Nokia 7750 Service Router and 7450 Ethernet Service Switch

Integrated Service Adapters

Nokia Integrated Service Adapters (ISAs) extend the level of networking functionality and generalized processing capability for IP/MPLS routing applications for integrated services on the Nokia 7750 Service Router (SR) and the Nokia 7450 Ethernet Service Switch (ESS).

Nokia ISAs are powerful resource platforms that provide specialized packet processing and buffering for deeper levels of integrated services and application functionality in the Nokia Service Router Operating System (SR OS) with improved scalability, without the need for external dedicated appliances.

ISAs are available in two hardware variants. Integrated services enabled by the ISA are available to all ports across the chassis. Traffic flows are directed to the ISA through the router backplane and fabric.

Integrated services use case support includes:

- Application Assurance (AA)
- Layer 7 Stateful Firewall
- Layer 2 Tunneling Protocol (L2TP) Network Server (LNS)
- Carrier Grade - Network Address Translation (CG-NAT)
- IP security (IPsec)
- IP tunneling
- IPv4 reassembly
- Wireless LAN Gateway (WLGW)
- Virtualized residential gateway (vRGW)
- Advanced video functionality.

MS-ISM

MS-ISA2

Features

- Provides multicore processing on carrier-grade hardware, operating within an industry-leading, highly available and proven chassis
- The Nokia Multiservice Integrated Service Adapter 2 (MS-ISA2) is a general-purpose multicore processor based on the Nokia FP3 network processing (NP) silicon. It delivers up to 40 Gb/s of integrated service and application processing in a hot-swappable, half-slot form factor that inserts into an Input/Output Module 4-e (IOM4-e) and IOM-e.
- The FP3-based Nokia Multiservice Integrated Service Module (MS-ISM) contains two embedded ISA2 general-purpose multicore processors. It delivers up to 80 Gb/s of integrated service and application processing throughput in a hot-swappable, full-slot form factor.

Benefits

- Seamless integration into an existing Nokia 7750 SR or 7450 ESS chassis that fully interoperates with all existing interfaces, thereby reducing dedicated external appliances with associated space and cabling while reducing power consumption, topology churn and network latency
- A single ISA is equivalent to multiple external appliances. This offers significant scalability and resiliency advantages, simplified network topology, common management of the platform, and operational savings from reduced network elements, power consumption and operating systems to manage. It also reduces CAPEX through the elimination of external appliances and more efficient sparing.
- Consistent management of the ISA services using the Nokia Network Services Platform (NSP) Network Functions Manager for Packet (NFM-P) module eliminates the need to train and staff a team to maintain a large set of external servers, thereby significantly reducing OPEX

Application Assurance

Application Assurance (AA) functionality on the Nokia ISA extends the service depth and application capabilities of the Nokia 7750 SR and 7450 ESS by enabling Layer 3 to Layer 7 (L3–L7) visibility and intelligent control of IP applications, with extensive per-application, per-subscriber or per-VPN service policies, and providing application reporting and traffic management capabilities.

AA enables service providers to monetize applications by offering enhanced and personalized services with per-application charging and control capabilities. AA features include optional Layer 7 Stateful Firewall capabilities.

With AA, target traffic for AA processing is diverted to the ISA based on an application profile assigned to the subscriber or service. The application profile also contains match and action criteria parameters that are used by the Application QoS Policy (AQP) rules to determine the QoS treatment applied. This functionality enables any combination of passive monitoring and reporting, active bandwidth and/or flow policing, and flow-based QoS re-marking to provide per application services.

Feature highlights

Application identification

- Real-time, per-flow stateful packet inspection on OSI Layers 3 to 7, to dynamically identify and intelligently meter traffic flows, applications and underlying protocols
- Unique identification of all enterprise, mobile, and residential applications using IP address and ports, Uniform Resource Identifier (URI) strings, Differentiated Services Code Point (DSCP) values or traffic direction in addition to protocol signatures to detect end-to-end application and flow performance behavior
- Full support for IPv4 and IPv6 traffic and applications
- Application detection is highly flexible and release-independent, allowing in-service configuration of new application types. It is enabled by in-service upgrade of protocol signatures as well as fully programmable application and application group definitions.
- Accurate traffic identification by avoiding or eliminating asymmetric traffic flows. When AA is deployed at the IP edge router, this is a single processing point for all flows for each site/subscriber, so there is no need to eliminate traffic asymmetry. When AA is deployed on a transit router behind the IP edge/Broadband Network Gateway (BNG), asymmetry is automatically removed by the AA solution, ensuring accurate identification and control.
- Flow attribute classification (e.g., video, audio, download, available bit rate (ABR), encrypted Server Name Indication (eSNI)) using deterministic and heuristic machine-learning algorithms. Flow attributes are complementary to application classification and can be used in conjunction with confidence-level thresholds for charging, control and analytics use cases.

