Nokia 7705 Service Aggregation Router-1

Release 26

The Nokia 7705 Service Aggregation Router (SAR)-1 delivers versatile services and applications in a compact, fixed platform. These routers provide IP/MPLS/ Ethernet demarcation and branch office connectivity, ensuring seamless and efficient network operations.

Overview

The 7705 SAR-1 is designed to deliver best-in-class capabilities, with a fully programmable datapath providing enhanced features today and flexibility to evolve with changing requirements. The 7705 SAR-1 uses the Nokia Service Router Operating System (SR OS), which is built to power the most demanding and dynamic Ethernet and IP/MPLS networks. Furthermore, comprehensive built-in security features enable network operators to safeguard against cybersecurity threats, ensuring the protection of sensitive data.

Versatile capabilities

The 7705 SAR-1 is built with a fully-programmable data-path, which allows it to deliver on feature requirements today and to accommodate new services and standards as they evolve over time. This allows network operators to protect their investment by integrating new capabilities as they emerge and to stay ahead of the innovation curve. Industry proven IP/MPLS service functions, security and reliability are delivered by the SR OS, the operating system of the 7705 SAR-1.

The 7705 SAR-1 inherits the software reliability and evolution of the SR OS, reflecting the move towards automation, programmability, and agility for scalable and secure network connectivity.

7705 SAR-1

Compact and power saving

All interfaces and power supply inputs on the Nokia 7705 SAR-1 are accessible from the front. Featuring a front-to-back airflow design in a rack mountable 1RU, 7.4 inch (18.9 cm) depth provides a compact footprint for easy and efficient deployment. Additionally, the systems offer significantly lower power consumption compared to equivalent competing solutions, while providing redundant power inputs for enhanced reliability.

Granular services offering

It is critical to maintain end-to-end Quality of Service (QoS) for different types of traffic, as not all traffic shares the same set of requirements. Hierarchical QoS, traffic classification, traffic management policies, and QoS statistics and monitoring are among the capabilities of the 7705 SAR-1. These features make it an excellent choice for multi-tenant applications and service providers seeking to deliver high-performance, SLA-compliant services while optimizing network resource utilization.

Network security

The Nokia 7705 SAR-1 offers a multi-faceted approach to security. It ensures traffic encryption through various methods, including IPsec, NGE and MACsec[1]. Its NAT capabilities enhance security by obfuscating internal addresses and providing firewall-like functionality. Additionally, it incorporates Trusted Platform Module (TPM) 2.0 technology, along with support for secure boot and measured boot, to strengthen system integrity.

Automation

The 7705 SAR-1 simplifies and automates network operations by leveraging model-driven network management capabilities through the Nokia SR OS. It is managed by the Nokia Network Services Platform (NSP), which provides an extensive suite of service management features to automate end-to-end service provisioning, operations, administration, and maintenance. Additionally, the system offers Zero touch provisioning (ZTP) solutions that enables automatic node configuration. These features enhance the end-user experience while reducing operating costs.

The model-driven management capabilities of SR OS enable configuration and state management using a YANG-based CLI, the NETCONF protocol, and gRPC/gNMI interfaces. They also support real-time streaming telemetry through gRPC and gNMI subscriptions, ensuring seamless operations via YANG-based CLI and NETCONF protocols.

Hardware features

The 7705 SAR family of products is available in a range of models to suit a broad range of mission-critical, enterprise, communication service providers applications. Please visit the 7705 SAR web page to learn more about the different variants available.

1 Future software deliverable

Technical specifications

Table 1. Nokia 7705 SAR-1 platform specifications

Feature	7705 SAR-1
System throughput: Full duplex (FD)	Up to 50 Gb/s
Ports	• 10 x 10G SFP+/SFP, including 4 x MACsec-capable 10G ports[2]. • 6 x 1G SFP
Control interfaces	Console, management, USB
Indicators	• Management, power supply status LEDs • Per port link and activity status LEDs • System (Stat), fan status LED
Hardware redundancy	Power inputs, cooling fans
Dimensions	• Height: 4.3 cm (1.7 in); 1 RU • Width: 44.45 cm (17.5 in) • Depth: 18.9 cm (7.4 in) • Fits in standard 19-in rack
Power	• AC input (rated): 100 V to 240 V • DC input (rated): -48 V to -60 V
Cooling	• Internal non-replaceable fans • Front-to-back airflow
Normal operating temperature range	0°C to +40°C (up to 1800m) (32°F to +104°F) sustained
Shipping and storage temperature range	-40°C to +70°C (-40°F to +158°F)
Normal humidity	5% to 95%, non-condensing

Software features

The 7705 SAR-1 supports, but is not limited to, the following SR OS software features.

