------------------------------------------
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

14.2.3 NAT command reference

The 7705 SAR-Hm series of routers supports the NAT commands listed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

14.2.3.1 ISA configuration commands

```
config
    - isa
        - nat-group  nat-group-id [create]
        - no nat-group nat-group-id
            - active-mda-limit number
            - no active-mda-limit
            - description description-string
            - no description
            - [no] mda mda-id
            - [no] shutdown
            - [no] suppress-lsn-events
            - [no] suppress-lsn-sub-blks-free
```

14.2.3.2 NAT service configuration commands

```
configure
    - service
        - nat
            - nat-policy nat-policy-name [create]
            - no nat-policy nat-policy-name
                - block-limit [1..40]
                - no block-limit [
                - description description-string
                - no description
                - filtering filtering-mode
                - no filtering
                - pool nat-pool-name service-name service-name
                - pool nat-pool-name router router-instance
                - no pool
                - port-limits
                    - forwarding limit
                    - no forwarding
                    - watermarks high percentage-high low percentage-low
                    - no watermarks
                - session-limits
                    - max num-sessions
                    - no max
                    - watermarks high percentage-high low percentage-low
                    - no watermarks
                - tcp-mss-adjust segment-size
                - no tcp-mss-adjust
                - [no] timeouts
                    - icmp-query [min minutes] [sec seconds]
                    - no icmp-query
                    - tcp-established [hrs hours] [min minutes] [sec seconds]
                    - no tcp-established
                    - tcp-rst [min minutes] [sec sec]
                    - no tcp-rst
                    - tcp-syn [hrs hours] [min minutes] [sec seconds]
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                    - no tcp-syn
                    - tcp-time-wait [min minutes] [sec seconds]
                    - no tcp-time-wait
                    - tcp-transitory [hrs hours] [min minutes] [sec seconds]
                    - no tcp-transitory
                    - udp [hrs hours] [min minutes] [sec seconds]
                    - no udp
                    - udp-dns [hrs hours] [min minutes] [sec seconds]
                    - no udp-dns
                    - udp-inital [min minutes] [sec seconds]
                    - no udp-inital
                - [no] udp-inbound-refresh
            - port-forwarding
                - lsn router router-instance [b4 ipv6-address] [aftr ipv6-address] ip ip-
address protocol {tcp | udp} [port port] [outside-ip ipv4-address] [outside-port port] [nat-
policy nat-policy-name]
                - no lsn router router-instance [b4 ipv6-address] ip ip-address protocol {tcp
 | udp} port port [nat-policy nat-policy-name]
```

14.2.3.3 NAT VPRN commands

```
config
    - service
        - vprn service-id customer cust-id create
            - [no] nat
                - inside
                    - classic-lsn-max-subscriber-limit max
                    - no classic-lsn-max-subscriber-limit
                    - destination-prefix ip-prefix/length [nat-policy nat-policy-name]
                    - no destination-prefix ip-prefix/length
                    - deterministic
                        - prefix ip-prefix/length subscriber-type nat-sub-type nat-policy nat-
policy-name [create]
                        - prefix ip-prefix/length subscriber-type nat-sub-type
                        - no prefix ip-prefix/length subscriber-type nat-sub-type
                            - map start lsn-sub-address end lsn-sub-address to outside-ip-
address
                            - no map  start lsn-sub-address end lsn-sub-address
                            - [no] shutdown
                    - nat-policy nat-policy-name
                    - no nat-policy
                - outside
                    - mtu value
                    - no mtu
                    - poolnat-pool-name nat-group nat-group-id type pool-
type [applications applications] [create]
                    - no pool nat-pool-name
                        - address-range start-ip-address end-ip-address [create]
                        - no address-range start-ip-address end-ip-address
                            - description description-string
                            - no description
                            - [no] drain
                        - description description-string
                        - no description
                        - mode {auto | napt | one-to-one}
                        - no mode
                        - port-forwarding-range range-end
                        - no port-forwarding-range
                        - port-reservation blocks num-blocks
                        - port-reservation ports num-ports
                        - no port-reservation
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                        - subscriber-limit limit
                        - no subscriber-limit
                        - watermarks high percentage-high low percentage-low
                        - no watermarks
```

14.2.3.4 NAT persistence commands

The 7705 SAR-Hm series of routers supports the persistence commands listed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

```
config
    - system
        - persistence
            - nat-port-forwarding
                - description description-string
                - no description
                - location cflash-id
                - no location
```

14.2.3.5 NAT IPv4 filter policy commands

The 7705 SAR-Hm series of routers supports the NAT IPv4 filter policy commands listed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

```
config
    - filter
        - ip-filter filter-id [name filter-name] [create]
        - no ip-filter {filter-id | filter-name}
            - entry entry-id [create]
            - no entry entry-id
                - [no] action [secondary]
                    - nat [nat-policy nat-policy-name]
```

14.2.3.6 NAT routing protocol commands

The 7705 SAR-Hm series of routers supports the NAT routing protocol commands listed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

```
config
    - router
        - [no] policy-options]
            - [no] policy-statement name
                - entry entry-id [create]
                - no entry entry-id
                    - [no] from
                        - protocol protocol [all | instance instance]
                        - no protocol
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

14.2.3.7 NAT on IPv4 interface commands

The 7705 SAR-Hm series of routers supports the NAT on IPv4 commands listed in this section. For command descriptions, see the *7705 SAR Gen 2 Classic CLI Command Reference Guide*.

```
config
    - router
        - interface if-name [create] [pdn]
            - [no] nat
                - [no] cpm-nat-policy policy-name
                - [no] cpm-spf-nat-policy policy-name
```

```
config
    - service
        - ies/vprn service-id [customer] cust-id [create]
            - interface if-name [create]
                - [no] nat
                    - [no] cpm-nat-policy policy-name
                    - [no] cpm-spf-nat-policy policy-name
```

14.3 Application Assurance firewall

The 7705 SAR-Hm series of routers supports Application Assurance (AA) firewall (FW). The AA FW feature extends AA ISA Layer 3 and Layer 4 packet analysis to provide an in-line integrated stateful FW for additional security from malicious attacks. The AA stateful packet filtering feature empowers operators with per-session tracking features to monitor the security of each session. The AA FW runs on the AA ISA.

In a stateful inspection, the AA FW not only inspects Layers 3 and 4, but also monitors and keeps track of each connection’s state. If the operator configures a “deny” action within a session filter, the packets that match the session filter match conditions are dropped and no flow session state or context is created.

The AA FW feature is supported on the following SAP types

- VLLs (Epipes)
- VPLS
- IES/VPRN interfaces

Note: On the 7705 SAR-Hm series of routers, the AA FW supports application-level inspection at Layer 4 and below. References to application-level inspection above Layer 4 are not supported.

For general information about configuring an AA FW on the 7705 SAR-Hm series of routers, see the following topics in the *7450 ESS, 7750 SR, and VSR Multiservice ISA and ESA Guide*, “Application Assurance":

- AA overview
    - AA inline policy enforcement
    - Stateful firewall service
- AA system architecture
    - AA ISA resource configuration
        - AA ISA groups

© 2026 Nokia.

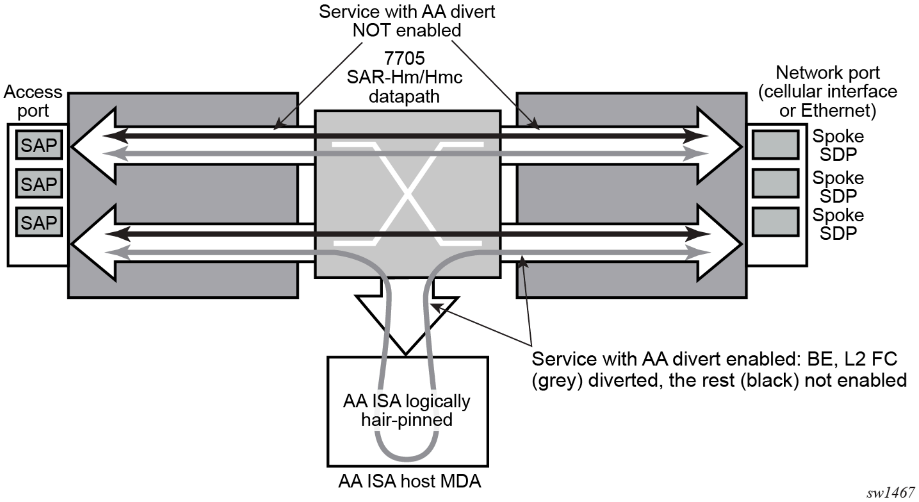
Use subject to Terms available at: www.nokia.com/terms.

  - AA packet processing
    - Divert of traffic and subscribers
    - Traffic identification
    - Statistics and accounting
    - AQP
    - AA firewall
  - Service monitoring and debugging (firewall stastistics)
  - CLI batch: begin, commit and abort commands
- Configuring AA with CLI
  - Configuring an AA ISA group
  - Configuring a group policy
    - Beginning, committing, and aborting a policy configuration
    - Configuring AA session filters
    - Configuring an application group
    - Configuring a policer
    - Configuring an application QoS policy

An AA FW is enabled by assigning an application profile to a SAP that requires flows to be inspected. The assignment enables the AA FW functionality for all traffic that is deemed of interest to and from the SAP. An application profile can be assigned to a VLL (Epipe) via the **config>service>epipe>sap>app-profile** command, to a VPLS via the **config>service>vpls>sap>app-profile** command, and to an IES or VPRN via the **config>service>ies | vprn>interface>sap>app-profile** commands.

Figure 24: AA FW datapath shows the general mechanism for filtering traffic of interest and diverting this traffic to the AA ISA. This traffic diversion method applies to both bridged and routed configurations.

Figure 24: AA FW datapath


Service with AA divert NOT enabled
7705 SAR-Hm/Hmc datapath
Access port
SAP
SAP
SAP
Network port (cellular interface or Ethernet)
Spoke SDP
Spoke SDP
Spoke SDP
Service with AA divert enabled: BE, L2 FC (grey) diverted, the rest (black) not enabled
AA ISA logically hair-pinned
AA ISA host MDA
sw1467

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

The following CLI output shows an example of an AA FW configured on a 7705 SAR-Hm series router. It includes ISA, application asssurance, and application assurance group configurations.