Application control policies

- Extensive per-application policy enforcement and charging with granular bandwidth shaping, policing and prioritization, defined per subscriber or per VPN site, to intelligently categorize application traffic based on policy
- Delivery of deterministic end-to-end application behavior through application performance optimization and application-based QoS policies
- URL filtering using local lists imported in-service; used for blacklist internet filtering
- HTTP and HTTPs redirect with application-aware context for selective redirect use cases, including HTTP white-listing for non-authenticated WLGW subscribers
- Transmission Control Protocol (TCP) maximum segment size (MSS) adjusted to prevent packet fragmentation
- TCP Optimization for Wireless LAN Gateway DSM subscribers
- Real-time detection, control and reporting of access network congestion using Dynamic Experience Management; this provides control of the user experience by application even during resource congestion.

Application reporting

- Per-protocol, per-application, and per-application group volume statistics accounting for all subscribers, as well as L2 and -3 VPNs (every byte, every packet, every flow for every application counted)
- End-to-end application volume statistics available between subscribers, VPN sites and servers
- Performance reporting for TCP-based applications (including client and server side), network delay/loss/jitter, session establishment/closure delay/ jitter, and client-server transaction delay/jitter
- XML record export for volume accounting
- cflowd v10 record export for application volume and performance measurements
- RADIUS accounting export of application-based charging groups for application-aware, usage-based billing plans
- Reporting on application use by device types and reporting of top web domains visited
- Reporting of flow attributes for all traffic (e.g., video, audio, download, ABR, etc.), including encrypted applications

Benefits

- Provider Edge (PE) integration for residential subscribers or enterprise services as well as AA on spoke service distribution points (SDPs) allows optimal distribution for personalized, on-demand service deployments, with consistent operational provisioning and subscriber policy management through a common unified service management platform.
- Transit subscriber integration in edge or aggregation routers for residential and enterprise services allows AA deployments for topologies requiring multiple subscriber policy enforcement points under common provisioning and subscriber policy management.
- Value-added services for residential and Wi-Fi® consumers and content partners by leveraging AA to enable a premium quality of experience (QoE) for internet video, audio, voice, gaming and other value-added content
- Comprehensive application recognition and assurance for WAN Application-Assured VPN services, including internet access, Virtual Private Routed Network (VPRN), Virtual Private LAN Service (VPLS) and ePipe services, to address enterprise requirements
- Pay-as-you-grow service rollout, which scales to any number of active ISAs as required per chassis, with flexible redundancy options
- No impact on network topology when adding AA services to residential, Wi-Fi or enterprise networks
- No risk to service availability by insertion of new links or appliances; the fail-to-fabric bypass ensures services remain up even if the needed ISA is not available

Layer 7 Stateful Firewall

Layer 7 Stateful Firewall functionality on the Nokia ISA uses AA application-level analysis, enabling the 7750 SR to provide an in-line integrated stateful firewall that protects mobile packet core infrastructure from malicious security attacks by blocking unsolicited traffic. Using the AA stateful packet filtering feature combined with AA L7 classifications and control empowers operators with advanced, next-generation firewall functionality.

In stateful inspection, the firewall inspects packets at L3–7 and also monitors the connection's state. If the operator configures a "deny" action in a session filter, the matching packets (matching both the AQP and associated session filter match conditions) are dropped and no flow session state/context is created.

Feature highlights

- Full application-level gateway support for all AA signaling protocols, including Session Initiation Protocol (SIP), File Transfer Protocol (FTP) and Real Time Streaming Protocol (RTSP)
- Automatic detection of Domain Name Server (DNS) tunneling
- Next-generation firewall protection that includes detection and control of flows based on L7 application types; this allows the operator to configure L7 rules such as rate limiting peer-to-peer traffic or blocking certain HTTP(s) domains.
- Syslog events and threshold crossing alerts (TCAs) as well as complete set of related firewall statistics; complete graphics-based reporting of these statistics is provided by the Nokia Network Services Platform (NSP)
- Denial of Service (DoS) protection to detect malformed packets, fragmented packets attacks and volumetric attacks
- Stateful detection of TCP misbehavior
- IPv4, IPv6, GTPv1 and GTPv2 traffic

The Layer 7 Stateful Firewall supports features needed to provide mobile network protection on S1-U, S1-MME MME (Mobility Management Entity), IuPS and roaming interface protection on S8 and Gn interfaces:

- GTP validation: Checks for anomaly attacks that involve malformed, corrupt or spoofed traffic through:
  - Header length checks
  - Information Element (IE) length validation
  - Invalid reserved field validation
  - Reserved Information Elements validation
  - Missing mandatory information
  - Elements validation
  - Sequence number validation
- Gateway GPRS Support Node/Packet Data Network Gateway (GGSN/PGW) and Serving GPRS Support Node/Serving Gateway (SGSN/SGW) redirection protection
- Handover control to prevent session hijacking
- Source address for user equipment (UE) spoofing protection
- Protection against unauthorized Public Land Mobile Network and/or Access Point Name (APN) access via APN/IMSI (International Mobile Subscriber Identity) filtering
- Protection against unsupported GTP messages types
- Protection against GTP-in-GTP traffic attacks
- Stream Control Transmission Protocol (SCTP) inspection and filtering.