L1/L2 networking

- Ethernet ports: access, network, hybrid
- Link aggregation groups (LAG)
- Link Aggregation Control Protocol (LACP)
- Multi chassis LAG (MC-LAG)
- Encapsulation on ports and LAGs: null, 802.1Q VLANs (dot1q), Q in Q (802.1ad)
- Configurable media access control (MAC) addresses
- Configurable MTU and jumbo frame support
- Interface statistics at multiple levels: ports, LAGs, router/MPLS interfaces, SAPs, services
- Network interfaces
- Spoke Service Distribution Point (SDP) tunnels
- IEEE 802.1x EAP

IPv4 and IPv6 routing protocols

- IPv4 and IPv6 forwarding
- Static routes
- Open Shortest Path First (OSPF) v2, v3
- Intermediate System to Intermediate System (IS IS)
- Routing Information Protocol (RIP) and Routing Information Protocol next generation (RIPng)
- Border Gateway Protocol v4 (BGP4) and Multiprotocol BGP (MP BGP)

2 MACsec is roadmap feature

- Address Resolution Protocol (ARP), IPv6 Neighbor Discovery (ND)
- Internet Control Message Protocol (ICMP), v6
- Equal cost multipath (ECMP)
- Virtual Router Redundancy Protocol (VRRP)

IPv4 and IPv6 multicast protocols

- Base router and Virtual Private Routed Network (VPRN) support for:
  - Internet Group Management Protocol (IGMP) v1, v2, v3
  - Multicast Listener Discovery (MLD) v1, v2
  - Protocol Independent Multicast (PIM) v4/v6
  - Multicast Source Discovery Protocol (MSDP)
- Multicast aware VPLS with IGMP snooping, MLD snooping, and PIM snooping to constrain Layer 2 multicast flooding

MPLS and segment routing

- Label Distribution Protocol (LDP) for IPv4 FECs
- Point to point RSVP label switched paths (LSPs)
- LDP over RSVP
- BGP labelunicast IPv4 (RFC 3107) unicast IPv4 (RFC 3107)
- OSPFv2/IS IS shortcuts to IPv4 prefixes (using LDP or RSVP)
- BGP shortcuts to IPv4 prefixes (using LDP, RSVP or BGP 3107)
- OSPFv2 segment routing extensions
- IS IS segment routing extensions
- Segment Routing – Traffic Engineering (SR TE)
- BGP segment routing policies

Layer 2 VPNs

- E pipe:
  - Ethernet virtual leased line (VLL) signaled by T LDP using MPLS or GRE transport
  - Ethernet VLL signaled by BGP using MPLS or auto bind GRE SDP transport
  - Ethernet VLL signaled by BGP EVPN using MPLS
- Virtual Private LAN Service (VPLS):
  - Ethernet VPLS signaled by T LDP using MPLS or GRE transport
  - Ethernet VPLS signaled by BGP using MPLS or auto bind GRE transport
  - Ethernet VPLS signaled by BGP EVPN (Ethernet VPN) using MPLS
- Routed VPLS (R VPLS)
- Resiliency:
  - Pseudowire redundancy
  - Dual homed virtual private wire service (VPWS)/VLL
  - BGP multihoming for VPLS
  - MC-LAG (with L2 Services)
  - Spanning Tree Protocol (STP), Rapid STP (RSTP) and Multiple STP (MSTP)
- Dot1q and QinQ VLAN manipulation/translation in L2 services
- Layer 2 Control Protocols tunneling

Layer 3 services

- Internet Enhanced Services (IES)
- IPv6 PE router (6PE)
- MPLS and GRE auto bind and spoke SDPs
- RFC 4364 IPv4 VPNs using MPLS or GRE transport
- RFC 4659 IPv6 VPNs using MPLS or GRE transport
- IP VPN inter AS option B
- GRE IP tunnelling
- Global Routing Table (GRT) lookup and VPRN to GRT route leaking

Filtering and control plane protection

- Ingress and egress IPv4 and IPv6 filters
- Wide range of match criteria including: src/dst port/IP, tcp flags
- Standard actions: forward and drop
- Conditional actions:
  - Drop extracted traffic (for control plane protection)
  - Drop based on packet length
  - Drop based on time to live (TTL)
- Ingress policy based routing (PBR) actions:
  - Forward to next hop
  - Forward to router (another routing instance)
  - redirect policy
- Advanced forward processing actions:
  - NAT action
  - TCP MSS adjust action
- Filter logging (ingress and egress)
- Distributed CPU protection (static policers)

