

# ALCATEL-LUCENT 7750 SERVICE ROUTER AND 7450 ETHERNET SERVICE SWITCH MULTISERVICE INTEGRATED SERVICE ADAPTER RELEASE 10

The Alcatel-Lucent Multiservice Integrated Service Adapter (MS-ISA) extends the level of intelligence of the industry-leading Alcatel-Lucent 7750 Service Router (SR) and 7450 Ethernet Service Switch (ESS) platforms by virtualizing advanced service capabilities into a unified service edge. The Alcatel-Lucent MS-ISA provides purpose-built, extended functionality and enables deeper levels of integrated service capabilities with higher scale than typically available from costly dedicated appliances.



The Alcatel-Lucent MS-ISA provides a powerful platform for delivering advanced business and residential services on the 7750 SR and 7450 ESS without the need for costly external dedicated appliances. The Alcatel-Lucent MS-ISA is a half-slot, hot-swappable resource blade that inserts into an Input/Output Module (IOM). It features a flexible multi-core network processor designed for high-touch packet operations. MS-ISA services are virtualized and available to all ports across the chassis. Traffic flows are directed to the MS-ISA through the router's backplane and fabric, with support for more than 10 Gb/s bandwidth. Multiple MS-ISAs can be installed in the system to provide redundancy and deliver greater service scale.

Services currently supported on the Alcatel-Lucent MS-ISA include Application Assurance, L2TP Network Server (LNS), Network Address Translation (NAT), Dual-Stack Lite AFTR services, WLAN Gateway, IPsec services, MS-ISA Threat Management System (TMS) and advanced video services.

## MS-ISA FEATURES

- Provides multi-core network processor-based, carrier-grade hardware, operating within an industry-leading highly available and proven chassis
- 10 Gb/s data path connectivity through the chassis backplane and fabric
- Multiple MS-ISAs can be installed within a chassis to scale services

## MS-ISA BENEFITS

- Seamless integration into existing Alcatel-Lucent 7750 SR or 7450 ESS chassis that fully interoperates with all existing interfaces, thereby reducing standalone network elements with associated space and cabling, while reducing power consumption, topology churn and network latency.
- A single MS-ISA is equivalent to multiple external servers, offering huge scalability and resiliency advantages while reducing CAPEX.
- Consistent management of the MS-ISA services using Alcatel-Lucent 5620 Service Aware Manager (SAM) 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) on the Alcatel-Lucent MS-ISA extends the service depth and functionality of the Alcatel-Lucent 7750 SR and 7450 ESS by enabling visibility and intelligent control for IP applications, with extensive per-application, per-subscriber, or per-VPN Layer 2 and Layer 3 service policies, providing application reporting and traffic management capabilities. Application Assurance enables service providers to deliver enhanced and personalized Quality of Service (QoS)-managed application performance in highly differentiated consumer, business and mobile service offerings with industry-leading scale.

With Application Assurance, target traffic for AA processing is diverted to the ISA, based on an Application Profile assigned to the subscriber or service, which also contains parameters used by the Application QoS Policy (AQP) rules, comprising match and action criteria that determine the QoS treatment applied. This 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 business, mobile and residential applications, using IP address and ports, 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. This 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 routers behind the IP edge/BNG, asymmetry is automatically removed by the AA solution ensuring accurate identification and control.

#### Application Assurance

- Extensive per-application policy enforcement with granular bandwidth shaping, policing and prioritization, defined on a 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, application-based QoS, application admission control and application-level mirroring

#### Application reporting

- Per-protocol, per-application and per-application group volume statistics accounting for all subscribers and Layer 2 and Layer 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
- Aggregated snapshot of IP flows provided per subscriber and per VPN site
- 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
- Integrated Telchemy VQmon® passive performance measurement technology on in-service traffic for VoIP and video conferencing MOS-related measurements for RTP-based A/V applications
- 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