Benefits

- Nokia SR OS integrated firewall dramatically reduces cost compared to dedicate firewall appliances
- Software licensed features allow tailoring of features and scale to support needed use cases
- Fully coupled to Security Gateway IPsec tunnel services for S1-U, S1-MME and IuPS protection
- Offered as a component of Nokia mobile packet core solutions

LNS

L2TP Network Server (LNS) functionality on the Nokia ISA allows network operators to offer the same industry-leading Enhanced Subscriber Management (ESM) functionality to subscribers terminated on L2TP sessions that are already available on the 7750 SR. They include IP over Ethernet (IPoE), Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol over Ethernet (PPPoE), and Point-to-Point Protocol over ATM (PPPoA) subscribers. By integrating an LNS into the 7750 SR, a single platform can support PPP-based customers and provide an evolution toward IPoE (DHCP) while delivering a consistent user experience.

One application of LNS is the ability to introduce IPv6 services over an existing Broadband Remote Access Server (BRAS), where IPv6 subscriber traffic is carried transparently in an L2TP tunnel and over IPv4 without any IPv6 support in the L2TP Access Concentrator (LAC). LNS supports the Nokia SR OS IPv4 and IPv6 ESM features, so IPv4, IPv6 and dual-stack IPv4 and IPv6 subscribers are supported concurrently.

Feature highlights

- Retains all ESM features for IPv4 and IPv6
- Concurrent support for NAT and Dual-Stack Lite (DS-Lite) Softwire Concentrator on the same ISA

Benefits

- Features, management and accounting for LNS subscribers are consistent with ESM services on existing IPoE (DHCP), PPP, PPPoE and PPPoA subscriber access methods
- Allows the introduction of IPv6 services over an IPv4 access network and LAC

CG-NAT

Carrier Grade NAT (CG-NAT) functionality on the Nokia ISA allows network operators to conserve IPv4 addresses and maintain IPv4 internet access while migrating to IPv6. In addition, CG-NAT allows for the forwarding of traffic between VPN services with overlapping address spaces; for example, where a branch office VPN service needs to be merged into a larger corporate VPN service.

CG-NAT offers high scalability and high rate transactions that are suitable to centralized deployments. CG-NAT offers several redundancy models:

- Inter-chassis stateful redundancy model where flows are synchronized between the chassis. Flow synchronization is performed per NAT group (active/standby NAT group). Up to four NAT-groups, each with its own sets of ISAs, can be deployed to achieve traffic distribution between the chassis.
- Active/standby inter-chassis stateless redundancy model where one of the chassis in a pair is in a standby mode
- Active/standby intra-chassis stateless redundancy model where one of the service cards in the chassis is in a standby mode waiting to protect another failed service card in the same chassis
- Active/active intra-chassis stateless redundancy model where all service cards in the chassis are ready to accept a portion of the load from any one failed card in the same chassis.

Feature highlights

- Four types of translation:
  - **NAT44** performs source IPv4 address and source port translation. IPoE/PPPoE subscriber awareness from the BNG can be optionally added to NAT44. With subscriber awareness, NAT44 notifies the operator via RADIUS logging about the IP and port-block mappings that it performs and also about the BNG subscriber identity that owns the mapping. Subscriber awareness does not require BNG and NAT44 to be collocated on the same node.
  - **L2-Aware NAT** offers tight integration between BNG subscribers and NAT44. BNG and NAT44 functionality are collocated on the same Nokia SR OS node. The address/port translation is performed based on the subscriber ID as defined in the BNG; this allows multiple subscribers to share the same IPv4 address.

- **DS-Lite** is an IPv6 transition technique that allows the tunneling of IPv4 traffic across an IPv6-only network. Dual-stack IPv6 transition strategies allow network operators to offer IPv4 and IPv6 services and save on OPEX by allowing the use of a single IPv6 access network instead of running concurrent IPv6 and IPv4 access networks. DS-Lite has two components: the client in the customer network, known as the Basic Bridging BroadBand element (B4), and Address Family Transition Router (AFTR) deployed in the service provider network.

  The Nokia SR OS provides the AFTR functionality, which encompasses translation based on the combination of the IPv6 address of the customer premises equipment and the encapsulated IPv4 address within the IPv6 tunnel.
- **NAT64** allows IPv6-only hosts to communicate with IPv4 hosts. NAT64 technique relies on stateful translation between IPv6 and IPv4 packets.

- Several modes of logging:
  - Port-block-based and flow-based syslog
  - Port-block-based RADIUS
  - Flow-based IPFIX and query-based in deterministic NAT.
- In deterministic NAT, mappings are performed in a predefined way that can be predictably reversed via a query or a Python script; this eliminates the need to deploy complex logging infrastructure such as logging servers or storage for logs.

Benefits

- Mitigates network operator IPv4 address exhaustion
- Allows IPv4 service to continue and evolve during the migration to IPv6 services
- L2-Aware NAT removes the requirement for unique private IP address per subscriber.
- DS-Lite allows IPv4 and IPv6 services to run across a single IPv6-only infrastructure.

IPsec

IPsec functionality on the ISA provides comprehensive, highly scalable and network-integrated L3 IPsec VPN connectivity as a Remote Access Concentrator or for site-to-site or network-to-network encrypted IPsec security. IPsec can also be used in mobile networks as a highly scalable 3GPP Security Gateway.