OAM

- IEEE 802.1ag / ITU T Y.1731 ETH CFM:
  - Down/Up MEPs
  - Continuity Check Messages (ETH-CC)
  - Linktrace (ETH-LT)
  - Loopback (ETH-LB)
  - Delay Measurement (ETH-DM)
  - Link Loss Forwarding (ETH-LLF)
- Ethernet Synthetic Loss Measurement (ETH-SLM)
- Ethernet Performance Monitoring and Fault Management
- G.8013/Y.1731 Ethernet Bandwidth Notification (ETH-BN) with egress-rate adjust
- IEEE 802.3ah EFM-OAM
- SAA for ETH-CFM loopback and linktrace
- Bidirectional Forwarding Detection (BFD) single hop, multi hop
- LLDP
- TWAMP/STAMP reflector
- TWAMP-light/STAMP sender and reflector
- TWAMP server
- OAM tools: lsp-ping/trace, sdp-ping/sdp-mtu, sdp-keepalive ping/trace, ping/ mtu keepalive
- ETH-CFM integration with MC-LAG
- LSP-BFD for RSVP-TE and SR-TE LSPs

Model driven management

- Configuration via model driven interfaces:
  - NETCONF
  - MD CLI
  - gRPC/gNMI
- State information retrieval via model driven interfaces:
  - NETCONF
  - MD CLI
  - gRPC/gNMI
- Streaming telemetry through gRPC/gNMI subscriptions; operations via NETCONF and gNOI using YANG models

Quality of Service

- Ingress classification to forwarding class based on 802.1p, DSCP, MPLS EXP or IPv4/IPv6 filter rules
- Egress re classification
- Ingress and egress unicast policing and hierarchical policing
- Egress marking of 802.1p, DSCP or MPLS EXP
- Egress queue shaping based on configurable Peak Information Rate (PIR) and Maximum Burst Size (MBS)
- LAG degradation aware IGP cost and operational state control

Security

- Network Address Translation (NAT)
- IP Security (IPsec)
- Internet Key Exchange (IKEv1 and IKEv2), including support for post quantum PPK as per RFC 8784
- Network Group Encryption (NGE) for:
  - MPLS SDPs (VPLS, VPRN, IES, VPWS)
  - VPRN unicast and multicast (NG mVPN)
  - Router interfaces (IPv4 only) for user plane and control plane encryption
  - PW templates
- Public Key Infrastructure (PKI) supporting X.509v3 certificates
- IPv4 and IPv6 filters using access control lists (ACLs)
- Management access control filters
- User profile management, strict login controls and scope of command/control
- Remote Authentication Dial In User Service (RADIUS) client
- Terminal Access Controller Access Control System Plus (TACACS+)
- Simple Network Management Protocol (SNMP) v3
- Secure Shell v2 (SSHv2)
- Transport layer security (TLS)

Standard compliance[3]

Environmental

- ETSI EN 300 019-2-1; Storage Tests, Class 1.2
- ETSI EN 300 019-2-2; Transportation Tests, Class 2.3
- ETSI EN 300 019-2-3; Operational Tests, Class 3.2
- ETSI EN 300 753; Acoustic Noise, Class 3.2
- GR-3160-CORE

Safety

- AS/NZS 62368.1
- IEC 60529 IP20
- IEC/EN 60825-1
- IEC/EN 60825-2
- IEC/EN/UL/CSA 62368-1

Electromagnetic compatibility

- AS/NZS CISPR 32 (Class A)
- BSMI CNS 15936 (Class A)
- BT GS-7
- EN 300 386
- EN 55032 (Class A)
- EN 55035
- ETSI EN 300 132-1 (AC)
- ETSI EN 300 132-2 (LVDC)
- ETSI ES 201 468
- FCC Part 15 (Class A)
- ICES-003 (Class A)
- IEC 61000-3-2
- IEC 61000-3-3
- IEC 61000-6-2
- IEC 61000-6-4
- IEC CISPR 32 (Class A)
- IEC CISPR 35
- IEC/EN 61000-4-2 ESD
- IEC/EN 61000-4-3 Radiated Immunity
- IEC/EN 61000-4-4 EFT
- IEC/EN 61000-4-5 Surge
- IEC/EN 61000-4-6 Conducted Immunity
- IEC/EN 61000-4-11 Voltage Interruptions
- KS C 9832
- KS C 9835
- VCCI (Class A)

3 System design intent is according to the listed standards. Refer to product documentation for detailed compliance status.

Directives and regional approvals

- Directive 2011/65/EU RoHS (including Commission Delegated Directive EU 215/863)
- Directive 2012/19/EU WEEE
- Directive 2014/30/EU EMC
- Directive 2014/35/EU LVD
- BSMI Mark: Taiwan
- CE Mark: Europe
- CRoHS: China RoHS
- KC Mark: South Korea
- RCM Mark: Australia
- VCCI Mark: Japan
- UKCA: United Kingdom

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 214663 (April)