```
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        application-assurance-group 1 create
            description "ISA AA FW Group"
            primary 1/6
            fail-to-open
            divert-fc be
            statistics
                performance
                    collect-stats
                exit
            exit
            no shutdown
        exit
    exit

#--------------------------------------------------
echo "Application-assurance Configuration"
#--------------------------------------------------
    application-assurance
        flow-table-low-wmark 80
        flow-table-high-wmark 90
        group 1
            policer "flowCountPerSub_DL" type flow-count-limit granularity subscriber create
                description "Allow only a certain number of active flows at a time per
 subscriber"
                flow-count 50
                tod-override 1 create
                    time-range daily start 09:00 end 17:00
                    flow-count 25
                    no shutdown
                exit
            exit
            policer "flowCountPerSub_UL" type flow-count-limit granularity subscriber create
                flow-count 50
                tod-override 1 create
                    time-range daily start 09:00 end 17:00
                    flow-count 25
                    no shutdown
                exit
            exit
            policer "singeBucketSub" type single-bucket-bandwidth granularity subscriber create
                description "Sample bandwidth policer"
                rate 4096
                mbs 300
            exit
        exit
        group 1:0 create
            description "AA partition config"
            ip-prefix-list "IPL" create
                description "A sample IP prefix list"
                prefix 1.1.1.0/24
                prefix 10.1.1.135/32
                prefix 2607::/32
            exit
            event-log "EL" create
                buffer-type circular
                max-entries 1000
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                no shutdown
            exit
            port-list "PL" create
                description "Sample port list"
                port range 80 443
                port 8080
            exit
            policy
                begin
                app-service-options
                    characteristic "ASO" persist-id 1 create
                        value "val1" persist-id 1
                        value "val2" persist-id 2
                        default-value "val1"
                    exit
                exit
                app-profile "aa_firewall" create
                    divert
                    characteristic "ASO" value "val2"
                exit
                commit
            exit
            tcp-validate "TV" create
                description "A TCP validate object with strict checked linked to event-log"
                event-log "EL"
                strict
            exit
            session-filter "SF" create
                description "Deny unsolicited network flows except for a known TCP port"
                default-action deny event-log "EL"
                entry 1 create
                    match
                        ip-protocol-num tcp
                        src-ip ip-prefix-list "IPL"
                        src-port port-list "PL"
                    exit
                    action permit event-log "EL"
                exit
            exit
            session-filter "SF2" create
                description "Deny subscribers from sending ICMP"
                default-action permit
                entry 1 create
                    match
                        ip-protocol-num icmp
                    exit
                    action deny
                exit
            exit
        exit
    exit

#--------------------------------------------------
echo "Application-assurance Configuration"
#--------------------------------------------------
    application-assurance
        group 1:0
            policy
                begin
                app-qos-policy
                    entry 1 create
                        action
                            overload-drop
                            error-drop
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                            fragment-drop all
                        exit
                        no shutdown
                    exit
                    entry 2 create
                        action
                            tcp-mss-adjust 1500
                        exit
                        no shutdown
                    exit
                    entry 4 create
                        match
                            traffic-direction subscriber-to-network
                        exit
                        action
                            flow-count-limit "flowCountPerSub_UL"
                        exit
                        no shutdown
                    exit
                    entry 5 create
                        match
                            traffic-direction network-to-subscriber
                        exit
                        action
                            flow-count-limit "flowCountPerSub_DL"
                        exit
                        no shutdown
                    exit
                    entry 6 create
                        match
                            traffic-direction subscriber-to-network
                        exit
                        action
                            session-filter "SF2"
                        exit
                        no shutdown
                    exit
                    entry 7 create
                        match
                            traffic-direction network-to-subscriber
                        exit
                        action
                            session-filter "SF"
                        exit
                        no shutdown
                    exit
                    entry 8 create
                        action
                            tcp-validate "TV"
                        exit
                        no shutdown
                    exit
                    entry 9 create
                        match
                            characteristic "ASO" eq "val1"
                        exit
                        action
                            remark
                                fc ef
                            exit
                        exit
                        no shutdown
                    exit
                exit
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                commit
            exit
            policy-override
                policy aa-sub sap 1/2/3 create
                    characteristic "ASO" value "val1"
                exit
            exit
            statistics
                aa-admit-deny
                    collect-stats
                    session-filter-stats
                    policer-stats-resources
                    policer-stats
                    tcp-validate-stats
                exit
                aa-partition
                    collect-stats
                    traffic-type
                exit
                threshold-crossing-alert
                    fragment-drop-all direction from-sub create
                        high-wmark 4294967295 low-wmark 0
                    exit
                    session-filter "SF"
                        default-action direction to-sub create
                            high-wmark 4294967295 low-wmark 0
                        exit
                    exit
                exit
            exit
        exit
   exit
```

The following CLI output shows an example of an Epipe service configured with an "aa_firewall" application profile.

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
     service
        sdp 1 create
            description "Default sdp description"
            signaling off
            far-end 10.25.81.103
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        customer 1 name "1" create
            description "Default customer"
        exit
        epipe 1 name "1" customer 1 vpn 1 create
            description "Default epipe description for service id 1"
            service-mtu 1200
            sap 1/2/1 create
                description "Default sap description for service id 1"
                app-profile "aa_firewall"
                no shutdown
            exit
            spoke-sdp 1:101 create
                description "Description for Sdp Bind 1 for Svc ID 1"
                ingress
```

```
                    vc-label 101
                exit
                egress
                    vc-label 101
                exit
                no shutdown
            exit
            no shutdown
     exit
```

The following CLI output shows an example of a VPRN service configured with an "aa-firewall" application profile.

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 name "1" create
            description "Default customer"
        exit
        vprn 2 name "Sample VPRN 2" customer 1 create
            description "Default Description For VPRN ID 2"
            interface "interface_1" create
                address 1.1.1.1/24
                static-arp 1.1.1.2 8a:5a:47:e5:1d:7f
                ipv6
                    address 1::1/126
                    neighbor 1::2 8a:5a:47:e5:1d:7f
                exit
                sap 1/2/3:2 create
                    description "sap-2-none"
                    app-profile "aa_firewall"
                exit
            exit
            bgp-ipvpn
                mpls
                    auto-bind-tunnel
                        resolution-filter
                            no bgp
                        exit
                        resolution disabled
                    exit
                    route-distinguisher 100:2
                    no shutdown
                exit
            exit
            no shutdown
        exit
```

The following CLI output shows an example of an Epipe configured with AA FW event logging.

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 name "1" create
            description "Default customer"
        exit
        epipe 1 name "1" customer 1 create
            sap 1/2/3:10 create
                app-profile "aa_firewall"
                no shutdown
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
            exit
            sap 1/2/4:10 create
                no shutdown
            exit
            no shutdown
        exit
        ies 100 name "100" customer 1 vpn 100 create
            description "Default Ies description for service id 100"
            aa-interface "aa_if" create
                address 10.1.1.2/31
                sap 1/6/aa-svc:1 create
                    no shutdown
                exit
                no shutdown
            exit
            interface "ies-100-9.9.9.1" create
                address 9.9.9.1/24
                sap 1/2/6 create
                    description "sap-100-9.9.9.1"
                exit
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "Application-assurance Configuration"
#--------------------------------------------------
    application-assurance
        group 167:30712 create
            event-log "la8PQRgzyz6q87nIdJBolFLCiVRp0IG4" create
                buffer-type syslog
                max-entries 50000
                syslog
                    address 9.9.9.9
                    facility kernel
                    port 20001
                    severity notice
                    vlan-id 1
                exit
                no shutdown
            exit
            policy
                begin
                app-profile "aa_firewall" create
                    description "default-description for AppProfile aa_firewall"
                    divert
                exit
                app-qos-policy
                    entry 10 create
                        description "default-description for entry 10"
                        match
                            aa-sub sap eq 1/2/3:10
                        exit
                        action
                            fragment-drop out-of-order event-log "la8PQRgzyz6q87n
IdJBolFLCiVRp0IG4"
                        exit
                        no shutdown
                    exit
                exit
                commit
            exit
            statistics
                aa-admit-deny
                    collect-stats
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                    session-filter-stats
                    policer-stats-resources
                    policer-stats
                exit
            exit
        exit
```