Any physical interface can operate as an encrypted IPsec VPN port, enabling support for a diverse range of network traffic types, interfaces and topologies. In addition, IPsec can be combined with the Nokia 7750 SR comprehensive range of IP/MPLS service offerings. Hardware-based crypto processing provides up to 40 Gb/s IPsec throughput per MS-ISA2.

Feature highlights

- Internet Key Exchange (IKE) v1/v2
- Quantum safe: RFC8784
- Load sharing across multiple ISAs with a single gateway address
- Up to 500,000 IKEv2 remote-access tunnels per system
- Static/dynamic LAN-to-LAN tunnel
- Remote-access tunnel support with address assignment options for remote-access tunnel:
  - IKEv1-RADIUS
  - IKEv2-RADIUS/Local Pool/External DHCPv4/v6 server
- Stateful inter-chassis redundancy (IKEv2 only)
- Authentication methods:
  - IKEv1: Pre-Shared Key (PSK)/Extended Authentication (XAUTH)
  - IKEv2: PSK/Certificate/ Extensible Authentication Protocol (EAP)
- RADIUS-based AAA for IKEv2 remote-access tunnel
- Support for Online Certificate Status Protocol (OCSP)

- Support for Certificate Revocation List (CRL)
- Certificate Management Protocol version 2
- Enrollment Over Secure Transport Protocol
- N:M stateful inter-chassis redundancy
- High-performance, hardware-based encryption and decryption
- Tunnel-mode Encapsulating Security Payload (ESP) with authentication support
- Transport mode for GRE tunnel
- Comprehensive IPv6 support as transport or payload
- IKEv2 Traffic Selector support for address range, protocol and port range
- IPsec Client Database (IKEv2 Dynamic LAN-to-LAN tunnel only)
- TCP MSS Adjust for IPsec tunnel

Benefits

- Integrated IPsec allows combining of connectivity services, greater service scale and resiliency, and reduced network latency.
- Full integration with the Nokia SR OS provides unified service management, encryption and security, available to any L3 service on any physical port.
- The hardware-based security gateway provides industry-leading throughput.
- The carrier-grade platform with comprehensive failure protection mechanisms provides highly available IPsec-based services.
- Quantum safe IPsec implements RFC 8784 which mixes high entropy pre-shared key during IKEv2 key derivation process.

IP tunneling

IP tunneling functionality on the ISA enables IPv4 and IPv6 payload packets to be tunneled to remote devices using generic routing encapsulation (GRE), L2TPv3 or IP-in-IP encapsulation. The ISA implementation models each tunnel as an IP interface, allowing capabilities such as filters/access control lists, QoS policies and IP routing protocols to control the flow of traffic into and out of each tunnel. IP tunneling allows a remote customer edge device to be logically connected to an L3 PE over a routed IP network that lacks visibility of the customer routes.

Feature highlights

- Tunnel interface as an IP numbered interface associated with a VPRN or Internet Enhanced Service service access point (IES SAP)
- IPv4 and IPv6 payload support
- Support for IP routing protocols, including static, OSPFv2/v3 and BGP
- Support for bidirectional forwarding detection (BFD) bootstrapped by the routing protocol
- GRE over IPv4 or IPv6 transport
- IP-in-IP encapsulation over IPv4 or IPv6 transport
- Backup tunnel destination if there is no route to the primary tunnel destination
- Ability to use a different routing instance for transport of the encapsulated packets
- Support for IPv4 reassembly
- IPv4 payload fragmentation according to configurable maximum termination unit (MTU) and support for clearing IPv4 DF flag
- Multi-active ISA support
- GRE tunnel could be protected by applying IPsec transport mode encryption

Benefits

- Increased deployment flexibility by allowing logical tunnel interconnections
- Fully integrated with the Nokia SR OS for unified service management, available to any L3 service on any physical port
- A carrier-grade platform with comprehensive failure protection mechanisms provides highly available IP tunneling capabilities

IPv4 reassembly and TCP MSS adjustment

IPv4 reassembly functionality on the ISA provides support for reassembling received IPv4 packets that are fragmented. The reassembled packets then go through normal IP processing. IP fragmentation is performed by systems when the packet size exceeds the MTU size of the outgoing interface, and the DF bit is not set. Fragmentation can commonly occur when remote systems tunnel IP packets (for example, GRE, IP-in-IP, L2TP, GTP), and the tunnel overhead results in exceeding the configured MTU.

For TCP traffic, the ISA also provides support for adjusting the TCP MSS to a configured value during TCP session setup, which can prevent fragmentation.

Feature highlights

- In IPv4 reassembly, fragmented packets can be diverted to the ISA for reassembly based on applying an IP filter on the ingress forwarding complex.
- Adjusts the TCP MSS to a configured value; TCP SYN and SYN-ACKs are diverted to the ISA based on applying an IP filter on the ingress forwarding complex.

Benefits

- IP reassembly on the ISA supports networks where fragmentation cannot be avoided. The reassembly function on the ISA is performed without impacting normal fast-path traffic.
- The TCP MSS adjust function on the ISA removes the need for fragmenting TCP traffic, resulting in higher throughput and end-to-end network performance.