#### Benefits

- Provider Edge (PE) integration for residential subscribers or business 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 business services allows AA deployments for topologies requiring multiple subscriber policy enforcement points under common provisioning and subscriber policy management
- Enhanced managed services for residential consumers and content partners by leveraging Application Assurance 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, VPRN, VPLS and E Pipe services, to address enterprise requirements
- Scalable, pay-as-you-grow service with up to seven active MS-ISAs using Application Assurance per chassis
- No impact on network topology to add AA services to residential or business 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 MS-ISA is not available

## LNS SERVICES

LNS services on the Alcatel-Lucent MS-ISA add L2TP Network Server functionality to the Alcatel-Lucent 7750 SR, allowing service providers to offer the same industry-leading Enhanced Subscriber Management (ESM) services to subscribers terminated on L2TP sessions that are already available on the 7750 SR for IPoE (DHCP), PPPoE and PPPoA subscribers. By integrating an LNS into the 7750 SR, a single platform can support both PPP-based customers and provide an evolution towards IPoE (DHCP) while delivering a consistent user experience.

One of the featured applications of LNS services is the ability to introduce IPv6 services over existing 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 services support the Alcatel-Lucent Service Router Operating System (SR OS) IPv4 and IPv6 ESM features, so IPv4, IPv6, and dual-stack IPv4 and IPv6 subscribers are concurrently supported.

### Feature highlights

- Retains all ESM features for IPv4 and IPv6
- Supports up to 64,000 L2TP sessions and 16,000 L2TP tunnels per chassis
- Concurrent support for NAT and Dual-Stack Lite Software Concentrator on the same MS-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

## NAT SERVICES

NAT services on the Alcatel-Lucent MS-ISA add large-scale NAT capabilities to the Alcatel-Lucent 7750 SR, allowing service providers to conserve IPv4 addresses and maintain IPv4 Internet access while migrating to IPv6. NAT services on the MS-ISA were developed to satisfy service providers' large-scale NAT requirements, starting with the carrier-grade 7750 SR and MS-ISA platform and optimizing the software implementation to provide scale, transaction rates, and complete logging and accounting.

NAT services operate in two modes: Network Address and Port Translation (NAPT), with optimizations to provide scale and a subscriber-aware, Layer 2-aware NAT. In NAPT mode, an operator can deploy centralized Alcatel-Lucent 7750 SR to provide IPv4 continuity with minimal changes to the access network and customer equipment. Layer 2-aware NAT enhances NAPT to create a virtual NAT table per subscriber, allowing customized NAT policies and integrated RADIUS accounting, and it uniquely permits all subscribers to share a common inside IP address to simplify IPv4 address assignment and administration.

NAT services on the MS-ISA can also be used to extend IPv4 services and provide additional sources of revenue. NAT services allow for 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. NAT services can also be used to provide Internet access to an existing VPRN service.

### Feature highlights

- NAT44 and NAT64 with high scaling, high transaction rate and N+1 MS-ISA redundancy
- Two modes of operation:
  - NAPT with traditional inside and outside addresses
  - Layer 2-aware NAT, where NAT is agnostic to subscriber (inside) IP addresses, allowing for overlap and reuse
- Each host assigned port range blocks for greater scalability and reduced logging requirements
- Per-subscriber port limits with application priority based on traffic-forwarding class
- Configurable high/low prioritization of applications traversing the NAT, based on traffic-forwarding class

- Concurrent support for L2TP Network Server and Dual-Stack Lite Software Concentrator on the same MS-ISA

### Benefits

- Mitigates service provider IPv4 address exhaustion
- Allows IPv4 services to continue and evolve during the migration to IPv6 services
- Layer 2-aware NAT removes requirement for unique private IP addresses per subscriber
- Allows for unique NAT subscriber policies that are consistent with other Alcatel-Lucent 7750 SR service access methods: PPP, PPPoE, PPPoA, L2TP LNS and IPoE (DHCP)

## DUAL-STACK LITE

The Dual-Stack Lite AFTR services on the Alcatel-Lucent MS-ISA add Dual-Stack Lite software termination functionality to the Alcatel-Lucent 7750 SR. Dual-Stack Lite is an IPv6 transition technique that allows the tunneling of IPv4 traffic across an IPv6-only network. Dual-stack IPv6 transition strategies allow service providers 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. Dual-Stack Lite has two components: the client in the customer network, known as the Basic Bridging BroadBand element (B4), and the Address Family Transition Router (AFTR) deployed in the service provider network.