14.3.1 AA FW command reference

The 7705 SAR-Hm series of routers supports the AA FW commands listed in this section. For command descriptions, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

14.3.1.1 ISA AA group configuration commands

```
— config
            — isa
               — application-assurance-group application-assurance-group-index [create] [aa-
subscale sub-scale]

               — no application-assurance-group application-assurance-group-index
                  — description description-string
                  — no description
                  — divert-fc fc-name
                  — no divert-fc
                  — [no] fail-to-open
                — [no] shutdown
                — statistics
                    — performance
                    — [no] collect-stats
```

14.3.1.2 AA configuration commands

```
— config
        — application-assurance
            — bit-rate-high-wmark high-watermark
            — no bit-rate-high-wmark
            — bit-rate-low-wmark low-watermark
            — no bit-rate-low-wmark
            — datapath-cpu-high-wmark high-watermark
            — datapath-cpu-high-wmark max
            — datapath-cpu-low-wmark low-watermark
            — flow-setup-high-wmark high-watermark
            — flow-setup-low-wmark low-watermark
            — no flow-setup-low-wmark
            — flow-table-high-wmark high-watermark
            — no flow-table-high-wmark
            — flow-table-low-wmark low-watermark
            — no flow-table-low-wmark
            — packet-rate-high-wmark high-watermark
            — packet-rate-low-wmark low-watermark
            — no packet-rate-low-wmark low-watermark
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

14.3.1.3 AA group configuration commands

```
config
        — application-assurance
                    — group  aa-group-id[:partition-id [create]]
                    — no group  aa-group-id:partition-id
                      — [no] aa-sub-remote
                      — description description-string
                      — no description
                      — event-log event-log-name [create]
                      — no event-log event-log-name
                         — buffer-type buffer-type
                         — max-entries max-entries
                         — [no] shutdown
                         — syslog
                           — address ip-address
                           — no address
                           — description description-string
                           — no description
                           — facility syslog-facility
                           — port port
                           — severity syslog-severity
                           — vlan-id  service-port-vlan-id
                           — no vlan-id
                      — ip-prefix-list ip-prefix-list-name [create]
                      — no ip-prefix-list ip-prefix-list-name
                          — description description-string
                          — no description
                          — prefix ip-prefix/ip-prefix-length [name prefix-name]
                          — no prefix ip-prefix/ip-prefix-length
                     — policer policer-name type type granularity granularity [create]
                     — no policer policer-name
                          — action  {priority-mark | permit-deny}
                          — adaptation-rule pir adaptation rule [cir {adaptation rule}]
                          — no adaptation-rule
                          — cbs  committed-burst-size
                          — no cbs
                          — description description-string
                          — no description
                          — flow-count flow-count
                          — no flow-count
                          — mbs maximum-burst-size
                          — no mbs
                          — rate  pir-rate [cir cir-rate]
                          — no rate
                          — tod-override tod-override-id create
                          — no tod-override tod-override-id
                              — cbs committed-burst-size
                              — no cbs
                              — description  description-string
                              — no description
                              — flow-count flow-count
                              — no flow-count
                              — mbs maximum-burst-size
                              — no mbs
                              — rate pir-rate [cir cir-rate]
                              — no rate
                              — [no] shutdown
                              — time-range daily start start-time end end-time [on day [day]]
                              — time-range weekly start start-time end end-time
                              — no time-range
                     — policy
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                          — abort
                          — app-profile app-profile-name [create]
                          — no app-profile app-profile-name
                              — [no] aa-sub-suppressible
                              — capacity-cost cost
                              — no capacity-cost
                              — characteristic  characteristic-name value value-name
                              — no characteristic  characteristic-name
                              — description description-string
                              — no description
                              — [no] divert
                          — app-qos-policy
                              — entry  entry-id [create]
                              — no entry  entry-id
                                  — action
                                      — bandwidth-policer policer-name
                                      — no bandwidth-policer
                                      — [no] drop
                                      — error-drop [event-log event-log-name]
                                      — no error-drop
                                      — flow-count-limit policer-name [event-log eventlogname]
                                      — no flow-count-limit [event-log eventlogname]
                                      — flow-rate-limit policer-name [event-log eventlogname]
                                      — no flow-rate-limit
                                      — fragment-drop {all | out-of-order} [event-log event-
log-name]

                                      — no fragment-drop
                                      — mirror-source [all-inclusive] mirror-service-id
                                      — no mirror-source
                                      — [no] overload-drop
                                      — remark
                                          — dscp in-profile dscp-name out-profile dscp-name
                                          — no dscp
                                          — fc fc-name
                                          — no fc
                                          — priority priority-level
                                          — no priority
                                      — session-filter session-filter-name
                                      — no session-filter
                                      — tcp-mss-adjust segment-size
                                      — no tcp-mss-adjust
                                      — tcp-validate tcp-validate-name
                                      — no tcp-validate
                              — description description-string
                              — no description
                              — match
                                — aa-sub sap {eq | neq} sap-id
                                — aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
                                — no aa-sub
                                — dscp {eq | neq} dscp-name
                                — no dscp
                                — dst-ip {eq | neq} ip-address
                                — dst-ip {eq | neq} ip-prefix-list ip-prefix-list-name
                                — no dst-ip
                                — dst-port {eq | neq} port-num
                                — dst-port {eq | neq} port-list port-list-name
                                — dst-port {eq | neq} range start-port-num endport-num
                                — no dst-port
                                — ip-protocol-num {eq | neq} protocol-id
                                — no ip-protocol-num
                                — src-ip {eq | neq} ip-address
                                — src-ip {eq | neq} ip-prefix-list ip-prefix-list-name
                                — no src-ip
                                — src-port {eq | neq} port-num
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                                – src-port {eq | neq} port-list port-list-name
                                – src-port {eq | neq} range start-port-num endport-num
                                – no src-port
                                – traffic-direction {subscriber-to-network | network-to-
subscriber | both}
                            – [no] shutdown
                          – app-service-options
                             – characteristic charateristic-name [create]
                             – no characteristic charateristic-name
                              – default-value value-name
                              – no default-value
                              – [no] value value-name
                          – begin
                          – commit
                     – port-list port-list-name [create]
                     – no port-list port-list-name
                          – description description-string
                          – no description
                          – [no] port port-number
                          – [no] port range start-port-number end-port-number
                     – session-filter session-filter-name [create]
                     – no session-filter session-filter-name
                          – default-action {permit | deny} [event-log event-log-name]
                          – description description-string
                          – no description
                          – entry entry-id[create]
                          – no entry
                             – action  {permit | deny | tcp-strict-order} [event-log event-
logname]
                             – action  http-redirect http-redirect-name[event-log event-
logname]
                             – description description-string
                             – no description
                             – match
                              – dst-ip ip-address
                              – dst-ip dns-ip-cache dns-ip-cache-name
                              – dst-ip ip-prefix-list ip-prefix-list-name
                              – no dst-ip
                              – dst-port {eq | gt | lt} port-num
                              – dst-port port-list  port-list-name
                              – dst-port range  start-port-num end-port-num
                              – no dst-port
                              – ip-protocol-num {ip-protocol-number | protocolname}
                              – no ip-protocol-num
                              – src-ip ip-address
                              – src-ip ip-prefix-list ip-prefix-list
                              – no src-ip
                              – src-port  {eq | gt | lt} port-num
                              – src-port range  start-port-num end-port-num
                              – no src-port
                     – statistics
                          – aa-admit-deny
                             – [no] collect-stats
                             – [no] policer-stats
                             – [no] policer-stats-resources
                             – [no] session-filter-stats
                             – [no] tcp-validate-stats
                          – aa-partition
                             – [no] collect-stats
                             – [no] traffic-type
                          – threshold-crossing-alert
                             – error-drop direction direction [create]
                             – no error-drop direction direction
                              – high-wmark high-watermark low-wmark low-watermark
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

```
                             — fragment-drop-all direction direction [create]
                             — no fragment-drop-all direction direction
                              — high-wmark high-watermark low-wmark low-watermark
                             — fragment-drop-out-of-order direction direction [create]
                             — no fragment-drop-out-of-order direction direction
                              — high-wmark high-watermark low-wmark low-watermark
                          — overload-drop direction direction [create]
                          — no overload-drop direction direction
                             — high-wmark  high-watermark low-wmark low-watermark
                          — policer policer-name direction direction [create]
                          — no policer policer-name direction direction
                             — high-wmark high-watermark low-wmark low-watermark
                          — session-filter session-filter-name
                             — default-action direction direction [create]
                             — no default-action direction direction
                              — high-wmark high-watermark low-wmark low-watermark
                             — entry entry-id direction direction [create]
                             — no entry entry-id direction direction
                              — high-wmark high-watermark low-wmark low-watermark
                          — tcp-validate tcp-validate-name direction direction [create]
                          — no tcp-validate tcp-validate-name direction direction
                              — high-wmark high-watermark low-wmark low-watermark
                — tcp-validate tcp-validate-name create
                — no tcp-validate tcp-validate-name
                          — description description-string
                          — no description
                          — event-log log event-log-name [all]
                          — no event-log
                          — [no] strict
```