Wireless LAN Gateway

Wireless LAN gateway (WLGW) functionality on the Nokia ISA aggregates tunneled traffic and/or L2 switched traffic from the WLAN APs and/or WLAN Access Controllers (ACs). The WLGW features in the 7750 SR with the ISA support a variety of wholesale and retail deployment scenarios so both wireline and wireless providers can leverage unlicensed Wi-Fi® as an access technology.

The WLGW supports mechanisms to coordinate with the provider's backend subscriber, policy and billing infrastructure for authentication and the parameters needed to create subscriber context.

Feature highlights

- Supports both wholesale and retail service scenarios for wireline and wireless providers
- Highly scalable solution based on 3GPP S2a Mobility using the GTP (SaMOG) Release 11 "fat pipe" model, which minimizes the number of tunnels terminating on the WLGW because the tunnels originate on the APs instead of on UE
- Supports both open and closed service set identifiers (SSIDs)
- Supports multiple authentication methods, including EAP and web-based authentication
- Supports a RADIUS proxy function for IEEE 802.1x/EAP authentication
- Supports inter-AP mobility for seamless roaming between APs and cellular–Wi-Fi intermobility (cellular offload over Wi-Fi access), allowing UE to switch between cellular and Wi-Fi access
- Concurrent support for NAT functions on the same ISA
- Supports dual-stack deployments
- Supports L2 wholesale. L2 traffic for a retailer's SSID can be forwarded into a VPLS instance per retailer. The SSID is indicated by unique .1q tag inserted by the Wi-Fi AP.
- Supports access over stateless soft-GRE (L2oGRE and L2VPNoGRE) and soft-L2TPv3 tunnels from the AP or AC. This additional encapsulation allows access from an AP or AC behind a NAT.

- Supports the internal VLAN-to-ISA anchor function, enabling all the Wi-Fi features available with soft-GRE to be used for VLAN access from the AP over Layer 2 aggregation
- Per-AP or per-AP/per-SSID dynamic QoS from RADIUS
- Supports scalable distributed subscriber management (on MS-ISM)
- Python support on WLGW MS-ISM
- Supports packet counters in mobility-triggered interim accounting updates
- Supports all AA embedded L4–L7 use cases, including Wi-Fi AP congestion control
- Seamless inter-WLGW mobility based on cross-connect tunnel from visited WLGW to home WLGW

Benefits

- Allows wireline and wireless providers to leverage Wi-Fi access to expand service footprint
- Allows providers to deploy carrier-grade Wi-Fi service offerings, maintain customer visibility, and foster customer loyalty
- Allows wireless providers to preserve cellular spectrum by offloading data onto unlicensed Wi-Fi
- Allows provider wholesale Wi-Fi access service at L2 and/or L3 to retail providers

Virtualized Residential Gateway

Virtualized Residential Gateway (vRGW) functionality on the Nokia ISA allows operators to simplify a residential gateway. Functionality such as DHCP (L3), NAT and firewall (L3/L4), and deep packet inspection (DPI) (L3–L7) can be virtualized on the BNG/WLGW. The residential gateway becomes a simple bridging device that provides local switching of home LAN/WLAN traffic while tunneling or bridging traffic destined outside the home into a tunnel or a VLAN.

The subscriber-aware NAT function that is moved to the BNG/WLGW runs on an ISA. The vRGW allows a single outside IP address per home and supports static NAT port forwards as well as dynamic NAT port forwarding via universal plug and play internet gateway device (UPnP IGD) 1.0 support on an ISA.

Existing ESM functions apply to the vRGW.

The vRGW solution allows easier and faster introduction of services and visibility of devices on the home LAN for better troubleshooting as well as device-specific policy and services.

Feature highlights

- Subscriber-aware NAT with a single outside IP address per home
- Home-aware IPv4 address pool management
- Sticky and static private or public IPv4 addresses for home devices
- Static NAT port forwards with subscriber-aware NAT
- UPnP IGD 1.0
- Per-home NAT DMZ
- Per-home IPv6 stateless address autoconfiguration (SLAAC) prefix
- Per-device address via DHCPv6 IA_NA
- Per-device DNS override
- SLA management per home and per device on the home LAN
- Per-home and per-device configuration, including dynamic overrides and per-device AA deep packet inspection (DPI) processing
- Access based on soft-tunnels (L2oGRE, L2TPv3) or VLANs (L2 AP)
- Support for inter-chassis redundancy (based on data-triggered subscriber creation)
- Support for externally managed multiple NAT outside IP addresses per subscriber
- Support for extending home LAN to the data center for value-added services such as shared network attached storage (NAS)
- Support for AP-agnostic access for multi-tenant premises
- Support for a stateful residential IPv6 firewall
- Support for a PPPoE client to allow interoperability with existing BRAS deployments

Benefits

- Simplification of residential gateway
- Easier and faster introduction of services because these services can be provided in the network, either on the physical BNG or on appliances or servers in the cloud
- Consistent and vendor-agnostic feature rollout for residential services via a single instance of feature implementation on the vRGW in the network
- Visibility of devices on the home LAN, which can provide better troubleshooting by the provider
- Extension of the home LAN to a data center for value-added services such as shared NAS
- Home LAN visibility also allows device-specific policy and services in the network, such as parental control, cloud storage and home automation

Video

The Nokia ISA can be used to deliver superior IPTV QoE into the network elements, offering high scalability and flexible deployment scenarios. Advanced video functionality by the ISA includes:

- CDN for Live
- Perfect Stream
- Retransmission (RET)
- Fast Channel Change (FCC) for IPTV running over RTP
- Video Quality Monitoring (VQM).