The Dual-Stack Lite AFTR services on the MS-ISA supports software termination, as described in draft-ietf-softwire-dual-stack-lite-06 for IPv4-in-IPv6 [RFC 2473] softwires, that encapsulate IPv4 traffic from the home network and IPv4-Internet across the carrier's IPv6 network.

### Feature highlights

- Highly scalable IP-in-IP tunneling of IPv4 over IPv6 for unmetered, best-effort services up to the scaling limits of Large Scale NAT Services
- Concurrent support for L2TP Network Server and IPv4 NAT functions on the same MS-ISA

### Benefits

- Allows IPv4 and IPv6 services to run across a single IPv6-only network infrastructure
- The Alcatel-Lucent 7750 SR also provides a complete IPv6 Broadband Network Gateway function, including built-in DHCPv6 server

- Simple-to-deploy Dual-Stack Lite with the 7750 SR Dual-Stack Lite AFTR

## WLAN GATEWAY

Within the Alcatel-Lucent lightRadio™ Wi-Fi solution, the Alcatel-Lucent 7750 SR functions as the Wireless LAN (WLAN) Gateway and aggregates tunneled traffic from the WLAN Access Points (APs). The WLAN Gateway features in the 7750 SR with the MS-ISA support a variety of wholesale and retail deployment scenarios, allowing both wireline and wireless providers to leverage unlicensed Wi-Fi® as an access technology. The WLAN Gateway supports mechanisms to coordinate with the provider's back-end subscriber, policy and billing infrastructure for authentication and 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 the 3GPP S2a Mobility based on GPRS Tunneling Protocol (GTP) (SaMOG) Release 11 "fat pipe" model which minimizes the number of tunnels between the APs and the WLAN Gateway
- Supports multiple authentication methods including Extensible Authentication Protocol (EAP) and web-based authentication
- Supports inter-AP mobility for seamless roaming between APs and cellular - Wi-Fi intermobility (cellular offload over Wi-Fi access) allowing user equipment to switch between cellular and Wi-Fi access
- Concurrent support for NAT functions on the same MS-ISA

### Benefits

- Allows wireline and wireless providers to leverage Wi-Fi access to expand service footprint
- Providers can deploy carrier-grade Wi-Fi service offerings and maintain customer visibility and foster customer loyalty
- Allows wireless providers to preserve cellular spectrum by offloading data onto unlicensed Wi-Fi

## IPSEC SERVICES

IPsec services on the MS-ISA provide comprehensive, highly scalable and network-integrated Layer 3 IPsec VPN connectivity, as a Remote Access Concentrator (RAC) or for site-to-site or network-to-network encrypted IPsec security. IPsec services can also be used in mobile networks as a highly scalable 3GPP Security Gateway (SeGW).

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 services can be combined with the Alcatel-Lucent 7750 SR comprehensive range of IP/MPLS service offerings.

### Feature highlights

- IKE v1/v2
- Pre-Shared Key/XAUTH/Certificate Authentication
- High-performance, hardware-based encryption and decryption
- Tunnel-mode Encapsulating Security Payload (ESP) with authentication support
- Bidirectional Forward Detection (BFD) within IPsec tunnels for fast tunnel failure detection

### Benefits

- Integrated IPsec services allow combining of connectivity services, greater service scale and resiliency, and reduced network latency
- Fully integrated with Alcatel-Lucent SR OS for unified service management, encryption and security, available to any Layer 3 service on any physical port