14.3.1.4 AA interface configuration commands

```
config
        — service service-id
            — ies | vprn
                — aa-interface aa-if-name [create]
                — no aa-interface aa-if-name
                    — address  {ip-address/mask | ip-address netmask}
                    — no address  [ip-address/mask | ip-address netmask]
                    — description  description-string
                    — no description
                    — ip-mtu octets
                    — no ip-mtu
                    — sap  sap-id [create]
                    — no sap  sap-id
                        — description  description-string
                        — no description
                        — egress
                            — filter ip ip-filter-id
                            — no filter [ip ip-filter-id]
                            — qos  policy-id
                            — no qos  [policy-id]
                        — ingress
                            — qos  policy-id
                            — no qos  [policy-id]
                        — [no] shutdown
                    — [no] shutdown
```

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

14.3.1.5 AA show commands

```
— show
         — application-assurance
               — group aa-group-id[:partition-id]
                  — aa-sub sap sap-id [snapshot]
                  — aa-sub-list [isa mda-id]
                  — policy
                      — app-qos-policy [entry-id]
                  — status [isa mda-id]
                  — status isa mda-id overload
                  — tcp-validate tcp-validate-name [isa mda-id]
               — threshold-crossing-alert [detail]
```

14.3.1.6 AA tools commands

```
— tools
    — dump
          — application-assurance
               — group aa-group-id resources
               — group aa-group-id [:partition-id]
                  — admit-deny-stats
                  — event-log isa sap-id [snapshot]
```

15 Acronyms

Table 7: Numbers

Acronym	Definition
1DM	One-way Delay Measurement
6PE	IPv6 Provider Edge router. An MPLS IPv4 core network that supports IPv6 domains which communicate over an IES service.
6VPE	IPv6 Provider Edge router with IP-VPN Services. An MPLS IPv4 core network that supports the communication using IPv6 VPRN services.
2G	Second-generation wireless telephone technology
3DES	Triple DES (data encryption standard)
3G	Third-generation mobile telephone technology
4G	Fourth-generation mobile telephone technology
5G	Fifth-generation mobile telephone technology
NSP NFM-P	Network Services Platform Network Functions Manager - Packet
1830 PSS	1830 Photonic Service Switch
7705 SAR	7705 Service Aggregation Router
7210 SAS	7210 Service Access Switch
7450 ESS	7450 Ethernet Service Switch
7705 SAR	7705 Service Aggregation Router
7705 SAR-Hm	7705 Service Aggregation Router (vSR-based)
7750 SR	7750 Service Router
7950 XRS	7950 eXtensible Routing System

Table 8: A

Acronym	Definition
AA	Application Assurance
AA-ISA	Application Aware Integrated Service Adapter

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
AAA	AA-Answer
AAL	ATM Adaptation Layer
AAL5	ATM Adaptation Layer 5
AAR	AA-Request
AARP	AA Redundancy Protocol
ABM	Asynchronous Balanced Mode
ABR	Area Border Router Available Bit Rate
AC	Alternating Current Attachment Circuit
ACA	Accounting-Answer
ACCM	Async-Control-Character-Map
ACFC	Address and Control Field Compression
ACH	Associated Channel
ACK	Acknowledgment
ACL	Access Control List, also called filter policy
ACR	Accounting-Request Adaptive Clock Recovery
ADC	Application Detection and Control
ADI	Ad Insertion
ADI-LZ	Ad Insertion Local and Zoned
ADM	Add/Drop Multiplexer
ADP	Active Diameter Proxy Automatic Discovery Protocol
AFI	Address Family Identifier Authority and Format Identifier
AFTR	Address Family Transition Router
AGI	Address Group Identifier

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
AIGP	Accumulated IGP
AII	Attachment Individual Identifier
AIS	Alarm Indication Signal
ALE	Access-Loop-Encapsulation
ALG	Application-Level Gateway
ALMP	Auto-Learn-Mac-Protect
ALTO	Application Layer Traffic Optimiser
AMI	Alternate Mark Inversion
AN	Association Number
AMO	Any Mode of Operation
ANSI	American National Standards Institute
ANCP	Access Node Control Protocol
ANL	Access Network Location
API	Application Programming Interface
APN	Access Point Name
Apipe	ATM VLL
AP	Access Point
APN	Access Point Name
APS	Automatic Protection Switching
AQP	Application QoS Policies
ARFCN	Absolute Radio-Frequency Channel Number
ARP	Address Resolution Protocol
A/S	Active/Standby
AS	Autonomous System
ASAP	Any Service Any Port
ASAM	Advanced Services Access Manager
ASBR	AS Boundary Routers

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
ASID	Acct-Session-Id
ASM	Any-Source Multicast
ASN	Autonomous System Number
ASO	Application Service Option
AT	ATtention
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair

Table 9: B

Acronym	Definition
B-bit	Beginning bit (first packet of a fragment)
BBF	Broadband Forum
BC	Bandwidth Constraint
BCB	Backbone Core Bridge
BCG	Burst Control Group
BCP	Bridging Control Protocol
B-DA	Backbone Destination MAC Address
BEB	Backbone Edge Bridge
BECN	Backward Explicit Congestion Notification
Bellcore	Bell Communications Research
BER	Basic Encoding Rules
BER	Bit Error Rate
BERT	Bit Error Rate Test
BFD	Bi-directional Forwarding Detection
BGP	Border Gateway Protocol
BITS	Building Integrated Timing Source Building Integrated Timing Supply
B-MAC	Backbone source and destination MAC address fields defined in the 802.1ah provider MAC encapsulation header

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
BMCA	Best Master Clock Algorithm
BMU	Broadcast, Multicast, and Unknown traffic
BNG	Broadband Network Gateway
BOF	Boot Option File
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BPG or BPGRP	Bundle Protection Group
BR	Border Router
BRAS	Broadband Remote Access Server
BRG	Bridged Residential Gateway
BSA	Broadband Service Aggregator
BSAN	Broadband Service Access Node
BSC	Base Station Controller
BSD	Berkeley Software Distribution
BSM	Basic Subscriber Management
BSR	Bootstrap Router Broadband Service Router
BTS	Base Transceiver Station
BTSH	BGP TTL Security Hack
BTV	Broadcast Television
BUM	Broadcast, Unicast unknown and Multicast
B-VPLS	Backbone VPLS
BVID	Backbone VLAN ID
BVPLS	See B-VPLS
BVS	Business VPN Service
BW	Bandwidth

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Table 10: C

Acronym	Definition
CA	Certificate Authority Connectivity Association
CAC	Call Admission Control
CAK	Connectivity Association Key
CAM	Content Addressable Memory
CAS	Channel Associated Signaling
CBC	Cipher Block Chaining
CBF	Class-Based Forwarding
CBR	Constant Bit rate
CBRS	Citizens Broadband Radio Systems
CBS	Committed Buffer Size Committed Buffer Space Committed Burst Size
CC	Content of Communication Continuity Check Control Channel
CCA	Credit Control Answer Cross Connect Adapter
CCA-I	Credit Control Answer-Initial
CCA-T	Credit Control Answer-Terminate
CCA-U	Credit Control Answer-Update
CCAG	Cross Connect Aggregation Group
CCFH	Credit Control Failure Handling
CCID	Cross Connect Identifier
CCM	Chassis Control Module Continuity Check Message
CCR	Credit Control Request

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
CCR-I	Credit Control Request-Initiate
CCR-T	Credit Control Request-Terminate
CCR-U	Credit Control Request-Update
CCS	Common Channel Signaling
CDMA	Code Division Multiple Access
CDN	Call Disconnect Notify
CDP	Cisco Discovery Protocol
CDVT	Cell Delay Variation Tolerance
CE	Circuit Emulation Customer Edge Customer Equipment
CEA	Capability Exchange Answer
CEC	Circuit Emulation Concentrator
CEM	Circuit-Emulation
CER	Capability Exchange Request
CES	Circuit Emulation Services
CESoPSN	Circuit Emulation Services over Packet Switched Network
CF	Compact Flash
CFHP	Class Fair Hierarchical Policing
CFM	Connectivity Fault Management Control Forwarding Module
CFP	C form-Factor Pluggable
CGA	Cryptographically Generated Address
CGI	Cell Global Identification
CGN	Carrier Grade NAT
CHAP	Challenge Handshake Authentication Protocol
cHDLC	Cisco High-Level Data Link Control protocol
CHLI	Consecutive High Loss Intervals