Nokia CDN for Live

The Nokia CDN for Live solution allows video to be streamed directly to any end subscriber without multicast or IGMP support. A single Nokia ISA can provide video content for TV streaming, FCC and RET simultaneously. This extends the market reach beyond standard broadband IPTV service and directly to over the top (OTT) clients. Because CDN for Live is extended from FCC unicast, FCC and RET are inherent features for IP video for live TV subscribers as well.

Feature highlights

- Efficient, low live latency (<1sec) and simple IPTV streaming solution for both IPTV and OTT subscribers
- Live video streaming over any IP access with concurrent support for both traditional broadband multicast IPTV service and OTT subscribers

Benefits

- Eliminates network boundaries where only multicast IPTV services is offered
- Reuse existing ISA to reach OTT subscriber reducing CAPEX

Perfect Stream

Perfect Stream functionality provides network failure protection to ensure the best IPTV viewing experience. A network reconvergence event typically causes an IPTV outage in the range of 300–1200 msec. A reconvergence event is also counterproductive to requests for packet retransmission on a reconverging network.

The best and most efficient way to protect a multicast stream is through an alternate transmission path. Perfect Stream allows an operator to split a single multicast stream into two different transmission paths that can have different transmission characteristics (e.g., latency and jitter). Perfect Stream evaluates each stream on a packet-by-packet basis and selects the first error-free packet to send to the end user. The result is a “Perfect Stream” that is protected against various network faults.

Feature highlights

- Multicast protection against network faults
- Concurrent support of Perfect Stream and VQM on the same ISA
- Support for multicast source and group address translation for example, (S, G) to (S1, G1)

Benefits

- Perfect Stream can ensure the best multicast viewing experience and serve as the new multicast source for CDN for Live, FCC and RET

Retransmission

Packet losses in a video stream have an immediate and noticeable negative impact on an end user's IPTV QoE. RTP Retransmission functionality is an IETF and Digital Video Broadcasting (DVB) standard for packet retransmission.

The Nokia ISA supports a RET server for downstream clients/set-top boxes /Smart UHD TV / mobile device or any IP connected devices, and also pre-emptively repairs losses. With support for a RET server, RET services can be deployed where they are most cost effective and most needed.

Feature highlights

- Supports a RET server on video packet retransmission on linear TV channels for downstream RET clients
- Concurrent support for both RET and FCC on the same ISA

Benefits

- Allows for a greater service footprint for IPTV services by ensuring quality video delivery where the last-mile infrastructure would otherwise have unacceptable packet loss
- Allows flexible, distributed and hierarchical deployment options that optimize network resources, improve scalability and reduce CAPEX

Fast Channel Change

Fast Channel Change (FCC) functionality is a Nokia method for providing sub-second channel change on multicast IPTV networks distributed over RTP. An FCC session is a unicast stream sent at an accelerated rate before the main multicast streamis joined.

The ISA FCC server supports two methods of time domain compression for the FCC unicast stream: bursting and denting. Bursting sends the unicast at above the nominal rate. Denting selectively omits less important video frames in the unicast FCC stream. Denting is a particularly useful FCC technique when last-mile bandwidth is limited.

Bursting and denting can be combined for faster than-real-time delivery of the most pertinent video frames.

Feature highlights

- Provides sub-second linear TV channel change performance for FCC requests from a downstream video broadcast optimizer client
- Concurrent support for RET and FCC on the same ISA

Benefits

- Improves the end user's QoE by providing sub-second channel change performance
- Allows more efficient use of the network bandwidth by allowing greater levels of video compression through larger Group of Picture (GOP) sizes without affecting channel-change performance

Video Quality Monitoring

Video Quality Monitoring (VQM) functionality provides IPTV operators with a tool to identify the cause of visual impairments.

For the head end, transport-stream monitoring can utilize full reference video analysis by comparing the source content to the encoded output. For the customer end, STB probes can measure the end-user experience. However, the delivery network between the head end and the client is very complex, making it difficult to pinpoint problems.

VQM is a tool that offers another measurement point in the network, just prior to the last mile. The solution provides an inspection point for the multicast video stream that is combined with other methods of analysis to create a full view of video issues and help pinpoint the part of the network causing the issue.

Feature highlights

- Provides video quality measurements and metrics for all video channels before delivery to the last mile
- Categorizes alarms from impaired to program off air for each channel

Benefits

- Identifies video quality problems before end customers do
- Proactively scans for video quality problems, raising and clearing alarms
- Reduces the number of STB probes required in the network

Technical specifications

Table 1 provides a summary of the integrated services supported on the Nokia MS-ISA2 when installed in the Nokia 7750 SR and 7450 ESS product portfolio. The Nokia MS-ISA2 is supported on the Nokia 7750 SR series and the Nokia 7450 ESS using the IOM4-e, and on the 7750 SR-e series using the IOM-e.