## MS-ISA THREAT MANAGEMENT SYSTEM DDOS MITIGATION

To meet the challenges of increasing DDoS scale and attack bandwidth, Arbor Networks and Alcatel-Lucent have teamed up to port the Arbor Networks Peakflow® SP Threat Management System software onto the Alcatel-Lucent MS-ISA card, creating a network- or cloud-based approach to DDoS scrubbing, where the TMS function is integrated within a carrier-class service router and can be distributed across a service provider's network:

Arbor Networks identifies all forms of DDoS attacks as well as the "network signature" of DDoS-related botnets as they try to scan for vulnerable PCs to infect. Once anomalies are identified, Peakflow SP signals the TMS within the service router to surgically mitigate attack traffic. Suspect traffic is forwarded to the MS-ISA TMS for scrubbing, or to a series of MS-ISA TMS blades using round-robin load balancing. Attack packets are dropped by MS-ISA TMS using a series of attack identification and mitigation techniques, and clean packets are forwarded by the service router to their original destination. The MS-ISA is managed through Alcatel-Lucent 5620 Service Aware Manager (SAM), and the TMS module is managed by the Arbor Networks Peakflow SP appliances.

### Feature highlights

- A carrier-class DDoS mitigation platform that enables greater scale, lower costs and simplified operations
- Leverages industry-leading technology from Arbor Networks and their ASERT threat research team, recognized experts in global carrier threat and traffic analysis
- Up to 60 Gb/s of DDoS processing per service router with other services active
- Surgically removes attack packets at the service provider network edge, eliminating the need to backhaul attack traffic deep within the service provider's network

### Benefits

- Allows service providers to extend their addressable market for DDoS protection services through flexible deployment of the mitigation function at any point in the router network
- Enables DDoS scrubbing across a wide range of verticals, customers and geographies, opening up new opportunities for DDoS mitigation services.
- Protects new and existing services from DDoS attacks and other threats

## VIDEO SERVICES

The Alcatel-Lucent MS-ISA can be used to deliver superior Internet Protocol Television (IPTV) QoE by incorporating advanced video services into the network elements, offering high scalability and flexible deployment scenarios.

Advanced video services enabled by the MS-ISA include:

- Retransmission (RET) and Fast Channel Change (FCC) for IPTV running over RTP
- Linear TV Ad Insertion (ADI)

### Retransmission

Packet losses in a video stream have an immediate and noticeable negative impact on an end user's IPTV QoE.

RTP Retransmission is an IETF and DVB standard for packet retransmission. The Alcatel-Lucent MS-ISA supports both a RET server, for downstream clients/set top boxes (STBs), and a RET client to request retransmissions upstream and preemptively repair losses. By supporting both a RET server and client in the MS-ISA, there is great flexibility in how RET services can be deployed, so services can be deployed where they are most cost-effective and most needed.

### Feature highlights

- Supports RET server on video packet retransmission on linear TV channels for downstream RET clients
- Supports RET client functions that allow more efficient use of the provider's network by preemptively recovering multicast packets lost upstream
- Concurrent support for RET and FCC on the same MS-ISA, providing up to 10 Gb/s of egress bandwidth

### 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, increase scale and reduce CAPEX

### Fast Channel Change

FCC is an Alcatel-Lucent method for providing sub-second fast 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 stream is joined.

The MS-ISA FCC server supports two methods of time domain compression for the FCC unicast stream: bursting and denting. Bursting sends the unicast above nominal rate, and 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, and both 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 Fast Channel Change requests from a downstream STB client
- Concurrent support for RET and FCC on the same MS-ISA, providing up to 10 Gb/s of egress bandwidth

### Benefits

- Improves the end user's Quality of Experience 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

## Linear TV Ad Insertion

The Alcatel-Lucent MS-ISA Video Services support local/zoned Linear TV ADI into the multicast video stream, thereby opening up new sources of revenue by allowing IPTV service providers to participate in the advertising value chain.