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
CHV1	Card Holder Verification
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CKN	Connectivity association Key Name
CLEI	Common Language Equipment Identification
CLI	Command Line Interface
CLLI	Common Language Location Identifier
CLP	Cell Loss Priority
CMA	Compact Media Adapter
CMAC	Customer MAC
CMP	Certificate Management Protocol
CMTS	Cable Modem Termination System
CO	Central Office
CoA	Change of Authorization
confed-EBGP	Confederation External BGP
CoS	Class of Service
CP	Connection-Profile
CPE	Customer Premises Equipment
Cpipe	Circuit Emulation Pipe
CPM	Control Processing Module
CP/SFM	Control Processor/Switch Fabric Module
CPU	Control Processing Unit
CRC	Cyclic Redundancy Check
CRC-32	32-bit Cyclic Redundancy Check
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
CRON	a time-based scheduling service (from chronos = time)
CRP	Candidate RP
CSC	Carrier Supporting Carrier
CSC-CE	Carrier Supporting Carrier – Customer Edge Router
CSC-PE	Carrier Supporting Carrier – Provider Edge Router
CSF	Client Signal Fail
CSM	Control and Switching Module
CSN	Complete Sequence Number
CSNP	Complete Sequence Number PDU
CSP	Cloud Service Provider
CSPF	Constraint-based Shortest Path First
CSR	Cellsite Service Router
CSU	Channel Service Unit
CSV	Certificate Status Verification
C-TAG	Customer VLAN tag
CV	Connection Verification Customer VLAN (tag)
CVID	Customer VLAN ID
CW	Control Word

Table 11: D

Acronym	Definition
DACS	Digital Access Cross-connect System
DAD	Duplicate Address Detection
DA/FAN	Distribution Automation/Field Area Network
DC	Direct Current
DCCA	Diameter Credit Control Application
DCD	Data Carrier Detect

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
DCE	Data Circuit-terminating Equipment Data Communications Equipment
DCI	Client Defect Clear Indication Data Center Interconnect
DCP	Distributed CPU Protection
DCSC	Digital Channel Switch Capable
DDM	Digital Diagnostics Monitoring
DDMAP	Downstream Detailed Mapping
DDoS	Distributed DoS
DDP	Dynamic Data Persistency
DDR	Dial On Demand Routing
DDS	Dynamic Data Services
DE	Discard-Eligible
DEM	Dynamic Experience Management
DES	Data Encryption Standard
DEI	Drop Eligibility Indicator
DER	Distinguished Encoding Rules
DF	Delivery Function Do not Fragment
DF	Designated Forwarder
DH	Diffie-Hellman
DHB	Decimal, Hexadecimal, or Binary
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DHT	Distributed Hash Protocol
DLC	Data Link Control
DLCI	Data Link Connection Identifier
DLCMI	Data Link Connection Management Interface

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
DM	Delay Measurement
DMM	Delay Measurement Message
DMR	Delay Measurement Reply
DN	Domain Name
DNAT	Destination-based Network Address Translation
DNS	Domain Name System
DNSSEC	DNS Security
DNU	Do Not Use
DOD	Downstream On Demand
DORA	Discovery/Offer/Request/Ack
DoS	Denial of Service
dot1p	IEEE 802.1p bits, in Ethernet or VLAN ingress packet headers, used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPA	Disconnect Peer Answer
DPD	Dead Peer Detection
DPI	Digital Program Insertion
DPL	Delegated Prefix Length
DPLL	Digital Phase Locked Loop
DPR	Disconnect Peer Request
DPV	Designated Priority Vector
DR	Designated Router
DRA	Diameter Routing Agent
DRM	Digital Rights Management
DSA	Digital Signal Algorithm Direct System Agent
DSAP	Destination Service Access Point
DSC	Dynamic Services Controller

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
DSCP	Differentiated Services Code Point
DSFS	Data SAP Forwarding State
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSM	Distributed Subscriber Management
DSMAP	Downstream Mapping
DSS	Digital Signature Standard
DTC	DHCP Transaction Cache
DTD	Dynamic Topology Discovery
DTE	Data Terminal Equipment
DTP	Digital Trunking Protocol
DU	Downstream Unsolicited
DUID	DHCP Unique Identifier
DUS	Do not Use for Synchronization
DVB	Digital Video Broadcasting
DVMRP	Distance Vector Multicast Routing Protocol
DWA	Device Watchdog Answer
DWDM	Dense Wavelength Division Multiplexing
DWR	Device Watchdog Request

Table 12: E

Acronym	Definition
e2e	End-to-End
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	Ending bit (last packet of a fragment)
eBGP or EBGP	External Border Gateway Protocol
EBS	Error Burst Size

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
E-BSR	Elected BSR
ECID	Emulated Circuit Identifiers
ECGI	E-UTRAN Cell Global Identifier
ECMP	Equal Cost Multipath
ECT	Equal Cost Tree
EEPROM	Electronically Erasable Programmable Read-Only Memory
EFCI	Explicit Forward Congestion Indication
EFEC	Enhanced Forward Error Correction
EFH	Extended Failure Handling
EFM	Ethernet in the First Mile
EGP	Exterior Gateway Protocol
EHS	Event Handling System
EIC	Ethernet Interface Counters
EIGRP	Enhanced Interior Gateway Routing Protocol
EIR	Excess Information Rate
E-LAN	Ethernet Local Area Network
eLER	Egress Label Edge Router
E-Line	Ethernet Virtual Private Line
eLMI	Ethernet Local Management Interface
EMR	Efficient Multicast Replication
EMS	Enhanced Subscriber Management
eNB	Evolved Node B
EOOL	End of Options List
EOM	End-of-Message
EOR	End-of-RIB
EPC	Evolved Packet Core
EPD	Ethernet Port Damping

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
Epipe	Ethernet Pipe Ethernet VLL
EPL	Ethernet Private Line
EPS	Equipment Protection Switching
ERO	Explicit Router Object
ERP	Ethernet Ring Protection
ES	Elementary Stream
ESF	Extended Super Frame
ESI	Ethernet Segment Identifier
ESM	Enhanced Subscriber Management
ESMC	Ethernet Synchronization Messaging Channel
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ESR	Extended Services Router
ETE	End-to-End
ETH	Ethernet
ETH-CFM	Ethernet Configuration and Fault Management Ethernet Connectivity Fault Management (IEEE 802.1ag)
ETH-TST	Ethernet Test
ETR	Extended Temperature Range
ETSI	European Telecommunications Standards Institute
ETYPE	EtherType
EUI-64	64-bit Extended Unique Identifier
EVC	Ethernet Virtual Connections
EVI	EVPN Instance
EVPL	Ethernet Virtual Private Link
EVPN	Ethernet VPN
EXEC	Execute

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
EXP bits	Experimental bits (currently known as TC)

Table 13: F

Acronym	Definition
FAP	Femto Access Point
FASTE	FastE SFP type
FC	Forwarding Class
FCC	Fast Channel Change
FCS	Frame Check Sequence
FD	Frame Delay Frequency Diversity
FDB	Forwarding Database
FDDI	Fiber Distributed Data Interface
FDI	Forward Defect Indication
FDL	Facilities Data Link
FDR	Frame Delay Range
FEAC	Far-End Alarm and Control
FEBE	Far-End Block Error
FEC	Forwarding Equivalence Class Forward Error Correction
FECN	Forward Explicit Congestion Notification
FENT	Fast Ethernet Network Termination
FEPL	Far-End Protection-Line
FF	Fixed Filter
FIB	Forwarding Information Base
FID	Forwarding ID
FIFO	First In, First Out
FIN	Finish Bit Set

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
FIPS	Federal Information Processing Standards
FIR	Fair Information Rate
FIX	Financial Information eXchange
FLR	Frame Loss Ratio
FOM	Figure of Merit
FPE	Forwarding Path Extension
FPGA	Field Programmable Gate Array
Fpipe	Frame-Relay VLL
F-PLMN	Forbidden PLMN
FPP	Floor Packet Percentage
FPRI	Fine-grained Priority
FQDN	Fully Qualified Domain Name
FQF	Fully Qualified Flows
FR	Frame Relay
FRG	Fragmentation bit
FRR	Fast Reroute
FSG	Fate Sharing Group
FSM	Finite State Machine
FTN	FEC-to-NHLFE
FTP	File Transfer protocol
FTTH	Fiber to the Home