Table 1. Integrated service support matrix for the Nokia MS-ISA2

Integrated service	7750 SR SR-7, SR-12, SR-12e	7750 SR-e SR-1e, SR-2e, SR-3e	7450 ESS ESS-7, ESS-12
Application Assurance	✓	✓	✓
Layer 7 Stateful Firewall	✓	✓	✓
LNS	✓	✓	—
CG-NAT	✓	✓	✓*
IPsec	✓	✓	✓*
IP tunneling	✓	✓	✓*
IPv4 reassembly	✓	✓	✓*
WLAN Gateway	✓	✓	—
Virtualized Residential Gateway	✓	✓	—
Video: IP video for live TV, Perfect Stream, RET, FCC and VQM	✓	—	—

* Requires mixed mode on the Nokia 7450 ESS

Table 2 provides a summary of the integrated services supported on the Nokia MS-ISM (with dual embedded ISA2s) when installed in the Nokia 7750 SR and 7450 ESS product portfolio.

Table 2. Service support matrix for the Nokia MS-ISM

Integrated service	7750 SR SR-7, SR-12, SR-12e	7450 ESS ESS-7, ESS-12
Application Assurance	✓	✓
Layer 7 Stateful Firewall	✓	✓
LNS	✓	✓*
CG-NAT	✓	✓*
IPsec	✓	✓*
IP tunneling	✓	✓*
IPv4 reassembly	✓	✓*
WLAN Gateway	✓	—
Virtualized residential gateway	✓	—
Video: IP video for live TV, Perfect Stream, RET, FCC and VQM	✓	—

* Requires mixed mode on the Nokia 7450 ESS

Feature and protocol highlights

Application Assurance & Layer 7 Stateful Firewall

- Up to 15 active ISA2s in up to 7 logical AA groups, each with N+1 MS-ISM and N+1 MS-ISA2 warm redundancy with “fail-to-fabric bypass”

Supported services

- 7450 ESS: ePipe, VPLS, IES and ESM subscribers
- 7750 SR: ePipe, iPipe, VPLS, IES, VPRN, ESM, ESM-MAC (device) and DSM subscribers
- AA on spoke SDPs is supported for services on spoke SDPs on the IOM3-XP, IOM4-e, IOM-e or MS-ISM

Standards support

- 3GPP Release 12 (ADC Rules over Gx Interfaces)
- RFC 3507, Internet Content Adaptation Protocol (ICAP)
- RFC 5101, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information
- RFC 5102, Information Model for IP Flow Information Export

LNS

- Up to six ISA2s (a mix of MS-ISMs, IMMs with ISA2s and MS-ISA2s) supported per chassis
- Up to four LNS groups
- Up to six ISA2s (a mix of MS-ISMs, IMMs with ISA2s and MS-ISA2s) supported per LNS group
- All MS-ISMs and MS-ISA2s in an LNS group are active, with sessions distributed based on least number of sessions and underlying IOM type load

Supported services

- L2TP tunnels can be terminated on any local router interface VPRN, IES, base router loopback and L33 SAP (VPRN and IES)

Standards support

- draft-mammoliti-l2tp-accessline-avp-04, Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions
- RFC 1332, The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1877, PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
- RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516, A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 2661, Layer Two Tunneling Protocol “L2TP”
- RFC 2809, Implementation of L2TP Compulsory Tunneling via RADIUS
- RFC 2868, RADIUS Attributes for Tunnel Protocol Support
- RFC 3438, Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update
- RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3)
- RFC 4638, Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) greater than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 4719, Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)
- RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) “failover”

CG-NAT

- Up to 28 ISA2s (a mix of MS-ISMs, IMMs with ISA2s and IOM4-e with MS-ISA2s are supported)
- Stateful inter-chassis redundancy with traffic preservation during switchover

Standards support

- draft-ietf-behave-address-format-10, IPv6 Addressing of IPv4/IPv6 Translators
- draft-ietf-behave-v6v4-xlate-23, IP/ICMP Translation Algorithm
- draft-miles-behave-l2nat-00, Layer2-Aware NAT
- draft-nishitani-cgn-02, Common Functions of Large Scale NAT (LSN)
- RFC 1918, Address Allocation for Private Internets
- RFC 4787, Network Address Translation (NAT) Behavioral Requirements for Unicast UDP

- RFC 5382, NAT Behavioral Requirements for TCP
- RFC 5508, NAT Behavioral Requirements for ICMP
- RFC 6146, Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 6333, Dual Stack Lite Broadband Deployments Following IPv4 Exhaustion
- RFC 6334, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual Stack Lite
- RFC 6888, Common Requirements For Carrier-Grade NATs (CGNs)
- RFC 7383, Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation

IPsec

- Up to 64 MS-ISA2s or 8 MS-ISMs supported in one tunnel-group with N:M active/standby configuration
- Support for 64 tunnel groups per system
- Stateful inter-chassis redundancy (IKEv2)
- Stateless intra-chassis redundancy