The Alcatel-Lucent MS-ISA supports up to 16 unique advertisement zones per main multicast channel stream. Because the splicer operates on the transport stream, ads can be spliced into either encrypted

or unencrypted main channel transport streams. As a result, the MS-ISA splicer is able to offer much higher scale and concurrency than elementary stream splicers.

### Feature highlights

- Provides the capability to insert up to 16 unique ads into each linear TV channel for 16 different areas or zones within each demographic market area
- Supports ad splicing for both encrypted and unencrypted main streams

### Benefits

- Linear TV ADI unlocks new revenue opportunities for service providers by participating in the advertising value chain

## PLATFORM SUPPORT

Table 1 provides a summary of the services supported on the Alcatel-Lucent MS-ISA when installed on IOM types within the Alcatel-Lucent 7450 ESS and 7750 SR product portfolio.

**Table 1. MS-ISA service support matrix**

SERVICE	7450 ESS		7750 SR		
	ESS-6, ESS-6V, ESS-7, ESS-12	SR-C4	SR-C12	SR-7, SR-12	SR-12E
Application Assurance	IOM-20G IOM3-XP	√	√	IOM-20G IOM2-20G IOM3-XP	IOM3-XP
LNS services	-	-	-	IOM3-XP	IOM3-XP
NAT services	-	-	-	IOM3-XP	IOM3-XP
Dual-Stack Lite AFTR services	-	-	-	IOM3-XP	IOM3-XP
WLAN Gateway	-	-	-	IOM3-XP*	IOM3-XP*
IPsec services	-	-	√	IOM2-20G IOM3-XP	IOM3-XP
Arbor TMS	-	-	-	IOM3-XP	IOM3-XP
Retransmission and Fast Channel Change	IOM-20G IOM3-XP	-	-	IOM-20G IOM2-20G IOM3-XP	IOM3-XP
Linear TV Ad Insertion	-	-	-	IOM-20G IOM2-20G IOM3-XP	IOM3-XP

\* WLAN Gateway functionality is configured in hardware on a slot basis where an IOM3-XP has two MS-ISA installed.

## ORDERING INFORMATION

Table 2 provides ordering information for the MS-ISA hardware. Services on the MS-ISA require the purchase of Right to Use (RTU) licenses. Please contact your Alcatel-Lucent sales representative for pricing information on service licenses.

**Table 2. Ordering information for the Alcatel-Lucent Multiservice ISA**

PART NUMBER	PART NAME	COMMENTS
3HE04922AA	ISA – 7x50 Multiservice ISA	Base Multiservice ISA card which can be used for AA, video, LNS, NAT and IPsec applications
3HE05154AA	ISA – 7x50 Multiservice ISA-E no encrypt	Base Multiservice ISA-E card which can be used for AA, video, LNS and NAT applications. No IPsec support (no encryption)



## TECHNICAL SPECIFICATIONS

### MS-ISA

#### Dimensions, weight and power

- Height: 3.6 cm (1.4 in.)
- Width: 19.0 cm (7.5 in.)
- Depth: 17.8 cm (7 in.)
- Weight: 0.45 kg (1 lb) (approx.)
- Maximum power consumption: 65 W

Note: Weights and dimensions are approximate and subject to change. Refer to the appropriate Installation Guide for the current weight and dimensions.

#### Environmental specifications

- Operating temperature: 5°C to 40°C (41°F to 104°F)
- Operating relative humidity: 5% to 85%
- Operating altitude: Up to 4000 m (13,000 ft) at 30°C (86°F)

#### Safety

- EN 60950-1 2nd Ed CE-Mark
- IEC 60950-1 2nd Ed CB Scheme
- CSA/UL 60950-1 2nd Ed NRTL

#### EMC emission

- ICES-003 Class A
- FCC Part 15 Class A
- EN 55022 Class A
- CISPR 22 Class A
- AS/NZS CISPR 22
- VCCI Class A
- BSMI Class A