Table 14: G

Acronym	Definition
G-ACh	Generic Associated Channel
GAL	Generic ACH Label
GARP	Gratuitous ARP
GBMAC	Group BMAC

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
GBR	Guaranteed Bit Rate
GFEC	G.709 FEC
GFP	Generic Framing Procedure
GGSN	Gateway GPRS Support Node
GID	Global-ID
GigE	Gigabit Ethernet
GIGE	GigE SFP type
GIGX	GigX SFP
gLSP	GMPLS LSP
GMPLS	Generalized Multi-Protocol Label Switching
GMR	IGMP Group-specific Membership Report
GMRE	GMPLS Routing Engine
GNSS	Global Navigation Satellite System
GOP	Group of Pictures
GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GPS	Global Positioning System
GR	Graceful Restart Guaranteed Restoration
GRACE	Graceful restart
GRE	Generic Routing Encapsulation
GRT	Global Routing Table
GSMP	General Switch Management Protocol
GSU	Granted Service Unit
GTP	GPRS Tunneling Protocol
GUA	Global Unicast Address
GVRP	GARP VLAN Registration Protocol

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 15: H

Acronym	Definition
HA	High Availability
HD	High Definition
HDLC	High-level Data Link Control protocol
HEC	Header Error Control
HGW	Home Gateway
HLI	High Loss Interval
HLR	Home Location Register
HMAC	Hash-based Message Authentication Code Hash Message Authentication Code
HLE	Home LAN Extension
H-OFS	Hybrid OpenFlow Switch
H-POL	Hierarchical Policing
H-QoS	Hierarchical Quality of Service
HSDPA	High-Speed Downlink Packet Access
HSDSL	High Speed Digital Subscriber Line
HSI	High Speed Internet
HSMDA	High Scale MDA
HSPA	High-Speed Packet Access
HSS	Home Subscriber Service
HTTP	Hyper-Text Transfer Protocol
HTTPS	HTTP Secure
HVPLS	Hierarchical Virtual Private Line Service

Table 16: I

Acronym	Definition
IAD	Integrated Access Device
IAID	Identity Association Identification

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
IANA	Internet Assigned Numbers Authority
IA-NA	Identity Association for Non-Temporary Addresses
IA-PD	Identity Association for Prefix Delegation
IAPP	Inter Access Point Protocol
IBGP	Interior Border Gateway Protocol
IBN	Isolated Bonding Network
IB-RCC	In-Band Ring Control Connection
ICAP	Internet Content Adaptation Protocol
ICB	Inter-Chassis Backup
ICC	Inter-Card Communication
ICCID	Integrated Circuit Card Identifier
ICCN	Incoming Call Connected
ICK	Integrity Connection Value Key
ICL	Inter-Chassis Link
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
ICP	IMA Control Protocol
ICRQ	Incoming Call Request
ICV	Integrity Connection Value Integrity Check Value
IDi	Identification Indicator (an IKEv2 protocol payload)
IDr	Identification Responder
IDS	Intrusion Detection System
IDU	InDoor Unit
IEEE	Institute of Electrical and Electronics Engineers
I-ES	Interconnect Ethernet-Segment
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
IFDV	InterFrame Delay Variation
IFF	Inbound FEC Filtering
IFG	Inter-Frame Gap
IGD	Internet Gateway Device
IGH	Interface Group Handler
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IID	Instance ID
IIH	IS-IS Hello
IIN	Issuer Identification Number
IKE	Internet Key Exchange
iLDP	Interface Label Distribution Protocol
ILER	Ingress Label Edge Router
ILM	Incoming Label Map
ILMI	Integrated Local Management Interface
IMA	Inverse Multiplexing over ATM
IME	Interface Management Entity
IMEI	International Mobile Equipment Identity
IMEISV	International Mobile Equipment Identity and its Software Version
IMET	Inclusive Multicast Ethernet Tag
IMM	Integrated Media Module
IMPM	Ingress Multicast Path Management
IMSI	International Mobile Subscriber Identification
IOM	Input/Output Module
IOTA	Internet Over the Air (CDMA)
IP	Internet Protocol

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
IP-CAN	IP Connectivity Access Network
IPCC	IP Communication Channel IP Control Channel
IPCP	Internet Protocol Control Protocol
IPFIX	IP Flow Information Export
IPG	Inter-Packet Gap
Ipipe	IP Pipe IP Interworking VLL
IPL	IP Length
I-PMSI	Inclusive Provider Multicast Service Interface
IPOE	IP over Ethernet
IPS	Intrusion Prevention System
IPsec	IP Security
IPTV	Internet Protocol Television
IP-VPN	Internet Protocol Virtual Private Network
IRB	Integrated Routing and Bridging
IRI	Intercept Related Information
ISA	Integrated Service Adapter
ISA-AA	Integrated Service Adapter - Application Assurance
ISAKMP	Internet Security Association and Key Management Protocol
ISAM	Intelligent Services Access Manager
ISID	I-component Service ID I-Service Instance Identifier
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSU	In-Service Software Upgrade
IST	Internal Spanning Tree

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
I-TAG	Service Instance TAG
ITU-T	International Telecommunications Union - Telecommunications
IWF	Interworking Function

Table 17: J

Acronym	Definition
JID	JabberID
JOLT	Java OnLine Transactions
JP	Join Prune

Table 18: K

Acronym	Definition
KAT	Keepalive Timer
KPI	Key Performance Indicators

Table 19: L

Acronym	Definition
L2TP	Layer 2 Tunneling Protocol
LA	Location Area
LAA	Local Address Assignment
LAC	L2TP Access Concentrator
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAI	Local Area Identity
L-AIS	Line Alarm Indication Signal
LAN	Local Area Network
LAND	Local Area Network Denial
LB	Label Base Loopback

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
LBM	Loopback Message
LBR	Loopback Reply Loopback Response
LCD	Loss of Cell Delineation
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL/STL
LDP	Label Distribution Protocol
LDPoRSVP	LDP over RSVP
LDRP	Lightweight DHCPv6 Relay Agent
LER	Label Edge Router
LFA	Loop-Free Alternate
LFI	Link Fragmentation and Interleaving
LIB	Label Information Base
LIF	Loss of IMA Frame
LIG	Lawful Intercept Gateway
LLA	Link Local Address
LLC	Link Layer Control Logical Link Control
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LLF	Link Loss Forwarding
LLGR	Long Lived Graceful Restart
LLID	Loopback Location ID
LM	Loss Measurement
LMM	Loss Measurement Message
LMI	Local Management Interface
LMR	Loss Measurement Response

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
LMP	Link Management Protocol
LNS	L2TP Network Server
LOC	Loss of Continuity
LODS	Link Out of Delay Synchronization
LOF	Loss of Frame
LOP	Loss of Packets
LOS	Loss of Signal
LoT	Loss of Transmission
LPM	Longest Prefix Match
LPN	Label per Next hop
LPP	Label per Prefix
LPT	Logical Port Type
LPT-S	Logical Port Type Subtype
LPT-V	Logical Port Type Value
LQR	Link Quality Report
LR	Label Route
LSA	Link-State Advertisement
LSB	Least Significant Bit
LSDB	Link-Sate Database
LSN	Large-Scale NAT
LSP	Link-State PDU (for IS-IS) Label-Switched Path
LSR	Link-state Request Label Switch Router
LSU	Link-State Update
LT	Linktrace
LTE	Line Termination Equipment Long Term Evolution

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
LTM	Linktrace Message
LTN	LSP ID to NHLFE
LTR	Linktrace Reply Linktrace Response
LTS	L2TP Tunnel Switching
LUB	Limit Unused Bandwidth
LUDB	Local User Data Base

Table 20: M

Acronym	Definition
MA	Maintenance Association
MA-ID	Maintenance Association Identifier
MAC	Media Access Control
MACsec	Media Access Control Security
MAF	Management Access Filter
MAM	Maximum Allocation Model
MAN	Metropolitan Area Network
MAR	Mobile Aggregation Router
MAT	MAC Address translation
MBB	Make-Before-Break
MBGP	Border Gateway Protocol with Multi-protocol extensions
MBH	Mobile BackHaul
MBR	Maximum Bit Rate
MBS	Maximum Buffer Size Maximum Burst Size Media Buffer Space
MBZ	Must Be Zero
MCAST	Multicast
MC-APS	Multi-Chassis Automatic Protection Switching