Encryption algorithms

- DES
- 3DES
- AES-CBC-128/192/256
- AESGCM-128/192/256

Authentication algorithms

- MD5
- SHA1
- SHA256
- SHA384
- SHA512
- AES-GMAC
- AES-XCBC

Key distribution methods

- Manual exchange
- IKEv1 and IKEv2 with Perfect Forward Secrecy (PFS) support

IPsec encapsulation methods

- Encapsulating Security Payload (ESP) with authentication support in tunnel mode
- ESP in Transport mode
- Extended sequence number for ESP

Key generation algorithms

- Diffie-Hellman Group: 1/2/5/14/15/19/20/21

Tunnel authentication methods

- Pre-shared keys
- XAUTH
- X.509 certificates (IKEv2)
- EAP (IKEv2)

Standards support

- draft-ietf-ipsec-isakmp-mode-cfg-05, The ISAKMP Configuration Method
- draft-ietf-ipsec-isakmp-xauth-06, Extended Authentication within ISAKMP/Oakley (XAUTH)
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2403, The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405, The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2407, IPsec Domain of Interpretation (IPsec DoI) for ISAKMP
- RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC 2410, The NULL Encryption Algorithm and its Use with IPsec
- RFC 3526, More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)
- RFC 3566, The AES-XCBC-MAC-96 Algorithm and its Use with IPsec
- RFC 3602, The AES-CBC Cipher Algorithm and its Use with IPsec

- RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3947, Negotiation of NAT-Traversal in the IKE
- RFC 3948, UDP Encapsulation of IPsec ESP Packets
- RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec ESP
- RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4211, Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
- RFC 4301, Security Architecture for the Internet Protocol
- RFC 4303, IP Encapsulating Security Payload
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308, Cryptographic Suites for IPsec
- RFC 4434, The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4945, The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX
- RFC 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
- RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5282, Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol
- RFC 5903, ECP Groups for IKE and IKEv2
- RFC 5998, An Extension for EAP-Only Authentication in IKEv2
- RFC 6379, Suite B Cryptographic Suites for IPsec
- RFC 6380, Suite B Profile for Internet Protocol Security (IPsec)
- RFC 6712, Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP)
- RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- RFC 7030: Enrollment over Secure Transport
- RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321, Cryptographic Algorithm Implementation Requirements and Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 7383, Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
- RFC 7427, Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
- RFC 7468, Textual Encodings of PKIX, PKCS, and CMS Structures
- RFC 8784, Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

IP tunneling

- Up to 8 MS-ISMs and 16 MS-ISA2s per chassis
- Support for 16 tunnel groups (active/standby MS-ISMs and IOM4-e with MS-ISA2s)

Standards support

- RFC 2003, IP Encapsulation within IP
- RFC 2473, Generic Packet Tunneling in IPv6 Specification
- RFC 2784, Generic Routing Encapsulation (GRE)
- RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3)
- RFC 4719, Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)

Wireless LAN Gateway

- Can be configured either per IOM or per ISA2 to provide flexibility in redundancy models
- Multi-chassis resiliency supporting N:1 redundancy

- Up to 7 active WLGW IOMs (IOM4-e with 2 MS-ISA2s) or MS-ISMs in IOM provisioning mode and up to 14 active WLGW ISA2s in Media Dependent Adapter (MDA) provisioning mode

Standards support

- 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses (S2a roaming based on GPRS)
- RFC 2784, Generic Routing Encapsulation (GRE)

Virtualized Residential Gateway

- Can be configured either per IOM or per ISA2 to provide flexibility in redundancy models
- Up to seven active vRGW IOMs (IOM4-e with two MS-ISA2s) or MS-ISMs in IOM provisioning mode and up to 14 active vRGW ISA2s in MDA provisioning mode

Video

- Up to six ISA2s (MS-ISMs, IMM with ISA2s, or MS-ISA2s) per chassis
- Up to six ISA2s (MS-ISMs, IMM with ISA2s, or MS-ISA2s) per video group with all active and load sharing to scale egress performance
- Up to four video groups, each with a distinct set of ingest channels

Standards support

- DVB BlueBook A86, Transport of MPEG-2 TS Based DVB Services over IP Based Networks
- ETSI TR 101 290
- RFC 3550 Appendix A.8, RTP: A Transport Protocol for Real-Time Applications (Estimating the Interarrival Jitter)
- RFC 4445, A proposed Media Delivery Index
- RFC 4585, Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)
- RFC 4588, RTP Retransmission Payload Format
- SCTE-143/ETSI TR 101 290 error counters

Dimensions and weights[1]

MS-ISA2

- Height: 3.6 cm (1.4 in)
- Width: 19.3 cm (7.6 in)
- Depth: 19.6 cm (7.7 in)
- Weight: 1.3 kg (2.86 lb)

MS-ISM

- Height: 3.6 cm (1.4 in)
- Width: 42.5 cm (16.7 in)
- Depth: 43.2 cm (17 in)
- Weight: 7.5 kg (16.5 lb)

Refer to the 7750 SR and 7750 SR-e data sheets and product documentation for full system details on dimensions, weights, hardware, safety standards, compliance agency certifications and protocol support.

1 Dimensions and weights are approximate and subject to change. Refer to the appropriate installation guide for the current dimensions and weight.

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

Document code: CID157673 (October)