#### EMC immunity

- EN 300 386
- EN 55024
- 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 61000-4-8 Magnetic Immunity
- IEC/EN 61000-4-11 Voltage Interruptions

#### Environmental

- ETS 300 019-1-1 Storage Tests, Class 1.2
- ETS 300 019-1-2 Transportation Tests, Class 2.3
- ETS 300 019-1-3 Operational Tests, Class 3.2
- ETS 300 019-2-4, pr A 1 Seismic
- WEEE
- RoHS
- China CROHS

### Network Equipment Building System (NEBS)

- NEBS Level 3 Compliant
  - Telcordia GR-1089-CORE
  - Telcordia GR-63-CORE
- Telcordia GR-295-CORE
- RBOC requirements
  - ATT-TP-76200
  - ATT-TP-76200 section 13, TEER per ATIS-0600015.02
  - VZ.TPR.9205 TEEER per ATIS-0600015.02
  - VZ.TPR.9305

### Application Assurance

#### Redundancy and scale

- 7750 SR-7 and 7750 SR-12
  - Up to eight MS-ISAs per chassis
  - Up to seven logical AA groups, each with N+1 MS-ISA warm redundancy with “fail-to-fabric bypass”
  - Up to 70 Gb/s of wire-speed packet processing and application recognition per system
- 7750 SR-c12
  - Up to two MS-ISAs per chassis
  - One logical AA group with 1+1 MS-ISA warm redundancy or 2+0 MS-ISA non-redundant
  - Up to 20 Gb/s of wire-speed packet processing and application recognition per system
- 7750 SR-c4
  - One MS-ISA per chassis
  - One logical AA group non-redundant
  - Up to 10 Gb/s of wire-speed packet processing and application recognition per system

#### Performance and scalability per ISA

- Up to 10 Gb/s processing capacity
- Traffic flow set-up rate of up to 70,000 new flows per second
- Induced packet latency of existing flows <20 µs
- Induced packet latency of new flows <100 µs

### Supported services

- 7450 ESS: E-Pipe, VPLS, IES, ESM subscribers
- 7750 SR: E-Pipe, I-Pipe, VPLS, IES, VPRN, Enhanced Subscriber Management (ESM) subscribers
- AA on Spoke SDPs is supported for services on spoke SDPs on the IOM3-XP as indicated in Table 3

### Standards support

- 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 services

#### Redundancy and scale

- Up to six MS-ISAs per chassis
- Up to four LNS groups
- Up to four MS-ISAs per group
- All MS-ISAs in an LNS group are active with sessions distributed based on least number of sessions and underlying IOM3-XP load
- Up to 60 Gb/s of throughput per system

#### Performance and scalability per ISA

- Up to 10 Gb/s processing capacity
- Scaling constrained by MS-ISA IOM3-XP service queue resources

### Supported services

- L2TP tunnels can be terminated on any local router interface VPRN, IES, base router loopback and Layer 3 SAP (VPRN and IES)

### Standards support

- RFC 1332 – The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 – PPP Authentication Protocols
- 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)

Table 3. Spoke SDP types and supported services

	SPOKE SDP TYPE					CONNECTED TO SERVICE				
	E-PIPE	VPLS	IES	VPRN	I-PIPE	E-PIPE	VPLS	IES	VPRN	I-PIPE
E-Pipe	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
I-Pipe	N	N	Y	Y	Y	N	N	Y	Y	Y
VPLS	N	Y	Y	Y	N	N	Y	Y	Y	N

- 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 3145 – L2TP Disconnect Cause Information
- RFC 3371 – Layer Two Tunneling Protocol “L2TP” Management Information Base
- RFC 3438 – Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update
- RFC 4638 – Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)
- draft-mammoliti-l2tp-accessline-avp-04.txt – Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions
- draft-ietf-behave-v6v4-xlate-stateful-12 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- draft-ietf-behave-v6v4-xlate-23 - IP/ICMP Translation Algorithm

## Dual-Stack Lite

### Redundancy and scale

- Up to six MS-ISAs per chassis
- Up to four NAT groups
- Up to four MS-ISAs per group with N+1 warm redundancy
- Up to 60 Gb/s of throughput (non-redundant) per system
- Up to 36,000,000 total mappings

### Performance and scalability per ISA

- 128,000 active DS-Lite AFTR endpoints per ISA, with full statistics collection and event logging
- 6,000,000 NAT mappings per ISA
- 10 Gb/s IMIX performance
- Support for static port forwarding via SAM API

### Standards support

- RFC 2473 – Generic Packet Tunneling in IPv6 Specification
- draft-ietf-softwire-dual-stack-lite-06.txt – Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
- draft-ietf-softwire-ds-lite-tunnel-option-05.txt – Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite

## WLAN Gateway

### Redundancy and scale

- WLAN Gateway is configured on a slot-basis with an IOM3-XP and two MS-ISA required per slot
- Up to four slots configured for WLAN Gateway operation
- Up to three slots active supporting N:M redundancy
- 128K tunnels per chassis
- 128K UEs per chassis

### Standards support

- S2a Mobility based on GPRS Tunneling Protocol within 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses. Release 11,
- RFC 2784 - Generic Routing Encapsulation (GRE)

## IPsec services

### Redundancy and scale

- Up to 16 MS-ISAs per chassis
- Support for 16 tunnel groups (active/standby MS-ISAs)

### Performance and scalability per ISA

- High-performance, hardware-based encryption and decryption

### Encryption methods

- DES, 3DES, AES-128, AES-192 and AES-256

### Authentication and hashing methods

- HMAC-MD5, HMAC-SHA1, HMAC-SHA2

### 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

### Key generation algorithms

- Diffie-Hellman

### Tunnel authentication methods

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

### Key IPsec RFC(s) supported

- RFC2315 – PKCS #7: Cryptographic Message Syntax
- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2409 – The Internet Key Exchange (IKE)
- RFC2986 – PKCS #10: Certification Request Syntax Specification
- RFC 3447 – PKCS #1: RSA Cryptography Specifications Version 2.1
- RFC 3706 – IKE Dead Peer Detection
- RFC 3947 – Negotiation of NAT Traversal in the IKE
- RFC 3948 – UDP Encapsulation of IPsec ESP Packets
- RFC 4306 – Internet Key Exchange (IKEv2) Protocol
- 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 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- draft-ietf-ipsec-isakmp-xauth-06.txt – Extended Authentication within ISAKMP/Oakley (XAUTH)
- draft-ietf-ipsec-isakmp-mode-cfg-05.txt – The ISAKMP Configuration Method

## **Arbor TMS**

### **Redundancy and scale**

- Up to 12 MS-ISAs per chassis
- Up to 60 Gb/s DDoS scrubbing capacity per chassis

### **Performance and scalability per ISA**

- Up to 5 Gb/s for DDoS scrubbing capacity

## **Video services**

### **Retransmission and Fast Channel Change**

#### **Redundancy and scale**

- Up to eight MS-ISAs per chassis
- Up to four MS-ISAs 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

### **Performance and scalability per ISA**

- More than 4 Gb/s ingest multicast video processing
- Up to 10 Gb/s RET/FCC egress capacity

### **Standards support**

- RFC 3550 – RTP: A Transport Protocol for Real-Time Applications
- RFC 4585 – Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)
- RFC 4588 – RTP Retransmission Payload Format
- Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks (DVB-IPTV Phase 1.4)

### **Local/zoned ad insertion**

#### **Redundancy and scale**

- One MS-ISA per video group
- Inter-chassis redundancy provided by multicast protocol reconvergence

### **Performance and scalability per ISA**

- More than 4 Gb/s ingest multicast video processing
- Up to 10 Gb/s egress throughput for main streams and ad splices
- Up to 16 zones per ingress multicast channel

### **Standards support**

- SCTE 30
- SCTE 35