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
MC-CTL	Multi-Chassis Control Link
MC-EP	Multi-Chassis Endpoint
MC-IPSec	Multi-Chassis IPSec redundancy
MC-LAG	Multi-Chassis Link Aggregation
MC-MLPPP	Multi-Chassis Multilink Point-to-Point Protocol Multi-Class Multilink Point-to-Point Protocol
MCAB	Maximum Configurable ATM Bandwidth
MCAC	Multicast Connection Admission Control
MCC	Mobile Country Code
MCLT	Maximum Client Lead Time
MCM	MDA Carrier Module
MCR	Mobile Core Router
MC-RING	Multi-Chassis Ring
MCS	Multi-Chassis Synchronization
MD	Maintenance Domain
MD5	Message Digest version 5 (algorithm)
MDA	Media Dependent Adapter
MDI	Media Dependent Interface
MDL	Maintenance Data Link
MDN	Mobile Directory Number
MDT	Multicast Distribution Tree
MDU	Multiple Dwelling Unit
MDX	Media Dependent Interface with crossovers
ME	Maintenance Entity
MED	Multi-Exit Discriminator
MEF	Metro Ethernet Forum
MEG	Maintenance Entity Group
MEP	Maintenance Association Endpoint

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
	Maintenance Endpoint
MEP-ID	Maintenance Association Endpoint Identifier
MFD	Mean Frame Delay
MFIB	Multicast Forwarding Information Base
MHD	Multi-Homed Device
MHF	MIP Half Function
MHN	Multi-Homed Network
MHV	Mirror Header Version
MI	Member Identifier
MIB	Management Information Base
MIMO	Multiple Input/Multiple Output
MIMP	MC-IPSec Mastership Protocol
MIP	Maintenance Domain Intermediate Point Maintenance Intermediate Points
MIR	Minimum Information Rate
MKA	MACSec Key Agreement
MLD	Multicast Listener Discovery
MLDP	Multicast Label Distribution Protocol
MLFR	Multi-Link Frame Relay
MLPPP	Multilink Point-to-Point Protocol
MME	Mobility Management Entity
MLT	Multi-Link Trunk
MMRP	Multiple MAC Registration Protocol
MNC	Mobile Network Code
MNO	Mobile Network Operator
MOP	Maintenance Operational Procedure
MOS	Mean Opinion Score
MP	Merge Point

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
	Multilink Protocol
MPBGP	Multi-Protocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MPLS-TP	Multiprotocol Label Switching - Transport Profile
MPLSCP	Multiprotocol Label Switching Control Protocol
MPTS	Multi-Program Transport Stream
MRAI	Minimum Route Advertisement Interval
MRIB	Multicast Routing Information Base
MRP	Multi-service Route Processor
MRRU	Maximum Received Reconstructed Unit
MRU	Maximum Receive Unit
MSAN	Multi-Service Access Node
MSAP	Managed Service Access Point
MSB	Most Significant Bit
MSCC	Multiple Services Credit Control
MSDP	Multicast Source Discovery Protocol
MSDU	MAC Service Data Unit
MSFP	Multicast Switch Fabric Plane
MSID	Mobile Station Identifier
MSIN	Mobile Subscriber Identification Number
MS-ISM	Multi-Service Integrated Services Module
MSK	Master Session Key
MS-PW	Multi-Segment Pseudowire
MSR	Mobile Service Router
MSS	Multi-Service Site Maximum Segment Size
MSTI	Multiple Spanning Tree Instances
MSTP	Multiple Spanning Tree Protocol

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
MSTV	Microsoft Television
MTBF	Mean Time Between Failures
MTSO	Mobile Telephony Switching Office
MTTR	Mean Time To Repair
MTU	Multi-Tenant Unit Maximum Transmission Unit
M-VPLS	Management Virtual Private Line Service
MVPN	Multicast VPN
MVR	Multicast VPLS Registration
MVRP	Multiple VLAN Registration Protocol

Table 21: N

Acronym	Definition
NAPT	Network Address and Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NBMA	Non-Broadcast Multiple Access network
NBNS	NetBios Name Server
NDF	Non-Designated Forwarder
NET	Network Entity Title
NETCONF	Network Configuration Protocol
NG-MVPN	Next-Generation Multicast VPN
NGE	Network Group Encryption
NH	Next-Hop
NHLFE	Next-Hop Label Forwarding Entry
NHOP	Next-Hop
NID	Network Interface Demarcation
NIST	National Institute of Standards and Technology

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
NLPID	Network Level Protocol Identifier
NLRI	Network Layer Reachability Information
NMS	Network Management System
NNI	Network-to-Network Interface
NPA	Network Processor Array
NPAT	Network and Port Address Translation
NRT-VBR	Non-Real-Time Variable Bit Rate
NSAP	Network Service Access Point
NSH	Next Signaling Hop
NSP	Network Services Platform
NSR	Nonstop Routing
NSSA	Not-So-Stubby Area
NTP	Network Time Protocol
NVE	Network Virtualization Edge

Table 22: O

Acronym	Definition
OAM	Operation, Administration and Management
OAMPDU	OAM Protocol Data Units
OC3	Optical Carrier level 3
OCD	Out-of-Cell Delineation
OCS	Online Charging Server
OCSP	Online Certificate Status Protocol
ODSA	On-Demand Subnet Allocation
OF	OpenFlow
OFS	OpenFlow Switch
OID	Object Identifier
OIF	Outgoing Interfaces

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
OIL	Outgoing Interface List
OLT	Optical Line Termination
OMCR	Oversubscribed Multi-Chassis Redundancy
ONT	Optical Network Terminal
OOB	Out-of-Band
OOP	Out-of-Profile
OPDL	Option Data structure List
OPS	On-Path Support
ORF	Outbound Route Filtering
ORR	Optimal Route Reflection
OS	Operating System
OSF	Oversubscription Factor
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSPF-TE	OSPF-Traffic Engineering (extensions)
OSS	Operations Support System
OTASP	Over the Air Services Provisioning (CDMA)
OTN	Optical Transport Network
OTU	Optical Transport Unit
OWAMP	One-Way Active Measurement Protocol
OXC	Optical Cross-connect

Table 23: P

Acronym	Definition
P2MP	Point-to-Multipoint
PAA	PDN Address Allocation
PADI	PPPoE Active Discovery Initiation

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-confirmation
PADT	PPPoE Active Discovery Terminate
PAE	Port Authentication Entities
PAGP	Port Aggregation Protocol
PAP	Password Authentication Protocol
PASTE	Provider Architecture for Differentiated Services and Traffic Engineering
PBB	Provider Backbone Bridging
PBF	Policy-Based Forwarding
PBO	Packet-Byte-Offset
PBR	Policy-Based Routing
PBT	Port-Based Timestamping
PCC	Path Computation Element Client
PCC	Policy and Charging Control
PCE	Path Computation Element
PCEF	Policy and Charging Enforcement Function
PCEP	Path Computation Element Protocol
PCM	Pulse Code Modulation
PCO	Protocol Configuration Options
PCP	Priority Code Point
PCR	Peak Cell Rate Proprietary Clock Recovery
PCRF	Policy and Rule Charging Function
PDN	Packet Data Network
PDP	Packet Data Protocol
PDU	Protocol Data Units

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
PDV	Packet Delay Variation
PE	Provider Edge Router
PFC	Protocol Field Compression
PFS	Perfect Forward Secrecy
PFSG	Pool Fate Sharing Group
PHB	Per-Hop Behavior
PHP	Penultimate Hop Popping
PHY	Physical layer
PIC	Prefix Independent Convergence
PID	Packet Identifier Protocol Identifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast – Sparse Mode
PIN	Personal Identification Number
PIP	Picture-in-Picture
PIR	Peak Information Rate
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PLR	Point of Local Repair
PMSI	P-Multicast Service Interface
PMSTP	Provider Multi-Instance Spanning Tree Protocol
PMT	Program Map Table
PN	Packet Number
POA	Program Off Air
POI	Purge Originator Identification
PON	Passive Optical Network
POP	Points of Presence

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
POS	Packet over SONET
PPID	Payload Protocol Identifier
PPP	Point-to-Point Protocol
PPPOE	Point-to-Point Protocol over Ethernet
PPS	Packets per Second
PPTP	Point-to-Point Tunneling Protocol
PRC	Path Restoration Combined Primary Reference Clock
PRF	Pseudorandom Function
PRI	Packet Priority
PSB	Path State Block
PSC	Protection Switching Coordination
PSCP	Programmable Subscriber Configuration Policy
PSD	Protection Switching Duration
PSI	Payload Structure Identifier
PSK	Pre-Shared Key
PSM	Peer State Machine
PSN	Packet-Switched Network
PSNP	Partial Sequence Number PDU
PTA	PMSI Tunnel Attribute PPP Termination Aggregation
PTB	Packet Too Big
P-TMSI	packet TMSI
PTP	Performance Transparency Protocol Precision Time Protocol
PUK	Personal Unblocking Code
PVC	Permanent Virtual Circuit
PVCC	Permanent Virtual Channel Connection

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
PVST	Per VLAN STP
PW	Pseudowire
PWE	Pseudowire Emulation
PWE3	Pseudowire Emulation Edge-to-Edge
PXC	Port Cross-Connect

Table 24: Q

Acronym	Definition
Q.922	ITU-T Q-series Specification 922
QCI	QoS Class Identifier
QL	Quality Level
QoS	Quality of Service
QPPB	QoS Policy Propagation via BGP
QSFP	Quad Small Form-factor Pluggable

Table 25: R

Acronym	Definition
RAA	Re-Authentication Answer
RADIUS	Remote Authentication Dial In User Service
RAI	Routing Area Identity
RAM	Reporting and Analysis Manager
RAN	Radio Access Network
R-APS	Ring Automatic Protection Switching
RAR	Re-Authentication Request
RC	Result Code
RCO	Routed Central Office
RD	Route Distinguisher
RDI	Remote Defect Indication

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
RDM	Russian Doll Model
RDNSS	Recursive DNS Server
RED	Random Early Discard
RESV	Reservation
RET	Retransmission
RFD	Route Flap Damping
RG	Routed Gateway
RGW	Residential Gateway
RIB	Routing Information Base
RIP	Routing Information Protocol
RNC	Radio Network Controller
RNCV	Ring Node Connectivity Verification
ROA	Route Origin Authorization
RP	Rendezvous Point
RPC	Remote Procedure Call
RPA	RP Address
RPF	Reverse Path Forwarding
RPL	Ring Protection Link
RPS	Radio Protection Switching
RR	Reporting Reason Route Reflector
RRC	Radio Resource Control Protocol
RRO	Record Route Object
RSA	Rivest, Shamir, and Adleman (authors of the RSA encryption algorithm)
RSB	Reservation State Block
RSC	Return Sub-Code
RSCP	Received Signal Code Power

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
RSHG	Residential Split Horizon Group
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RSU	Requested Service Unit
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
RT	Receive/Transmit
RT-VBR	Real-Time Variable Bit Rate
RTCP	RTP Control Protocol
RTM	Routing Table Manager
RTMP	Real-Time Messaging Protocol
RTMPE	Encrypted Real Time Messaging Protocol
RTMPT	Tunneled Real Time Messaging Protocol
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
RVPLS	Routed Virtual Private LAN Service

Table 26: S

Acronym	Definition
S2L	Source-to-leaf
S-A	Source-Active
SA	Security Association
SAA	Service Assurance Agent
SAC	State Advertisement Control
SAFI	Subsequent Address Family Identifier
SAI	Service Area Identity Secure Association Identifier
SAII	Source Access Individual Identifier

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
	Source Attachment Individual Identifier
SAK	Security Association Key
SAP	Service Access Point Subscriber Access Point
SASE	Stand Alone Synchronization Equipment
SAToP	Structure-Agnostic TDM over Packet
SBAU	Shared Buffer Average Utilization
SBR	Source-Based Reroute
SBU	Shared Buffer Utilization
SC	Security Channel
SCI	Secure Channel Identifier
SCP	Secure Copy
SCR	Sustained Cell Rate
SCTE	Society of Cable Telecommunications Engineers
SCUR	Session Charging with Unit Reservation
SD	Signal Degrade Space Diversity
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Network
SDP	Service Destination Point Service Distribution Point
SE	Shared Explicit
SecTAG	Security TAG
SecY	MAC Security Entity
SeGW	Secure Gateway
SeND	Secure Neighbor Discovery
SETS	Synchronous Timing Equipment Subsystem
SF	Signal Fail

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
SFF	Small Form Factor
SFM	Switch Fabric Module
SFP	Small Form-factor Pluggable (transceiver)
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SHCV	Subscriber Host Connectivity Verification
SHG	Split Horizon Group
SI	Strategic Industries
SID	Segment ID
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SIR	Sustained Information Rate
SL	Synthetic Loss Short Length
SLA	Service Level Agreement
SLAAC	Stateless Address Auto-Configuration
SLARP	Serial Line Address Resolution Protocol
SLIP	Serial Line Internet Protocol
SLM	Synthetic Loss Message
SLR	Synthetic Loss Reply
SMGR	Service Manager
SNAPT	Source Network Address and Port Translation
SNCP	Sub-Network Connection Protection
SNI	Server Name Indicator
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
SOAM	Service OAM
SONET	Synchronous Optical Network
SOO	Site of Origin
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC Mode
SPF	Shortest Path First
SPI	Security Parameter Index
S-PMSI	Selective Provider Multicast Service Interface
SPT	Shortest Path Tree
SR	Segment Routing Service Router (7750 SR)
SRGB	Segment Routing Global Block
SRLG	Shared Risk Link Group
SRRP	Subscriber Routed Redundancy Protocol
SR-MS	Segment Routing Mapping Server
SR-TE	Segment Routing Traffic Engineering
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Socket Layer
SSM	Source-Specific Multicast Synchronization Status Messages Synchronization Status Messaging
SSRC	Synchronization Source
SSU	System Synchronization Unit Synchronization Supply Unit
STA	Session-Termination-Answer
S-TAG	Service VLAN tag
STB	Set Top Box

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
STM1	Synchronous Transport Module, level 1
STP	Spanning Tree Protocol
STR	Session-Termination-Requests
SVC	Switched Virtual Circuit
SVID	Stacked VLAN ID
SYN	Synchronize

Table 27: T

Acronym	Definition
TAC	Technical Assistance Center
TACACS+	Terminal Access Controller Access-Control System Plus
TAF	Time Average Factor
TAII	Target Attachment Individual Identifier
TC	Traffic Class (formerly known as EXP bits)
TCA	Threshold Crossing Alert Traffic Crossing Alert
TCI	TAG Control Information
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TCSB	Traffic Control State Block
TDF	Traffic Detection Function
TDM	Time Division Multiplexing
TDP-ID	Time Descriptor Policy Identifier
TE	Traffic Engineering
TED	Traffic Engineering Database
TEID	Tunnel Endpoint Identifier
TFN	Tribe Flood Network
TFTP	Trivial File Transfer Protocol

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
TLDP	Targeted LDP
TLS	Transport Layer Security
TLV	Type Length Value
TM	Traffic Management
TMSI	Temporary Mobile Subscriber Identity
TNC	Technically Non-Conformant
TNS	Transparent Network Substrate
ToD	Time of Day
TOS	Type-of-Service
T-PE	Terminating Provider Edge router
TPID	Tag Protocol Identifier
TPMR	Two-Port MAC Relay
TPSDA	Triple Play Service Delivery Architecture
TS	Transport Stream
TSH	TTL Security Hack
TTI	Trail Trace Identifier
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TTM	Tunnel Table Manager
TWAMP	Two-Way Active Measurement Protocol

Table 28: U

Acronym	Definition
U-APS	Unidirectional Automatic Protection Switching
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card — SIM card

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
ULD	Uni-directional Link Detection
UMTS	Universal Mobile Telecommunications System (3G)
UNI	User-to-Network Interface
UPnP	Universal Plug and Play
uRPF	Unicast Reverse Path Forwarding
USIM	Universal Subscriber Identity Module — application
USM	User-based Security Model
USU	Used Service Unit
UTC	Coordinated Universal Time

Table 29: V

Acronym	Definition
VACM	View-based Access Control Model
VAS	Value Added Service
VBO	VE Block Offset
VBS	VE Block Size
VC	Virtual Circuit
VCC	Virtual Channel Connection
VCCV	Virtual Circuit Connectivity Verification
VCI	Virtual Circuit Identifier
VCP	Virtual Core Port
VE	VPLS Edge
VE-ID	VPWS Edge Identifier
V-GW	Visited WLAN-GW
VID	VLAN ID
VLAN	Virtual LAN
VLL	Virtual Leased Line
vMEPs	Virtual MEPS

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
VNI	VXLAN Network Identifier
VoD	Video on Demand
VoIP	Voice over IP
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VPWS	Virtual Private Wire Service
VQM	Video Quality Monitoring
VRF	Virtual Routing and Forwarding table
vRGW	Virtual Residential Gateway
VRID	Virtual Router ID
VRP	Validated ROA Payload
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor Specific Attribute
VSC	Virtual Services Controller
VSD	Virtual Services Directory
VSI-ID	Virtual Switch Instance identifier
VSM	Vendor-Specific Message Versatile Service Module
VSO	Vendor-Specific Option
VSP	Virtual Services Platform
VT	Validity Time Virtual Trunk
VTEP	VxLAN Tunnel Endpoint
VTP	Virtual Trunk Protocol

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Acronym	Definition
VxLAN	Virtual eXtensible Local Area Network

Table 30: W

Acronym	Definition
WAC	WiiMAX Access Controller
WAN	Wide Area Network
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
WLAN-GW	WLAN Gateway
WPP	Web Authentication Protocol Wireless Portal Protocol
WRED	Weighted Random Early Detection Weighted Random Early Discard
WRR	Weighted-Round-Robin

Table 31: X

Acronym	Definition
XML	Extensible Markup Language
X.21	ITU-T X-series Recommendation 21
XMPP	eXtensible Messaging and Presence Protocol

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

16 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.

© 2026 Nokia.

Use subject to Terms available at: www.nokia.com/terms.

Customer document and product support

Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback