Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R6

RELEASE DESCRIPTION

3HE 06473 AAAF TQZZA Edition 01

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

CONTENTS

I. RELEASE 9.0 – AT A GLANCE

Target Schedule

Four releases with new content are planned.

9.0 R1 – April 20, 2011

- Nodal Program Support: 7x50 9.0 R1, 7705, 9500, 7210, OMNI, 9412, eNodeB, 7750 MG, 9471 MME, 5780 DSC
- NSM content
- Platform Applications & New GUI Framework for Usability
- Scale @8.0 Limits & Long Lead Scale & Architecture work
- CPAM 5.0

9.0 R3 – July 20, 2011

- 1830 PSS-32/16 Release 2.5 and 2.5.1, 3.5, 3.5.1, 3.5.2
- 1830 PSS-4 Release 1.5
- 1830 PSS-1 GBEH Release 2.5, 2.5.1, 2.7
- 1830 PSS-1 MD4H Release 1.5, 1.7
- 1830 PSS-1 AHP Release 1.0
- 5620 SAM Application and Security enhancements

9.0 R5 – October 19, 2011

- Nodal Program Support: 7x50 9.0 R1, R3, R4; 7210 3.R5, 7750 MG3.0 R1, R5, OS 10K with AOS 7.1.1, 9412 eNodeB LA 4.0, 9471 MME LM 4.0.2, 9500 MPR 3.0, 3.0.1
- Templates: Cascading
- STM: Auto-OAM, per segment OAM
- TCA support for all MIB based Network and Server Performance Stats;
- SAM-O Extension of registerLogToFile method to Performance Stats
- Application Assurance Enhancements: business transit subscribers, business transit subscriber aggregation, support of AA on 7750-c12, usage base billing attributes

9.0 R7 – January 2012

There will also be maintenance releases scheduled in between content releases throughout the year.

Network Element Support

Please see the *5620 SAM Network Element Compatibility Guide* for information on release compatibility.

Feature List

The following table lists all candidate and committed nodal and NMS features to be supported in 5620 SAM, along with expected target releases. Features in support of LTE solution are included in this list, however there is a dedicated *5620 SAM LTE LE4.0 Release Description* providing detailed descriptions of those features. They are not covered in section IV of this document.

Note: This view is subject to change. Feature statuses for Release 9.0 R7 are tentative. View as of October 13, 2011. Ask your regional representative for an updated view if required.

Rel	Load	Feature Description	Status	Node Number	Node Rel	Node Load
Nodal Features						
9.0	R1	Out of Band management (SAS X)	Committed	7210	2.0	R1
9.0	R1	SAP-EgressAggRateLimit for SAS-X for 2.0 R7	Committed	7210	2.0	R7
9.0	R1	VCCV Trace support in 7210 SAS 3.0R1	Committed	7210	3.0	R1
9.0	R1	L2 uplink support on SAS-M. Requires 3.0 R2.	Committed	7210	3.0	R2
9.0	R1	QOS support for L2 uplink on SAS-M. Requires 3.0 R2.	Committed	7210	3.0	R2
9.0	R1	IGMP Snooping support for L2 uplink on SAS-M. Requires 3.0 R2.	Committed	7210	3.0	R2
9.0	R1	802.1ag and EFM support on L2 uplink on SAS-M. Requires 3.0 R2.	Committed	7210	3.0	R2
9.0	R1	IP interface support on L2 uplinks on SAS-M. Requires 3.0 R2.	Committed	7210	3.0	R2
9.0	R1	G.8032 - Ethernet Ring Protection for SAS-X	Committed	7210	3.0	R2
9.0	R1	IGMP Snooping on SAS-X.	Committed	7210	3.0	R2
9.0	R1	7210 SAS-D-6F4T support	Committed	7210	3.0	R3
9.0	R1	Support for Dot1q explicit NULL SAP	Committed	7210	3.0	R3
9.0	R1	BFD for FRR (Network Mode in SAS-M)	Committed	7210	3.0	R3
9.0	R1	MSTP on SAS-M/X	Committed	7210	3.0	R3
9.0	R1	SAR-18 HW Platform	Committed	7705	4.0	R1
9.0	R1	IPv6 with IES (static routing)	Committed	7705	4.0	R1
9.0	R1	IEEE 802.1x EAP	Committed	7705	4.0	R1
9.0	R1	DCR: Improve bring-up time for static LSP	Committed	7705	4.0	R1
9.0	R1	RSVP-TE Graceful Shutdown	Committed	7705	4.0	R1
9.0	R1	802.1ab LLDP	Committed	7705	4.0	R1
9.0	R1	DCR: Increase number of "management" static-routes	Committed	7705	4.0	R1
9.0	R1	MAC Swap on Enet Port Loopback	Committed	7705	4.0	R1
9.0	R1	Local LSR ID	Committed	7705	4.0	R1

9.0	R1	Service Retargetting (cPIPE)	Committed	7705	4.0	R1
9.0	R1	Increase# of VPRN SDPs	Committed	7705	4.0	R1
9.0	R1	VPLS - incl PPPoEoA into SAP	Committed	7705	4.0	R2
9.0	R1	Spoke SDP termination into IES/VPRN	Committed	7705	4.0	R2
9.0	R1	Bridged ATM VPLS SAP (on 4p OC3)	Committed	7705	4.0	R2
9.0	R1	PPP Relay (on Bridged ATM)	Committed	7705	4.0	R2
9.0	R1	32p T1/E1 adapter card	Committed	7705	4.0	R3
9.0	R1	16p T1/E1 ASAP MDA (de-stuffed 32p)	Committed	7705	4.0	R3
9.0	R1	DSC Alarms	Committed	5780 DSC	3.0	R1
9.0	R1	DSC Geo-Redundancy	Committed	5780 DSC	3.0	R1
9.0	R1	5780 DSC 3.0 Support	Committed	5780 DSC	3.0	R1
9.0	R1	SGW 3.0 R1 Support	Committed	7750 MG	3.0	R1
9.0	R1	3GPP R8 Compliance	Committed	7750 MG	3.0	R1
9.0	R1	3GPP Lawful Intercept Interface	Committed	7750 MG	3.0	R1
9.0	R1	Support MG3.0 nodes at a MG2.0 level	Committed	7750 MG	3.0	R1
9.0	R1	S1-based HO with MME relocation and no SGW relocation	Committed	7750 MG	3.0	R1
9.0	R1	Piggyback Support	Committed	7750 MG	3.0	R1
9.0	R1	UE Initiated Procedures	Committed	7750 MG	3.0	R1
9.0	R1	Primary KPIs and KCIs	Committed	7750 MG	3.0	R1
9.0	R1	Idle Mode TAU with MME Change	Committed	7750 MG	3.0	R1
9.0	R1	IPv6 support in Reassembly Interfaces	Committed	7750 MG	3.0	R1
9.0	R1	Graceful PGW shutdown	Committed	7750 MG	3.0	R5
9.0	R1	BFD Scalability improvements to 2.5K	Committed	7x50	8.0	R4
9.0	R1	GRE termination in VPRN - Part 1	Committed	7x50	8.0	R4
9.0	R1	MC-APS service parity for Sonet/SDH channelized and non-channelized interfaces	Committed	7x50	8.0	R5
9.0	R1	Short keep-alive time for limited number of PPPoE sessions	Committed	7x50	8.0	R6
9.0	R1	Tunable XFP support (JDSU's new c-band part)	Committed	7x50	9.0	R1
9.0	R1	7450/7750 mixed mode support - phase 2 (7750 (IPv6 in chassis mode B) and additi	Committed	7x50	9.0	R1
9.0	R1	CPM1/2 co-existing with CPM3 for upgrade purpose only (no downgrade or CPM4 supp	Committed	7x50	9.0	R1
9.0	R1	VSM2 support - VSM2 MDA with XPL+ - Support for current and new provisioning mod	Committed	7x50	9.0	R1
9.0	R1	G8032 --- multi-ring (completion from 8.0.R4)	Committed	7x50	9.0	R1
9.0	R1	IP interface stats with SNMP access on network ports (RFE 65823)	Committed	7x50	9.0	R1

9.0	R1	MEF SLM (Synthetic Loss Measurement)	Committed	7x50	9.0	R1
9.0	R1	CFM Hold-Down Timer	Committed	7x50	9.0	R1
9.0	R1	TWAMP server perf monitoring	Committed	7x50	9.0	R1
9.0	R1	Facility MEP (includes V-UNI & Port level MEP)	Committed	7x50	9.0	R1
9.0	R1	10k BGP Peers	Committed	7x50	9.0	R1
9.0	R1	Flowspec	Committed	7x50	9.0	R1
9.0	R1	mLDP in mVPN for I-PMSI (P2MP LDP I-PMSI)	Committed	7x50	9.0	R1
9.0	R1	M-VPN: MDT AFI/SAFI	Committed	7x50	9.0	R1
9.0	R1	MC-LAG support for IP services	Committed	7x50	9.0	R1
9.0	R1	cflowd enhancements (IPFIX, IPv6 & mcast)	Committed	7x50	9.0	R1
9.0	R1	multi-area adj OSPF (RFC 5185) - no support for OSPFv3	Committed	7x50	9.0	R1
9.0	R1	RTM async / lockless design	Committed	7x50	9.0	R1
9.0	R1	IPv6 BFD support: static, OSPFv3, BGP, VRRP	Committed	7x50	9.0	R1
9.0	R1	Converged TE database	Committed	7x50	9.0	R1
9.0	R1	Inter-Area RSVP-TE using manually provisioned ABR and ABR FRR node protection us	Committed	7x50	9.0	R1
9.0	R1	Scaling of RSVP, LDP, and BGP LSPs	Committed	7x50	9.0	R1
9.0	R1	Uniform sub50msec fail-over for LER/LSR FRR	Committed	7x50	9.0	R1
9.0	R1	VPLS & ISID Scale : 40k	Committed	7x50	9.0	R1
9.0	R1	ISID level shaping on B-SAP	Committed	7x50	9.0	R1
9.0	R1	LAG active/standby operation without LACP (RFE86488)	Committed	7x50	9.0	R1
9.0	R1	Block on mesh failure in BGP VPLS + BGP MH (RFE 87517)	Committed	7x50	9.0	R1
9.0	R1	IPVPN - Service Label per Next-hop operation	Committed	7x50	9.0	R1
9.0	R1	GRE termination in VPRN - Part 2 (support for OSPF and IPsec)	Committed	7x50	9.0	R1
9.0	R1	FIB prioritization per VPRN	Committed	7x50	9.0	R1
9.0	R1	Carrier-serving-Carrier VPN (CsC VPRN)	Committed	7x50	9.0	R1
9.0	R1	Support for BGP LSP type in mixed-LSP mode SDP (RFE 95794)	Committed	7x50	9.0	R1
9.0	R1	Unified RADIUS interface	Committed	7x50	9.0	R1
9.0	R1	NAT44 Enhancements	Committed	7x50	9.0	R1
9.0	R1	NAT: dynamic port-range block allocation	Committed	7x50	9.0	R1
9.0	R1	NAT: SIP ALGs	Committed	7x50	9.0	R1
9.0	R1	DHCPv6 server for IPv6 ESM	Committed	7x50	9.0	R1

9.0	R1	IPsec IKEv2 (Part 2)	Committed	7x50	9.0	R1
9.0	R1	Scale to 100G (simplex) IPsec per system	Committed	7x50	9.0	R1
9.0	R1	ISA Capacity information	Committed	7x50	9.0	R1
9.0	R1	Residential IP transit subs: static subs (CLI/SNMP) and dynamic subs (DHCP/RADIU	Committed	7x50	9.0	R1
9.0	R1	App performance stats for VoIP/Video (UDP MOS scores) as defined in 8.0 PRD	Committed	7x50	9.0	R1
9.0	R1	Improved overload handling (overall overload and cut-through)	Committed	7x50	9.0	R1
9.0	R1	AA Policer Resource Alarms	Committed	7x50	9.0	R1
9.0	R1	Soft rest support on Magma IMMs	Committed	7x50	9.0	R1
9.0	R1	HSMDA v2	Committed	7x50	9.0	R1
9.0	R1	T-LDP control plane support for Hash Label feature in PW-based services	Committed	7x50	9.0	R3
9.0	R1	Enable uRPF check on subscriber interface for managed-route hosts. "uRPF on group interfaces"	Committed	7x50	9.0	R3
9.0	R1	Unnumbered interfaces for PPPoE (IPv4 only)	Committed	7x50	9.0	R3
9.0	R1	10-port GE HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	RADIUS Accounting (per subscriber, IPv4/v6 addresses)	Committed	7x50	9.0	R3
9.0	R1	DSLAM and other stats	Committed	7x50	9.0	R3
9.0	R1	host tracking (aggregate rate only)	Committed	7x50	9.0	R3
9.0	R1	CoA on subscribers instead of hosts (aggr, pol, queue, root arbiter)	Committed	7x50	9.0	R3
9.0	R1	Last-mile-aware shaping on HS-MDA2 using control plane implementation and PPPoE encaps only	Committed	7x50	9.0	R3
9.0	R1	Aggregate rate dynamic override	Committed	7x50	9.0	R3
9.0	R1	Queue/Policer parameters (PIR/CIR/WRR) override	Committed	7x50	9.0	R3
9.0	R1	New fc->q overrides (new SLA)	Committed	7x50	9.0	R3
9.0	R1	New MDA type for HS-MDA2 BT QoS model	Committed	7x50	9.0	R3
9.0	R1	Everything under Config QoS for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	Everything under Config sub subscriber profile for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	Exp Secondary Shaper for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	Resource manager for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	SAP stats for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	SAP overrides for HS-MDA2	Committed	7x50	9.0	R3
9.0	R1	PPP keepalive timers	Committed	7x50	9.0	R3

9.0	R1	Route origin attribute for subscriber hosts used in routing policies	Committed	7x50	9.0	R3
9.0	R1	IGMP reporting of join/leave/expiry events (IGMP redirect)	Committed	7x50	9.0	R3
9.0	R1	RADIUS-triggered LI for IPv6 PPPoE only	Committed	7x50	9.0	R4
9.0	R1	Service Size Reduction	Committed	7x50		
9.0	R1	Dimensioning and KPI eNB for LE3 - step 2	Committed	9412 eNodeB	LA3.0	
9.0	R1	SAM support of eNB upgrade from TLA2.1 to TLA3.0	Committed	9412 eNodeB	TLA3	
9.0	R1	9500 R3.0 ANSI / ETSI Equipment Management	Committed	9500 MPR	3.0	
9.0	R1	9500 3.0 Dot1Q VLAN	Committed	9500 MPR	3.0	
9.0	R1	9500 3.0 STM support	Committed	9500 MPR	3.0	
9.0	R1	Services over SDH	Committed	9500 MPR	9.0	R1
9.0	R1	MPR Family DS1/E1 Synchronization	Committed	9500 MPR	2.0 A	
9.0	R1	9500 R2.x A/E Stream Support	Committed	9500 MPR	2.x	
9.0	R1	Path Management	Committed	9500 MPR		
9.0	R1	Port Segregation Usability	Committed	9500 MPR		
9.0	R1	Extended Backhaul Service	Committed	9500 MPR		
9.0	R1	OS6855-U24X capability- including VRF capabilities	Committed	OmniSwitch	6.4.3	
9.0	R1	G8032/Ethernet Ring Protocol	Committed	OmniSwitch	6.4.3 / 6.6.2	
9.0	R1	AOS Release 6.4.4 Support for OS6850/OS6855/OS6400/OS9000	Committed	OmniSwitch	6.4.4	
9.0	R1	OS6850-E support with AOS 6.4.4 Support	Committed	OmniSwitch	6.4.4	
9.0	R1	Usability Improvements incl. Service Type for Access IF	Committed			
9.0	R2	SAM model updates for TLA2.1 and TLA3.0	Committed	9412 eNodeB	TLA3	
9.0	R3	Support for 1830 PSS-1 GBEH 2.7	Committed	1830	GBEH 2.7	
9.0	R3	Support for 1830 PSS-1 MD4H 1.7	Committed	1830	MD4H 1.7	
9.0	R3	Mib Stats support till 3.5	Committed	1830	PSS-32	3.5
9.0	R3	PSS1/16/32 new release support up to 3.5.2	Committed	1830	PSS-32	3.5
9.0	R3	Backup/Restore support	Committed	1830	PSS-32	3.5
9.0	R3	11DPE12E(Release 3.5)	Committed	1830	PSS-32	3.5
9.0	R3	License support	Committed	1830	PSS-36	3.5
9.0	R3	1830 PSS-4 Release 1.5	Committed	1830	PSS-4	1.5
9.0	R3	Fault Management support	Committed	1830		
9.0	R3	Provisioning and management of Y cable protection on all supporting service conf	Committed	1830		
9.0	R3	OPSA Provision	Committed	1830		

9.0	R3	Provisioning and management of Regen services on all supporting service configur	Committed	1830		
9.0	R3	Card support up to 3.5.2	Committed	1830		
9.0	R3	File based Stats till 3.5.2	Committed	1830		
9.0	R3	Unprotected Service support	Committed	1830		
9.0	R3	Subrate Service Provision	Committed	1830		
9.0	R3	Supported NE's as Service Endpoints	Committed	1830		
9.0	R3	1830 OT support - Power Graph Read Only	Committed	1830		
9.0	R3	SR WDM network port support - Power Graph Read Only	Committed	1830		
9.0	R3	Power Readings support for WTOCM card - Power Graph Read Only	Committed	1830		
9.0	R3	Support configurations including SVAC, MVAC, OPSA and Raman cards - Power Graph Ready Only	Committed	1830		
9.0	R3	VLL-PW Standby status bit signalling	Committed	7210	3.0	R3
9.0	R3	Line Timing of Ethernet ports using synchE with SSM support on SAS M/X	Committed	7210	3.0	R3
9.0	R3	BFD for static routes (Network Mode in SAS-M)	Committed	7210	3.0	R3
9.0	R3	SAP-EgressAggRateLimit for SAS-X for 3.0 R3 enhancements	Committed	7210	3.0	R3
9.0	R3	Fractional T1 PPP on NW port (super rate)	Committed	7705	4.0	R1
9.0	R3	IEEE 1588 Boundary Clock	Committed	7705	4.0	R2
9.0	R3	SAA Support for CFM	Committed	7705	4.0	R2
9.0	R3	Standby Signalling Slave	Committed	7705	4.0	R2
9.0	R3	SAR-18 BITS clock (BASIC)	Committed	7705	4.0	R3
9.0	R3	BFD for T-LDP	Committed	7705	4.0	R3
9.0	R3	BFD for V6 Static Routes	Committed	7705	4.0	R3
9.0	R3	Enhancements to External Alarm Monitoring	Committed	7705	4.0	R3
9.0	R3	Dynamic ARP for Spoke SDP Termination	Committed	7705	4.0	R3
9.0	R3	PTS 604519: LDP Tunnel-Down Damp-Timer	Committed	7705	4.0	R3
9.0	R3	Multiple E1 multi-frames in a single PW	Committed	7705	4.0	R4
9.0	R3	DCR: ML-PPP sequence number re-design	Committed	7705	4.0	R4
9.0	R3	OSFP v3	Committed	7705	4.0	R4
9.0	R3	IPv6 Management	Committed	7705		
9.0	R3	Spanning tree Protocol (STP) with VPLS	Committed	7705		
9.0	R3	Lawful Intercept Enhancements	Committed	7750 MG	3.0	R1

9.0	R3	Trusted Peer Lists	Committed	7750 MG	3.0	R3
9.0	R3	MG: GGSN/SGW GA peer and stats support	Committed	7750 MG		
9.0	R3	IPSec - Discovery	Committed	7750 MG		
9.0	R3	IPsec IKEv2	Committed	7x50	8.0	R5
9.0	R3	Magma and BSX interaction	Committed	7x50	9.0	R1
9.0	R3	ETH-CFM Redundancy	Committed	7x50	9.0	R1
9.0	R3	VLAN in MAC filter inc. bitmask for ACL and QoS policies	Committed	7x50	9.0	R1
9.0	R3	Percentage based BW in QoS policies	Committed	7x50	9.0	R1
9.0	R3	Policer mapping to local-queue	Committed	7x50	9.0	R1
9.0	R3	NAT: lawful intercept (on BB-ISA)	Committed	7x50	9.0	R1
9.0	R3	DSLite support [IP in IP]	Committed	7x50	9.0	R1
9.0	R3	PPPoE idle timeout	Committed	7x50	9.0	R1
9.0	R3	IPCP subnet negotiation	Committed	7x50	9.0	R1
9.0	R3	N:1with N>1 ATM mapping on ATM PWE3	Committed	7x50	9.0	R1
9.0	R3	nxDS0 in E1 MLPPP access (RFE87309)	Committed	7x50	9.0	R1
9.0	R3	MSS for Hpol(QoS enhancements)	Committed	7x50	9.0	R1
9.0	R3	Mcast replication on sub-interfaces (ESM IPoE, IES & VPRN). Only "PPP multicast replication on HSMDA-2" for BT	Committed	7x50	9.0	R3
9.0	R3	Facility MEP support within MEF SLM (Synthetic Loss Measurement)	Committed	7x50	9.0	R3
9.0	R3	Vport stats	Committed	7x50	9.0	R3
9.0	R3	SFM4 for 7-slot and 12-slot ESS & SR chassis - PTP work	Committed	7x50	9.0	R3
9.0	R3	PTP IEEE1588v2 master, slave	Committed	7x50	9.0	R4
9.0	R3	IOM soft reset for HS-MDA2	Committed	7x50	9.0	R4
9.0	R3	SFM4 for 12-slot ESS & SR chassis to support all IOMs and IMMs	Committed	7x50	9.0	R4
9.0	R3	RFE 94001: Egress PE shouldn't reply - traceroute	Committed	7x50	7X50_70R10 7	
9.0	R3	RFE 104309: CPU Util over 1 & 5 min intervals	Committed	7x50	7x50_70R15 7	
9.0	R3	RFE 107684: allow FC option for ping	Committed	7x50	7x50_70R17 7	
9.0	R3	RFE 102687: Raise trap - addr change in Ipipe	Committed	7x50	7x50_70R19 7	
9.0	R3	RFE 77633: Decoding of CMM failure frames	Committed	7x50	7x50_80R1	
9.0	R3	RFE 67002: Missing Cleared Alarm Trap for DDM	Committed	7x50	7x50_80R4	
9.0	R3	RFE 91135: Increase flexibility - Event Throttling	Committed	7x50	7x50_80R4 7x	

9.0	R3	RFE 105119: CPM-1/2 co-existing with CPM-3	Committed	7x50	7x50_80R7	
9.0	R3	RFE 107397: Respond with exact outgoing interface	Committed	7x50	7x50_80R7 7x	
9.0	R3	RFE 105338: Warn. msg on BFD sessions	Committed	7x50	7x50_90R4	
9.0	R3	RFE 110312: AES payload encrypt. required	Committed	7x50	7x50_90R4	
9.0	R3	9.0 R3 RFEs - OAM	Committed	7x50		
9.0	R3	SAP-2-SAP Connection	Committed	7x50		
9.0	R3	ATT Delete unused service	Committed	7x50		
9.0	R3	RFE 85491: Use of AIS reception - fault notificatn	Committed	7x50		
9.0	R3	HSMDAv2 Configurable Burst Thresholds	Committed	7x50		
9.0	R3	MME: LM4.0.1 Support	Committed	9471 MME	LM4.0.1	
9.0	R3	MME: Netconf Support	Committed	9471 MME	LM4.0.1	
9.0	R3	MME support for Warning Message Delivery - new SBc interface	Committed	9471 MME	LM4.0.1	
9.0	R3	MME Support for Location Based Services - new SLs and SLg interfaces	Committed	9471 MME	LM4.0.1	
9.0	R3	MME Support for Multimedia Broadcast/Multicast Service (MBMS or eMBMS)	Committed	9471 MME	LM4.0.1	
9.0	R3	MME Support for Enhanced CALEA Functionality - exposing the X1_1 and X2 interfaces	Committed	9471 MME	LM4.0.1	
9.0	R3	MME High Performance MME OAM Blade - Molene2 based	Committed	9471 MME	LM4.0.1	
9.0	R3	MME Support for MIF and MAF Blade Commonality with SGSN	Committed	9471 MME	LM4.0.1	
9.0	R3	OS9GNI-P24E Support (OS9000E devices)	Committed	OmniSwitch	6.4.4	
9.0	R3	CPE Test Head Enhancements - AOS 6.6.2 R01	Committed	OmniSwitch	6.6.2 R01	
9.0	R3	SFTP client support in SAM for OMNI Backup/Restore and Software upgrade	Committed	OmniSwitch		
9.0	R4	7210 SAD-D 6F4T ETR support	Committed	7210	3.0	R5
9.0	R5	7210 VPLS Management Interface SAS-D	Committed	7210	3.0	R5
9.0	R5	G.8032 - Ethernet Ring Protection SAS-D 3.0 R5	Committed	7210	3.0	R5
9.0	R5	IGMP Snooping SAS D 3.0 R5	Committed	7210	3.0	R5
9.0	R5	IP Interface over VPLS for L2 Uplinks SAS-M 3.0 R5	Committed	7210	3.0	R5
9.0	R5	MSTP on SAS-E / SAS-D	Committed	7210	3.0	R5
9.0	R5	PBB for E-Pipe on SAS-M / SAS-X	Committed	7210	3.0	R5

9.0	R5	PortLoopback without– MAC Swap SAS-E / SAS-D	Committed	7210	3.0	R5
9.0	R5	SyncE on SAS-D 3.0 R5	Committed	7210	3.0	R5
9.0	R5	Y.1731 for SAS D 3.0 R5	Committed	7210	3.0	R5
9.0	R5	Port Threshold in LAG for SAS-E, SAS-D	Committed	7210	3.0	R5
9.0	R5	IGMP Snooping 10 GigMDA (SAS-M)	Committed	7210	3.0	R5
9.0	R5	7210 3.0 R6 Support	Committed	7210	3.0	R6
9.0	R5	Configurable Period for Writing A/C records into Flash 4.0 R1	Committed	7210	4.0	R1
9.0	R5	7210 4.0 R1 Equipment Support	Committed	7210	4.0	R1
9.0	R5	IP MTU support on L3 interfaces on SAS-M, SAS-X 4.0 R1	Committed	7210	4.0	R1
9.0	R5	Multi-chassis LAG on SAS-M, X	Committed	7210	4.0	R1
9.0	R5	Pseudowire redundancy in VPLS on SAS-M Ntwk Mode 4.0 R1	Committed	7210	4.0	R1
9.0	R5	Transit SAPs (*.* saps) all nodes	Committed	7210	4.0	R1
9.0	R5	7705 SAR-M support @ 4.0 level	Committed	7705	5.0	R1
9.0	R5	5780 DSC 4.0 R1 Equipment Management Support	Committed	5780 DSC	4.0	R1
9.0	R5	Distributed Architecture Simplification	Committed	5780 DSC	4.0	R1
9.0	R5	Active-Active Geo-redundancy	Committed	5780 DSC	4.0	R1
9.0	R5	GGSN: Radius	Committed	7750 MG	3.0	R1
9.0	R5	PGW/GGSN: Gn/S8 (S8 as per list)	Committed	7750 MG	3.0	R5
9.0	R5	GGSN: Gy/Ro Online Charging	Committed	7750 MG	3.0	R5
9.0	R5	KPI/KCI Threshold configuration - policy based	Committed	7750 MG	3.0	R7
9.0	R5	System Performance - Primary KPIs	Committed	7750 MG	3.1	R1
9.0	R5	Disconnect (RADIUS changes)	Committed	7750 MG	3.1	R1
9.0	R5	S2, S6b, PMIP Interfaces	Committed	7750 MG	3.1	R1
9.0	R5	MG: 3.1 R1 S-GW and 3.1 R1 P-GW Node Support	Committed	7750 MG	3.1	R1
9.0	R5	ISA AA Support	Committed	7750 MG	3.1	R1
9.0	R5	RFE 103014: DTS 108533 AT&T CBS Oversubscription	Committed	7x50	8.0	R10
9.0	R5	5 minute maximum throughput stats in per aa-sub accounting (holdover from 8.0)	Committed	7x50	9.0	R1
9.0	R5	ETH-CFM Redundancy - part 2	Committed	7x50	9.0	R1
9.0	R5	Multi-segment PW routing (aka dynamic MS-PW)	Committed	7x50	9.0	R3
9.0	R5	3-port 40GE (possibly oversubscribed) Magma-based QSFP IMM	Committed	7x50	9.0	R4
9.0	R5	OC-3/12 POS ROHS MDAs (16-port only)	Committed	7x50	9.0	R4
9.0	R5	OC-48 POS ROHS MDAs (4-port only)	Committed	7x50	9.0	R4

9.0	R5	CLI command to display active card alarms (RFE 65299)	Committed	7x50	9.0	R4
9.0	R5	Virtual MEP on VSI	Committed	7x50	9.0	R4
9.0	R5	Per-sub CPU protection for HTTP-redirect (WiFi access)	Committed	7x50	9.0	R4
9.0	R5	APS Annex B	Committed	7x50	9.0	R4
9.0	R5	QPPB	Committed	7x50	9.0	R4
9.0	R5	BGP Add Path	Committed	7x50	9.0	R4
9.0	R5	mVPN fast-failover (Source redundancy)	Committed	7x50	9.0	R4
9.0	R5	IPv6 FIB scale increase to 512k+	Committed	7x50	9.0	R4
9.0	R5	Inter-AS option C and option B/C with multi-hop eBGP and RSVP-TE support, respectively	Committed	7x50	9.0	R4
9.0	R5	Allow exclusion of RSVP LSP name from BGP next-hop resolution (RFE 88796)	Committed	7x50	9.0	R4
9.0	R5	PW Scale 128k	Committed	7x50	9.0	R4
9.0	R5	Extensions to ATM Aware QoS for Broadband Network Gateway	Committed	7x50	9.0	R4
9.0	R5	VPRN indirection for Edge resilience (aka. Edge Prefix Independent Convergence -	Committed	7x50	9.0	R4
9.0	R5	ESM on ATM interfaces: PPPoA and PPPoEoA (Routed CO)	Committed	7x50	9.0	R4
9.0	R5	NAT: RTSP ALGs	Committed	7x50	9.0	R4
9.0	R5	PPPoE dual-chassis redundancy with MCS	Committed	7x50	9.0	R4
9.0	R5	SRRP enhancements for PPPoE redundancy	Committed	7x50	9.0	R4
9.0	R5	ASM data MDT	Committed	7x50	9.0	R4
9.0	R5	Increasing Primary Path Associations with Bypass LSP	Committed	7x50	9.0	R4
9.0	R5	IS-IS lockless design	Committed	7x50	9.0	R4
9.0	R5	MMRP scaling increase: 40K	Committed	7x50	9.0	R4
9.0	R5	ISSU support for maintenance releases	Committed	7x50	9.0	R4
9.0	R5	multi-area adj OSPF (RFC 5185) - support for OSPFv3 (DTS 107137)	Committed	7x50	9.0	R4
9.0	R5	Down on CRC	Committed	7x50	9.0	R4
9.0	R5	Link LDP Hello Adjacency Tracking with BFD for LDP-FRR	Committed	7x50	9.0	R4
9.0	R5	Business prefix transits	Committed	7x50	9.0	R4
9.0	R5	AA on SR-c12	Committed	7x50	9.0	R4
9.0	R5	WAN-PHY support for 12-port 10GE Magma IMMs (RFE 100388)	Committed	7x50	9.0	R4
9.0	R5	RSVP-TE inter-area manual bypass with XRO	Committed	7x50	9.0	R4

9.0	R5	RFE 115017: Add support for x-online-host mode	Committed	7x50	9.0	R4
9.0	R5	RFE 115546: BSX: Add support for "http-match-all-requests" mode for HTTP expression matching	Committed	7x50	9.0	R4
9.0	R5	16-port OC-3 and 4-port OC-12 ATM ROHS MDAs	Committed	7x50	9.0	R6
9.0	R5	ESM support on Magma IMMs	Committed	7x50	9.0	R6
9.0	R5	IOM3-XP with MultiCore CPU	Committed	7x50	9.0	R6
9.0	R5	Multicore CPU-based 48-port GE SFP IMM	Committed	7x50	9.0	R6
9.0	R5	Multicore CPU-based 48-port GE TX IMM	Committed	7x50	9.0	R6
9.0	R5	V-port aggregate-rate-limit for Ethernet BNG	Committed	7x50	9.0	R6
9.0	R5	Support IPv6 on AA	Committed	7x50	9.0	R6
9.0	R5	HTTP 404 Re-direct AQP Action	Committed	7x50	9.0	R6
9.0	R5	HTTP Proxy	Committed	7x50	9.0	R6
9.0	R5	Service Label per next-hop for framed routes	Committed	7x50	9.0	R6
9.0	R5	RFE 118964: PBB EPIPE using Two SAPs and BVPLS (Three point EPIPE with Local Switching)	Committed	7x50	9.0	R6
9.0	R5	RFE 84859: increase default (vc-label-ttl) to 255	Committed	7x50	7x50_60R18 7	
9.0	R5	RFE 101800: Add the mfg assembly number to output	Committed	7x50	7x50_61R17 7	
9.0	R5	RFE 74962: TLL security check for Telnet SSH	Committed	7x50	7x50_70R14 7	
9.0	R5	RFE 62641: sub-sec ethernet hold timer values	Committed	7x50	7x50_80R1	
9.0	R5	RFE 81284: Generate detailed trap	Committed	7x50	7x50_80R1	
9.0	R5	RFE 96190: CLI cmd to show all lldp neighbors	Committed	7x50	7x50_80R10	
9.0	R5	RFE 111569: Periodic MAC notification	Committed	7x50	7x50_80R10 7	
9.0	R5	RFE 83726: CLI to log the cause of a LAG bounce	Committed	7x50	7x50_80R10 7	
9.0	R5	RFE 67711: Make TCP disconnect configurable	Committed	7x50	7x50_80R4	
9.0	R5	RFE 74908: Send GARP on outer VLAN saps	Committed	7x50	7x50_80R5 SA	
9.0	R5	RFE 101290: Add SNMP support for tree trace output	Committed	7x50	7x50_90R1	
9.0	R5	RFE 107448: Different PPPoE session-ids	Committed	7x50	7x50_90R1	
9.0	R5	RFE 104621: Linking IP Interface	Committed	7x50	7x50_90R4	

9.0	R5	RFE 105302: Add support for VPORT stats	Committed	7x50	7x50_90R4	
9.0	R5	RFE 92592: LSP manual path switchover command	Committed	7x50	7x50_90R4	
9.0	R5	RFE 95039: 4 byte AS error handling	Committed	7x50	7x50_90R4	
9.0	R5	RFE 97496: LSP stat feature in chassis mode B	Committed	7x50	7x50_90R4	
9.0	R5	Increase SAM SDP binding limits	Committed	7x50		
9.0	R5	Sub. QoS overrides and aggregate rate limit work	Committed	7x50		
9.0	R5	MVPN IPMSI SNMP MIB Tables	Committed	7x50		
9.0	R5	Configuration Rollback Start/Finish alarm Support	Committed	7x50		
9.0	R5	5620 SAM support of eNB LA4.0 (eNB models, release, backward compatibility and upgrade path)	Committed	9412 eNodeB	LA4.0	
9.0	R5	eNodeB Licensing improvement	Committed	9412 eNodeB	LA4.0	
9.0	R5	support of eUTRAN sharing (LTE RAN)	Committed	9412 eNodeB	LA4.0	
9.0	R5	support of IRAT ANR for eNB	Committed	9412 eNodeB	LA4.0	
9.0	R5	Wireless Equipment management improvement	Committed	9412 eNodeB	LA4.0	
9.0	R5	support of eNB Counter selection	Committed	9412 eNodeB	LA4.0	
9.0	R5	scalability tests - improvement for eNB	Committed	9412 eNodeB	LA4.0	
9.0	R5	SAM configuration evolution	Committed	9412 eNodeB	LA4.0	
9.0	R5	NEM cross-launch over IPv6	Committed	9412 eNodeB	LA4.0	
9.0	R5	5620 SAM framework for data transfer toward WPS	Committed	9412 eNodeB	LA4.0	
9.0	R5	5620 SAM to SAM rehoming procedure evolution	Committed	9412 eNodeB	LA4.0	
9.0	R5	5620 SAM support of sBBU configuration (TDD modem)	Committed	9412 eNodeB	TLA3	
9.0	R5	Support of eNB TLA4.0.0 (eNB release and backward compatibility)	Committed	9412 eNodeB	TLA4	
9.0	R5	MME: Granular Security Permissions	Committed	9471 MME	LM 4.0.2	MNCL 1
9.0	R5	MME: Custom QoS Parameter Mapping from EPS to Release 99	Committed	9471 MME	LM 4.0.2	MNCL 1
9.0	R5	MME: LM 4.0.2 Support	Committed	9471 MME	LM 4.0.2	
9.0	R5	MME: Bulk Provisioning	Committed	9471 MME	LM 4.0.2	
9.0	R5	MME: EMS Based Pool Support	Committed	9471 MME	LM 4.0.2	
9.0	R5	MME: EMS Based Load Balancing	Committed	9471 MME	LM 4.0.2	
9.0	R5	9500 R3.02 Element Support	Committed	9500 MPR	3.02	
9.0	R5	9500 R3.01 Element Support	Committed	9500 MPR	3.01	
9.0	R5	Service in Service: Auto Discovery	Committed	9500 MPR	3.00	
9.0	R5	Path Management - N x (1+0)	Committed	9500 MPR	3.00	

9.0	R5	Auto Tunnel Creation - N x (1+0)	Committed	9500 MPR	3.00	
9.0	R5	Common LOS Alarm	Committed	9500 MPR	3.00	
9.0	R5	9500 Time and Date Configuration	Committed	9500 MPR	2.02+	
9.0	R5	QoS Configuration	Committed	9500 MPR	3.02	
9.0	R5	Power Levels PM	Committed	9500 MPR	3.00	
9.0	R5	L2 Radio LAG Management	Committed	9500 MPR	3.01	
9.0	R5	L2 Radio LAG Configuration	Committed	9500 MPR	3.02	
9.0	R5	SDH Channelization	Committed	9500 MPR	3.01	
9.0	R5	Virtual Protection (VCL) Links	Committed	9500 MPR	3.01	
9.0	R5	XPIC (1+1 Redundancy)	Committed	9500 MPR	3.01	
9.0	R5	SDH 1+1 Support	Committed	9500 MPR	3.01	
9.0	R5	dot1Q VLAN Service (E2E)	Committed	9500 MPR	3.00	
9.0	R5	OmniSwitch 6900/AOS 7.2.1 R01 Node Equipment Support Only	Committed	OmniSwitch	7.1.1	
9.0	R5	OmniSwitch 10K/AOS 7.1.1 Node & AOS Support - LLDP support	Committed	OmniSwitch	7.1.1	
9.0	R5	OmniSwitch 6900/AOS 7.1.1 Node & AOS Support- LLDP Support	Committed	OmniSwitch	7.1.1	
9.0	R5	Ethernet Port Configuration on OS10k	Committed	OmniSwitch	7.1.1 R01	
9.0	R5	Ethernet Port Configuration on OS6900	Committed	OmniSwitch	7.2.1 R01	
9.0	R5	OmniSwitch 10K/AOS 7.1.1 R01 Equipment Support Only	Committed	OmniSwitch	7.7.1	
9.0	R5	DCR-597816: CFM options on VLAN service topology map	Committed	OmniSwitch		
9.0	R7	24v DC Pwr Supply Support	Committed	7210	3.0	R6
9.0	R7	Synch-E with SSM support	Committed	7210	3.0	R6
9.0	R7	L3 VPRNs (BGP) SAS M/X Network mode 4.0 R1	Committed	7210	4.0	R1
9.0	R7	Port Loop Back with MAC SWAP (enables RFC 2544, no traffic generation)	Committed	7210	4.0	R1
9.0	R7	Split Horizon Group support (Port and Service Level)	Committed	7210	4.0	R1
9.0	R7	Enhanced Network Ingress QoS Support for MPLS Packets using LDP Tunnels	Committed	7210	4.0	R1
9.0	R7	IGMP Snooping v3 support on L2 Uplinks (SAS-M)	Committed	7210	4.0	R1
9.0	R7	Storing of SAA results into flash	Stretch	7210	4.0	R1
9.0	R7	MC G.8032 - Multi Chassis Support on SAS-M	Stretch	7210	4.0	R2
9.0	R7	SNMP support for Dying Gasp (SAS-D)	Stretch	7210	4.0	R2
9.0	R7	SAR-18 Fan tray Led on Alarm Module	Candidate	7705	4.0	R3
9.0	R7	New 2.5G SAR-8 backplane	Committed	7705	4.0	R3
9.0	R7	Spanning Tree Protocol (STP) with Mgmt VPLS	Stretch	7705	4.0	R4

9.0	R7	DCR 602168 - Configurable Alarm Input (Normally Open vs Normally Closed) on Auxillary Alarm Module	Candidate	7705	4.0	R5
9.0	R7	OADM (Optical Add Drop Mux)	Candidate	7705	5.0	R1
9.0	R7	DCR 611034: Least Fill Bandwidth option for RSVP	Candidate	7705	5.0	R1
9.0	R7	IEEE 1588v2 on IES interfaces	Candidate	7705	5.0	R1
9.0	R7	SAR-18 IP Interface Scaling	Candidate	7705	5.0	R1
9.0	R7	IP Interface Statistics (DCR 600656)	Candidate	7705	5.0	R1
9.0	R7	SAR-M "Clear MDA / Hot Insert"	Candidate	7705	5.0	R1
9.0	R7	8p GE (WP3) MDA	Committed	7705	5.0	R1
9.0	R7	SAR-M Platform	Committed	7705	5.0	R1
9.0	R7	SAR-ME Platform	Committed	7705	5.0	R1
9.0	R7	SAR-M GPON Module	Committed	7705	5.0	R1
9.0	R7	SAR-M xDSL Module	Committed	7705	5.0	R1
9.0	R7	SAR-M DCM Module	Committed	7705	5.0	R1
9.0	R7	HDLC H-Pipes (on DS3, ASAP, SDI MDAs & SAR-M)	Committed	7705	5.0	R1
9.0	R7	ATM VT	Committed	7705	5.0	R1
9.0	R7	E3 ATM	Committed	7705	5.0	R1
9.0	R7	N:1 N>1 ATM PW	Committed	7705	5.0	R1
9.0	R7	TWAMP	Committed	7705	5.0	R1
9.0	R7	eBGP PE-CE	Committed	7705	5.0	R1
9.0	R7	Power injector card	Committed	7705	5.0	R1
9.0	R7	OSFP GR helper	Committed	7705	5.0	R1
9.0	R7	I-Pipes on channelized OC3	Committed	7705	5.0	R1
9.0	R7	I-pipes SAP-2-SAP	Committed	7705	5.0	R1
9.0	R7	increased 2P ch OC3 cards (to DS1) per SAR-8/18	Committed	7705	5.0	R1
9.0	R7	Frame Relay F-Pipes (on DS3, ASAP, SDI MDAs & SAR-M)	Stretch	7705	5.0	R1
9.0	R7	I-pipes on F/R ports	Stretch	7705	5.0	R1
9.0	R7	sub-rate X.21	Stretch	7705	5.0	R1
9.0	R7	4800bps X.21 and R232 on the SDI card	Stretch	7705	5.0	R1
9.0	R7	600bps RS232 on the SDI card	Stretch	7705	5.0	R1
9.0	R7	SAR-8 V2 Chassis and FAM (-48V only)	Stretch	7705	5.0	R1
9.0	R7	SDI & E&M in SAR-18 (Qual activities)	Stretch	7705	5.0	R1
9.0	R7	IEEE1588 Transparent Clock	Candidate	7705	5.0	R2
9.0	R7	IEEE 1588 Time Of Day	Candidate	7705	5.0	R2
9.0	R7	OSPF on IES interfaces	Candidate	7705	5.0	R2
9.0	R7	PPP/FR encap on SDI to IP PW	Candidate	7705	5.0	R2
9.0	R7	FR/HDLC on channelized DS3	Candidate	7705	5.0	R2

9.0	R7	1p 10GE XMDA card for SAR-18	Committed	7705	5.0	R2
9.0	R7	SAR-M Fanless WITH 16 T1/E1, 7 GIGE, -48/+24 VDC	Committed	7705	5.0	R2
9.0	R7	SAR-M Fanless WITH 7 GIGE, -48/+24 VDC	Committed	7705	5.0	R2
9.0	R7	LAG on ACCESS	Stretch	7705	5.0	R2
9.0	R7	DS3/E3/OC3 C-pipes (CC & ch to DS1)	Stretch	7705	5.0	R2
9.0	R7	cHDLC encap into I-Pipes (T1/E1)	Stretch	7705	5.0	R2
9.0	R7	Differential Clock Recovery on SAR-M	Stretch	7705	5.0	R2
9.0	R7	Voice & Tele-protection MDA	Candidate	7705	5.0	R3
9.0	R7	Packet Microwave Card	Candidate	7705	5.0	R3
9.0	R7	VRF scaling on sar-18 (from 16 to 32)	Candidate	7705	5.0	R3
9.0	R7	Ethernet (VPLS) "down when looped"	Candidate	7705	5.0	R3
9.0	R7	10p 1GE XMDA card for SAR-18	Stretch	7705	5.0	R3
9.0	R7	Add 7705 4.0 to Autoconfig	Candidate	7705		
9.0	R7	Extensions for c-pipes	Committed	7705		
9.0	R7	Auto tunnel enhancements	Committed	7705		
9.0	R7	ATM and Network Policy (4.0 -> 5.0)	Stretch	7705		
9.0	R7	Scale increase: 128K SAPs	Candidate	7x50	9.0	R1
9.0	R7	Increased scale to support 2K queue groups per system/IOM	Candidate	7x50	9.0	R1
9.0	R7	RFE 61737: Support Filter Matching	Candidate	7x50	7x50_90R5	
9.0	R7	Support for AOS 7.2.1 R02 for OS6900 and OS10k at a 9.0 R5 level.	Committed	OmniSwitch	7.2.1	R02
NMS Features						
9.0	R1	MAC and IPv6 Filter Policies	Committed	7705	4.0	R1
9.0	R1	Other Polcies for 7705	Committed	7705	4.0	R1
9.0	R1	Ipipe Enhancements	Committed	7705	4.0	R1
9.0	R1	Ethernet Port CFM Loopback	Committed	7705	4.0	R1
9.0	R1	Displayed Card Names	Committed	7705	4.0	R1
9.0	R1	Ethernet OAM Thresholds	Committed	7705	4.0	R1
9.0	R1	OAM Ping and Trace Results	Committed	7705	4.0	R1
9.0	R1	BGP Enhancements	Committed	7705	4.0	R1
9.0	R1	Security permissions (MG changes)	Committed	7750 MG		
9.0	R1	MG Peer Stat Aggregation	Committed	7750 MG		
9.0	R1	horizontal integration protocol - enabler for CDMA or GSM horizontal integration with SAM	Committed		LA3.0	
9.0	R1	Map Move by Association	Committed			
9.0	R1	Security Improvements incl. Service Deletion Confirmation	Committed			
9.0	R1	Improvements of SAP management	Committed			

9.0	R1	SAR support for channelization card workflows	Committed			
9.0	R1	Attach # of user sessions to a user group	Committed			
9.0	R1	Auto database reinstantiation	Committed			
9.0	R1	Manager specific controlled parameters configurati	Committed	7x50		
9.0	R1	Composite Service Mgt - Configure with Flat Map	Committed	7x50		
9.0	R1	Customer level Apdex Thresholds	Committed	7x50		
9.0	R1	Config Forms: Add a lock, unlock and close buttons to forms	Committed			
9.0	R1	Config Forms: Undock to forms	Committed			
9.0	R1	Config Forms: Element Search	Committed			
9.0	R1	New Frameworks: Collapsible panel	Committed			
9.0	R1	New Frameworks: Configs and lists in same form	Committed			
9.0	R1	New Frameworks: Editable table/config	Committed			
9.0	R1	Trees: Add Component tree to config forms	Committed			
9.0	R1	Component Tree (left pane), Config Form (right pane) for Services	Committed			
9.0	R1	Attribute indication on collapsible panel and tabs	Committed			
9.0	R1	Add mouse over to trees	Committed			
9.0	R1	Column Ordering for users	Committed			
9.0	R1	Map Endpoint Enhancement	Committed			
9.0	R1	Bearer List Query Filtering	Committed			
9.0	R1	5620 SAM Supervision	Committed			
9.0	R1	Convert key generation to ASLM for SAM	Committed			
9.0	R1	Document 3rd party Tool list	Committed			
9.0	R1	Oracle 11	Committed			
9.0	R1	SSO Proxy and LSM Session Management	Committed			
9.0	R1	x86 Blade Perf Comparison (HP blade vs Oracle rack mount)	Committed			
9.0	R1	9.0 R1 Licensing	Committed			
9.0	R1	Automated SSL/SSO Configs for Upgrades	Committed			
9.0	R1	LogViewer enhancements	Committed			
9.0	R1	Beta key support	Committed			
9.0	R1	Include Network Element Type in Alarms	Committed			

9.0	R2	5620 SAM-CDMA Horizontal Integration	Committed		LA3.0	
9.0	R3	Bearer Stats UI - Post Filtering	Committed	7750 MG		
9.0	R3	Confirmation needed for ACL filter re-ordering	Committed	7x50		
9.0	R3	Compression of backup files via tar/gzip	Committed			
9.0	R3	Display of PEM and fan trays in the equipment tree	Committed			
9.0	R3	Reply function to SAM text messages	Committed			
9.0	R3	Ethernet layer added to bulk change	Committed			
9.0	R3	Usability Improvements of the GUI builder, script manager and bulk updates	Committed			
9.0	R3	Switch user account without stopping the SAM client	Committed			
9.0	R3	Clarify the scope of Override Tabs	Committed			
9.0	R3	Enhanced Channelization Support	Committed			
9.0	R3	Document applicable alarms for eNodeB	Committed			
9.0	R3	Document applicable alarms for MME	Committed			
9.0	R3	Gather applicable node alarm info automatically	Committed			
9.0	R3	Security DCRs	Committed			
9.0	R3	9.0R3 Licensing	Committed			
9.0	R3	Alarm Statistics in SAM-S	Committed			
9.0	R5	TCAs for mib-based performance stats	Committed			
9.0	R5	Alarm Correlation - correlated alarm has highest s	Committed			
9.0	R5	Alarm Correlation - per alarm window enable/disabl	Committed			
9.0	R5	Shared MEG id	Committed	7x50		
9.0	R5	Testsuite for comp svc/seg svc	Committed			
9.0	R5	Path search - enhance svc tunnel selection	Committed	7x50		
9.0	R5	5670 RAM DCP Summarization Support	Committed			
9.0	R5	AA Support on Mixed Mode on 7450	Committed	7x50		
9.0	R5	Generic Object Attributes	Committed			
9.0	R5	Consolidated view of historical and active alarms	Committed			
9.0	R5	Filter on Topology Group	Committed			
9.0	R5	Expand only link groups with highlights or troubles	Committed			
9.0	R5	Increase max. number of discovery rules	Committed			

9.0	R5	Extend inactive user search to users not having logged in yet	Committed			
9.0	R5	Simplify NE full resync procedure	Committed			
9.0	R5	Show composite service id in service list	Committed			
9.0	R5	Add Software and Boot version in Managed Equipment	Committed			
9.0	R5	Script Scheduling	Committed			
9.0	R5	Increase JMS Filter flexibility	Committed			
9.0	R5	Use logToFile For STM	Committed			
9.0	R5	Target to increase 9500 max counts to 12K	Committed			
9.0	R5	Target to increase 7210-SAS max counts to 12K	Committed			
9.0	R5	Target to increase max NEs to 18K	Committed			
9.0	R5	East-West Interface Licensing in 5620 SAM	Committed			
9.0	R5	Binding of scripts to service components	Committed			
9.0	R5	Extension of "create all channels" to APS and APS ports	Committed			
9.0	R5	Offer the "create all channels" option, even if some channels exist already	Committed			
9.0	R5	Script & Template Cascading	Committed			
9.0	R5	Composite Service Mgt - Alarms	Committed	7x50		
9.0	R5	GNE in the service picture	Committed			
9.0	R5	Tunnels for services	Committed			
9.0	R5	Service Scale	Committed			
9.0	R5	Network Resource Management	Committed			
9.0	R5	CFM Test, Add AccountingFile and ContinuouslyExecution	Committed	7x50	9.0	R1
9.0	R5	Use logToFile For Performance Stats	Committed			
9.0	R5	Infocenter for User Docs	Committed			
9.0	R5	Composite Service support in service navigator	Committed			
9.0	R5	Template Support for Attribute Indicator	Committed			
9.0	R5	Message for lists that don't autopopulate	Committed			
9.0	R5	New button model for config forms	Committed			
9.0	R5	Consolidate equipment window and NE property form	Committed			
9.0	R5	Internal Improvements 9.0R5	Committed			
9.0	R5	Component refresh - JBoss 5	Committed			
9.0	R5	9.0R5 Licensing	Committed			

9.0	R5	'Does Not Contain' filter option	Committed			
9.0	R5	Retain customized test attributes with re-generating tests	Committed			
9.0	R5	Shared Domain ID	Committed			
9.0	R5	Distribution Progress	Committed			
9.0	R5	Framework: Add support for radio buttons	Committed			
9.0	R5	Add Port Descr Column during SAP creation	Committed			
9.0	R5	Listing Access port missing state info	Committed			
9.0	R5	Target to increase Performance stats (1M)	Committed			
9.0	R5	Usage Based Billing	Committed			
9.0	R5	Integration of East-West interface into 5620 SAM	Committed			
9.0	R5	RAM Properties	Committed			
9.0	R5	Map Handling of Unmanaged NEs	Committed			
9.0	R7	MBH Static Support	Candidate			
9.0	R7	VPLS MC Traffic Management (QoS)	Stretch	7705	4.0	R2
9.0	R7	Reference single links with history	Candidate			
9.0	R7	GNE: LLDP & LLDP based Alarm Aggregation	Candidate			
9.0	R7	User Activity Logs Enhancements	Candidate			

Table 1: 9.0 Feature Planning

II. ORDERING INFORMATION

Sales Engineering Information

5620 SAM H/W PLATFORM sizing web tool link.

5620 SAM DVD-ROM Request link.

5620 SAM License Key link (supported on IE browser only).

5620 SAM Pricing Information link.

- New part numbers are added to the pricing book to support 7210 SAS-D network element and 5620 SAM-S option.
- Note that 7750 MDAs running in mixed mode on a 7450 will count as 7750 MDAs. 7450 MDAs running in mixed mode on a 7750 will count as 7450 MDAs.

Note that as of Release 7.0, Integrated Service Adapters no longer require a Premium license.

Note that if a customer reaches the limit of licensed Premium MDAs but still has spare Standard MDAs and wishes to add another Premium MDA, two standard MDAs will be counted.

5620 SAM Technical Support link.

5620 SAM Documentation link.

Licensing Information

The 7705 SAR-8 requires two license pools, one for the 7705 SAR-8 chassis count and one for the 7705 SAR-8 daughter card count. Each discovered 7705 SAR-8 chassis shall consume one 7705 SAR-8 chassis license; and each daughter card within a discovered 7705 SAR-8 shall consume one 7705 SAR-8 daughter card license. If either license pool is negative, no additional 7705 SAR-8 nodes can be managed.

The 7705 SAR-F requires a license pool, separate from those used for the 7705 SAR-8. The 7705 SAR-F license pool shall be handled similarly to the 7705 SAR-8 chassis license pool.

7210 SAS M & 7210 SAS MX[ETR] is supported as node based license. User has to buy separate license for SAS-M and SAS MX (ETR). It is to be noted that the license for SAS-MX is also shared with SAS-MX ETR. So if user has 5 SAS-MX licenses, one can manage 3 SAS-MX and 2 SAS-MX ETR or 1 SAS-MX and 4 SAS-MX ETR.

5620 SAM management of the 7x50 SR nodes is supported by licensing the quantity of the individual MDA cards. MDA cards fall into two licensing categories: Premium and Standard. Generally, any non-high-performance MDA cards are considered Standard. All IMM, High Speed MDA (HSMDA) and Extended Performance (XP) MDA cards are considered "Premium" with the exception of the following cards (starting in Release 7.0 R1):

- MDA 1-PT 10GE-XP XFP (m1_10gb_xp_xfp)
- MDA 10-PT 1GE-XP SFP (m10_1gb_xp_sfp)

Please note that in Releases from 9.0 R1 to 9.0 R4, the following two cards were incorrectly downgraded to "Standard" category:

- MDA 20-PT 1GE-XP SFP (mda_m20_1gb_xp_sfp)
- MDA 20-PT 1GE-XP TX (mda_m20_1gb_xp_tx)

As such, for 5620 SAM Releases 9.0 R1 through 9.0 R4 managing 20-PT-GE-XP MDA cards, the license manager will incorrectly display the counts for "Premium" and "Standard" categories on 7750 SR and 7450 ESS chassis. With no other license limitations present, 5620 SAM will continue to function even though the licence manager will display warnings. The issue is fixed in 5620 SAM Release 9.0 R5; the issue is tracked in PTS 617646.

7450 Mixed Mode
In SROS Release 8.0 and onwards 'Mixed Mode' capability was introduced on the 7450 ESS-6v, ESS-7 and ESS-12 platform. To enable 5620 SAM management of the IMM cards [L3BQ, L2HQ and L3HQ h/w RTU license types] on the 7450 ESS platform in 'Mixed Mode', 7750 Premium MDA license is required.

7750 Mixed Mode
In SROS Release 9.0, mixed mode feature support has been extended to the 7750 SRs so that IPv6 can be enabled on a 7750 SR chassis that supports only "Chassis mode B" without having to upgrade the entire chassis. According to this capability supported MDAs, IMMs belonging to 7750 SR chassis in "Chassis Mode C" could be used in 7750 SR chassis that supports only "Chassis Mode B". There is no licensing impact according to this mixed mode feature.

Support for Beta Keys

5620 SAM Release 9.0 will have specific keys for Beta Releases of 5620 SAM. Production keys will no longer work with Beta software. Beta keys are controlled by 5620 SAM Product Management. To apply for the 5620 SAM Beta Program, see your Alcatel-Lucent Account representative.

Convert Key Generation to ASLM for 5620 SAM

Alcatel-Lucent has retired AKG as a supported internal tool for key generation. As a result, 5620 SAM keys will be generated via ASLM as of Release 9.0 R1. This poses a process change for internal teams wishing to order license keys on behalf of their customers.

Oracle Ordering Information

When purchasing the 5620 SAM application, sufficient licenses must be acquired for the utilization of the Oracle product, which is embedded into the 5620 SAM Database software. The licenses required to operate the Oracle product are computed based on the number of CPUs in the server workstation on which the 5620 SAM Database component will operate.

The table below provides examples of the type and possible number of CPUs that can be included in the servers that Alcatel-Lucent recommends for the operation of 5620 SAM.

The additional Oracle licensing requirements can be computed by looking at the number of CPUs that are included in the Server workstation on which the 5620 SAM Database component is installed. When a 5620 SAM installation is redundant, these Oracle licensing requirements must be doubled.

Sun Server	Number of CPUs	Additional Oracle Licensing Requirements
SPARC Single-core CPU Platforms (mono-core)		

SunFire v440 Server	4	Additional licensing for 2 CPUs
SunFire v445 Server	4	Additional licensing for 2 CPUs
SPARC Dual-core CPU Platforms		
SunFire v490 Server	2 or 4	If 2 CPUs, additional licensing for 1 CPUs (dual-core) If 4 CPUs, additional licensing for 3 CPUs (dual-core)
SunFire v890 Server	Up to 8	If 2 CPUs, additional licensing for 1 CPUs (dual-core) If 4 CPUs, additional licensing for 3 CPUs (dual-core) If 6 CPUs, additional licensing for 5 CPUs (dual-core) If 8 CPUs, additional licensing for 7 CPUs (dual-core)
Solaris x86 Platforms		
SunFire x4100, x4200	2 dual-core CPUs	No additional licensing requirements
SunFire x4200	2 dual-core CPUs	No additional licensing requirements
SunFire x4600, x4440	2 or 4 multi-core CPUs	If 4 dual-core CPUs, additional licensing for 2 CPUs (mono-core) If 2 quad-core CPUs, additional licensing for 2 CPUs (mono-core) If 4 quad-core CPUs, additional licensing for 6 CPUs (mono-core)
SunFire x4600	Up to 8 multi-core CPUs	If 2 dual-core CPUs, no additional licensing requirements If 4 dual-core CPUs, additional licensing for 2 CPUs (mono-core) If 6 dual-core CPUs, additional licensing for 4 CPUs (mono-core) If 8 dual-core CPUs, additional licensing for 6 CPUs (mono-core)
SunFire x4170, x4270	Up to 2 multi-core CPUs	If 1 quad-core CPU, no additional licensing requirements If 2 quad-core CPUs, additional licensing for 2 CPUs (mono-core) If 1 hex-core CPU, additional licensing for 1 CPU (mono-core) If 2 hex-core CPUs, additional licensing for 4 CPUs (mono-core)

Table 2: Platform CPU and Oracle Equivalent

III. SCALE & ARCHITECTURE

Scalability Targets

Aggressive network growth targets, entry of 5620 SAM into new markets, latency, and increased product functionality and usage are driving capacity requirements upward.

The table below shows the scale achieved in 5620 SAM Release 9.0 R5 Beta.

Note that:

- These limits require particular hardware specifications and specific deployment architectures.
- Scale limits for network elements including GNEs, 7705s, and 7210s assume a maximum sustained trap rate of 40 traps/second.

The following table represents the scalability limits supported in 9.0 R5.

Criteria	**9.0 R5**
Maximum network elements (excluding GNE)	18,000
Maximum number of GNEs (assumes 10 interfaces per)	18,000
Combined GNE/network elements (assumes 10 interfaces per GNE max)	18,000/3000
Combined network elements/GNE (assumes 10 interfaces per GNE max)	18,000/3,000
Maximum number of managed MDAs containing:	25,000
Max 7250 network elements	2,500 (= 5,000 MDAs)
Max 7705 network elements	12,000 (= 12,000 MDAs)
Max 9500 network elements	12,000 (=12,000 MDAs)
Max 7210 network elements	12,000 (= 12,000 MDAs)
Max 1830 PSS-32/16	250
Max 1830 PSS-1	5000
Number of Optical Transport Services	6000 service, 1200 endpoints
Max OMNISwitch 6000 series (1 MDA equivalent to 1 chassis)	12,000 (15K 6250)
Max OMNISwitch 9000 series (1 MDA equivalent to 1 NI)	1,000
Maximum number of SAPs	6,000,000
Maximum number of Services	2 Million
Maximum number of LSPs	50,000
Concurrent Clients	
Max OSS Clients [HTTP, JMS1]	30
Max GUI Clients	150
OAM Tests (10 minute interval)	
Standard Tests (not simultaneous with Lightweight)	6,000

Lightweight Tests (not simultaneous with Standard)	
Accounting Based Tests (when saved in database)	50,000
Accounting Based Tests (when not saved in database)	200,000
Statistics (15 minute interval)	
Accounting Statistics	10,000,000
Performance Statistics	1,000,000
Combined Accounting/Performance	10,000,000/1,000,000
Alarms	
Outstanding Alarms	50,000
Maximum number of Alarms (equivalent to 1 month retention assuming 50,000 per day)	2,000,000

Table 3: Scaling Commitments & Targets for Release 9.0

Performance Targets

The following table represents the performance targets for 5620 SAM R9.0. Factors that may result in fluctuation of these targets include:

- 5620 SAM Server and 5620 SAM Database hardware platforms (faster platforms switch faster)
- Network Activity
- User/OSS Activity
- DB activity (i.e. database backups)
- Network size
- Latency

Performance Item Description	9.0 Performance Targets
5620 SAM Client GUI Performance	
Time to launch a 5620 SAM Client GUI	~30 seconds
Time to launch a 5620 SAM Client GUI configuration form	~2 seconds
Time to save a 5620 SAM Client GUI configuration form	~2 seconds
5620 SAM Server Performance	
Time to restart the 5620 SAM Server when managing the maximum number of devices	~10 minutes
Estimated time to resynchronize one new router in domain	<20 minutes (subject to size of new router)
5620 SAM DB Backup (without stats)	Up to 60 minutes (subject to network size)
5620 SAM DB Restore	~45 minutes
5620 SAM Server activity switch	<10 minutes
5620 SAM DB switchover (by invoking through the GUI)	<10 minutes
5620 SAM DB failover (manually invoked)	<20 minutes until complete recovery, including 5620 SAM Server restart
5620 SAM DB failover (automatic)	<20 minutes until complete recovery,

	including 5620 SAM Server restart
Recovery of standby 5620 SAM Database after failover (This assumes a workstation is available and properly configured before the recovery begins)	<75 minutes
5620 SAM-O Performance	
Number of services created per day by an OSS workflow for VLL Service type	Up to 25K per day (24 hours)
Average time to create 1 VLL service	~3.0 seconds
Average time to create 1 VPLS service (3 sites, 1 SAP/site)	~4.5 seconds
Average time to create 1 VPLS service (6 sites, 1 SAP/site, 30 circuits fully meshed)	~10 seconds
Average time to configure 100 VPLS Service on 3 Sites using one SAP	~16 minutes
Average time to add 1 IES interface to an existing service	~1.5 seconds
Average time to create 1 static route on a 7750 SR	~0.6 seconds
Average time to create 1 MAC ACL filter	~0.8 seconds
Average time to create 1 GRE SDP	~0.75 seconds
Average time to create 1 MPLS SDP	~1.0 seconds
Average time to create 1 MPLS path	~0.8 seconds
Upgrade Performance	
5620 SAM Client Upgrade	<10 minutes
5620 SAM Complex Upgrade (Server, Database, Auxiliaries) *Note*: The target includes the installation of the software on the existing servers and 5620 SAM database conversion. Solaris Installation/Upgrades, patching, pre/post-upgrade testing and file transfers are excluded from the target.	<6 hours
5620 SAM Upgrade Maximum Visibility Outage with 5620 SAM Redundant system *Note*: Provided proper planning and parallel execution procedures were followed.	<15 minutes

Table 4: R9.0 Performance Targets

Performance improvements

A number of enhancements have been put into 9.0R5 to improve performance in some targeted areas. Notable ones are as follows.

Improvements to JMS that have increased 5620 SAM's JMS message rates for durable clients considerably. These messages no longer go through the database, which reduces the processing cost on the DB as well as increasing the message throughput. See the 5620 SAM Planning Guide for rates.

5620 SAM uses asynchronous calls to multiple network elements. This improves handling of resyncs and discovery of many nodes in large networks.

SNMP GetBulk is used in certain areas for SR-based NEs to also improve resync times.

Oracle 11

5620 SAM Release 9.0 R1 included an Oracle upgrade (from 10G to 11G). The upgrade is transparent to the end user; the upgrade is handled by the 5620 SAM installation.

IV. FEATURE DESCRIPTIONS

NMS FEATURES

NMS Applications

GUI Frameworks

A number of fundamental frameworks have been developed for designers to improve the usability of the 5620 SAM GUI going forward. New items developed in 5620 SAM will use these options. There will be an ongoing effort in 2011 to move some legacy over as well. These efforts will be done on a case by case basis.

Collapsible Panel

Designers now have the option of adding a collapsible panel to a form. Collapsible panels are used to save space and reduce clutter. Often their use makes it possible to put more items on a single tab without forcing an unbearably long list to scroll. See diagram below:

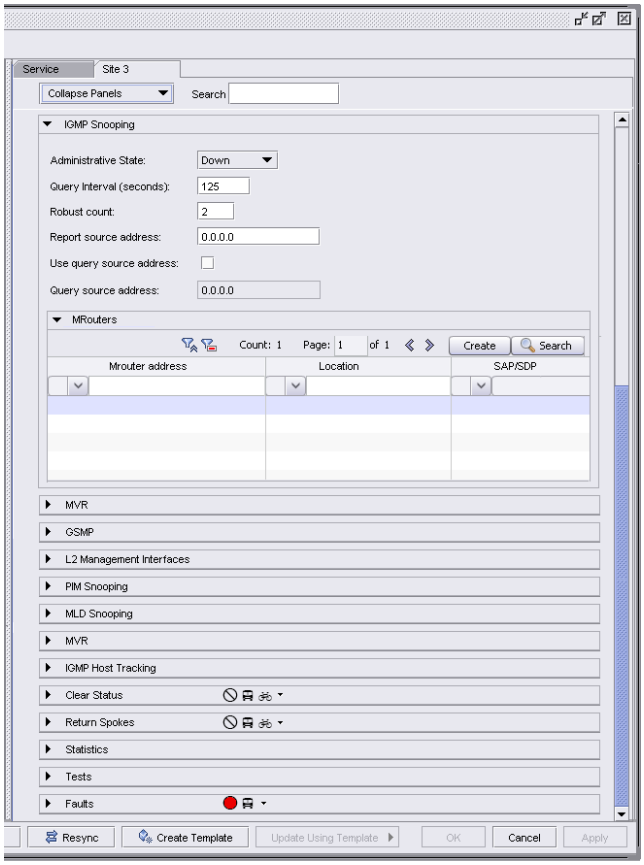


Figure 1: Collapsible Panel

Specific requirements include:

1. An operator must be able to “Open” and “Close” a collapsible panel
2. A designer must be able to specify the default (open or close)
3. May contain: configuration, lists, pictures, text, another collapsible panel, editable tables
4. A designer must be able to specify a label (default may be tab label)
5. Multiple panels shall be able to exist on a given tab.

All groups in 5620 SAM will appear in a collapsible panel in Release 9.0.

Editable Element Lists

Designers now have the option of adding an editable table to a config form. The target usage of this option would be in cases where there is a list of very straightforward elements to configure or read (for example: eNodeB). See sample diagram below.

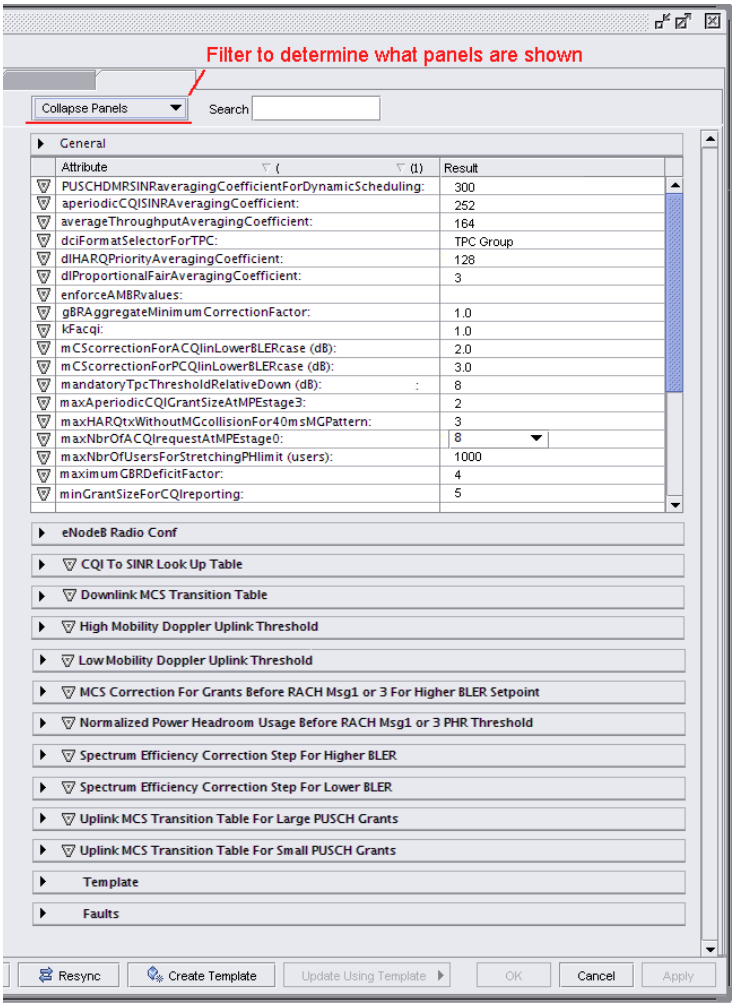


Figure 2: Sample Editable List

Specific requirements include:

1. Support all field types in the quick filter menu object.
2. Design controlled order of elements
3. Design controlled grouping of elements
4. Validation of the field
5. Mirrored properties
6. Display filters

Combine Configuration and List in a common tab

Designers now have the option of combining configuration and lists in a common tab. This will reduce the number of tabs.

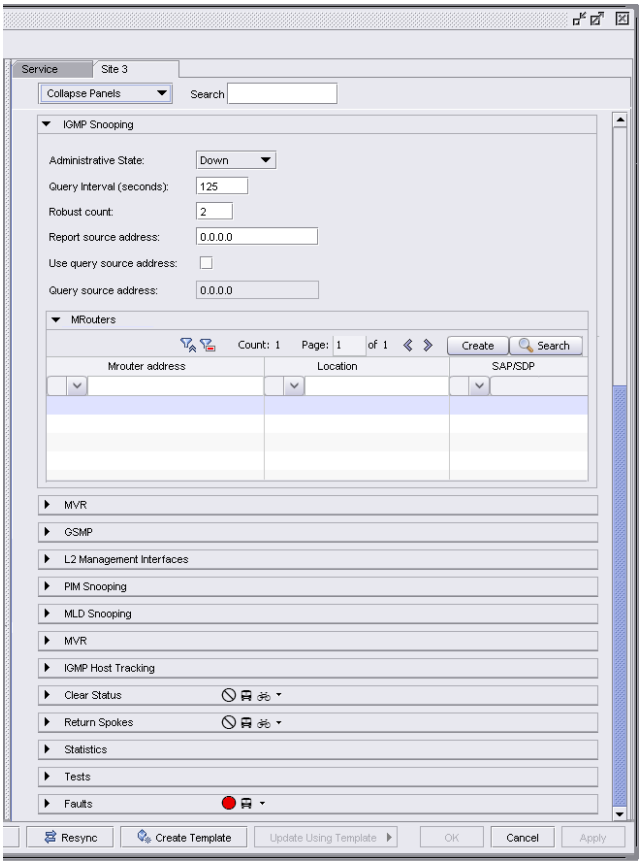


Figure 3: Config and List in Single Tab

Parameter Search

Release 9.0 offers an ability to search and navigate to specific parameters on a form.

Attribute Indication on Tabs and Collapsible Panels

5620 SAM configuration forms include visual indicators on configuration forms on tabs and collapsible panels. This is to assist in directing an operator's attention to a place in the form of most interest. Initial targets for indicators are:

- Mandatory attributes
- Attributes that have changed from their default value.

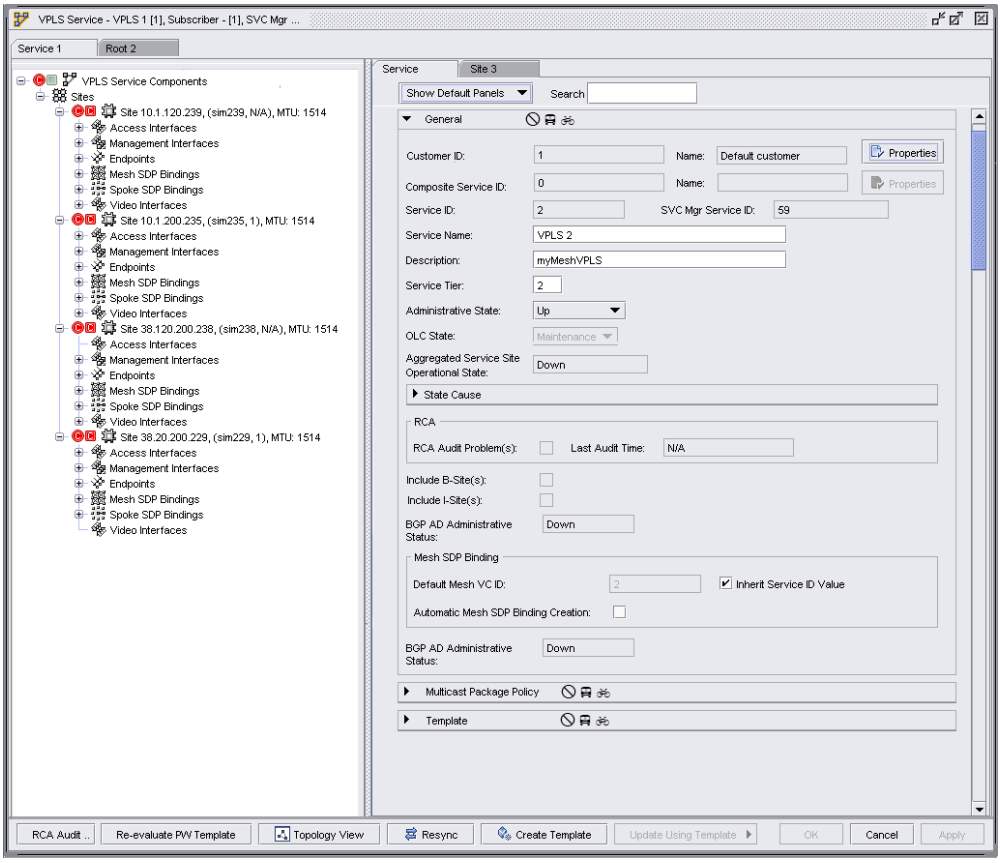
Release 9.0R5 adds support for attribute indicators in templates. Template developers can manipulate the usage in the GUI builder.

Component Tree Navigation

To improve service navigation and to reduce the number of windows Release 9.0 changes the component tree/configuration form paradigm.

The Component Tree has been moved outside the configuration form into its own pane on the left (see diagram below). As a user clicks on an object, the corresponding configuration form appears on the right hand side. If a user clicks on a container (i.e. Access Interfaces, Endpoints, etc), a list of all items in the container appears on the right. As a user clicks on another object, the right pane gets updated with the correct form.

In Release 9.0R5, composite services are also supported in the service navigators available in release 9.0R1.



Lock & Unlock of Service Configuration Forms

From time to time, as a user is navigating across various objects on a service component tree they may wish to lock one for reference later. A lock and unlock button will be available on the right pane for this. The flow is as follows:

- user clicks on SAP#1
- user locks SAP#1 configuration form
- user clicks on SAP#2
- a new tab appears in focus with the configuration form for SAP#2

Undocking Forms

From time to time, a user may wish to compare configuration forms. An undock button will be available on the right pane for this. The flow is as follows:

- user clicks on SAP#1
- user locks SAP#1 configuration form
- user clicks on SAP#2
- a new tab appears in focus with the configuration form for SAP#2
- user undocks the SAP#1 tab so this configuration form appears in its own window
- user has side by side comparison ability of SAP#1 and SAP#2

Customizing Columns and Ordering in Lists

5620 SAM offers the ability to drag columns as a way to customize column order. For lists with many columns this method is difficult to use. Release 9.0 offers the ability for a user to easily customize the columns that appear in a list and their order. This is available in all lists and the alarm window. To access this capability, right-click on a column and select “Column Display” from the contextual menu.

Consolidate Equipment Window and Network Element Property Form

As of 9.0R5 the Equipment Window (Application->Equipment Manager) and the Network Element properties forms have been merged so that the individual properties forms include all of the information. A Display tab has been added to the form to include the Shelf drawing where supported. This window is accessed via a number of ways in 5620 SAM. The most popular are by selecting in the equipment tree or map and choosing Properties from the right contextual menu.

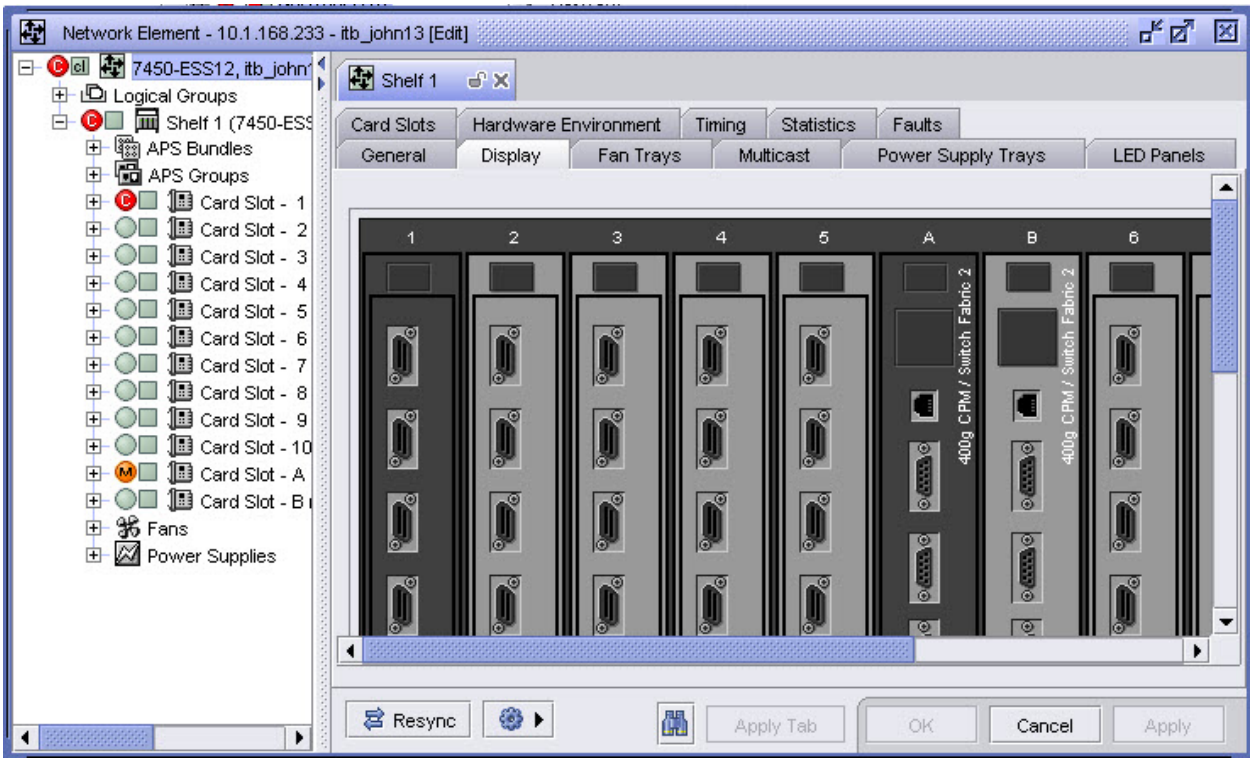


Figure 4: Revised Network Element Properties form

New Button Model for Config Forms

Many of the 5620 SAM config forms had limited real estate due to the volume and size of buttons. 5620 SAM 9.0R5 adds support for a drop down menu that contains the buttons. Forms are now much tidier and users can enjoy a better use of real estate.

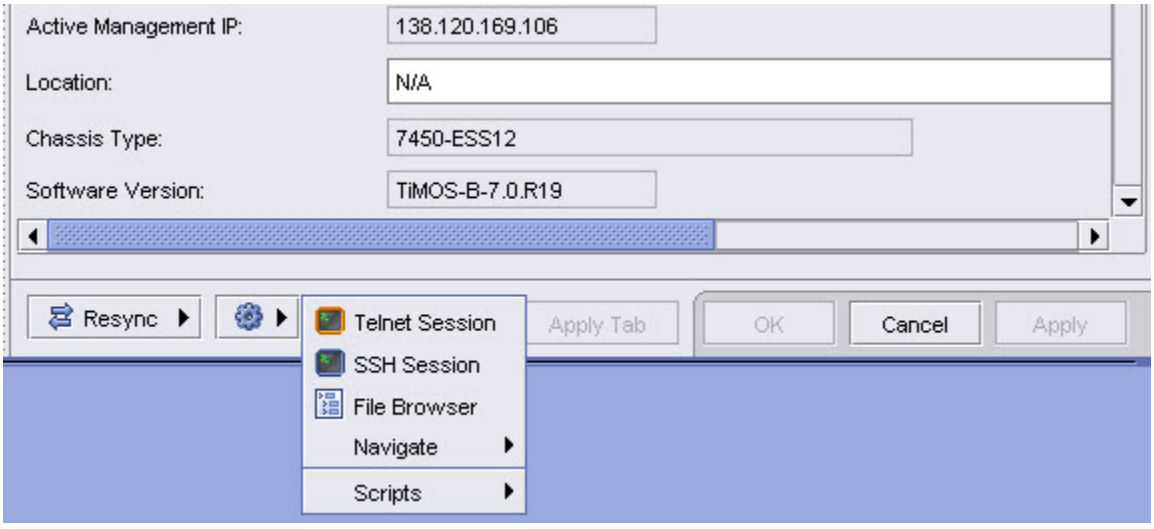


Figure 5: Button Drop Down Menu

Message for Lists that Don't Autopopulate

All list windows that don't autopopulate now contain the following message:

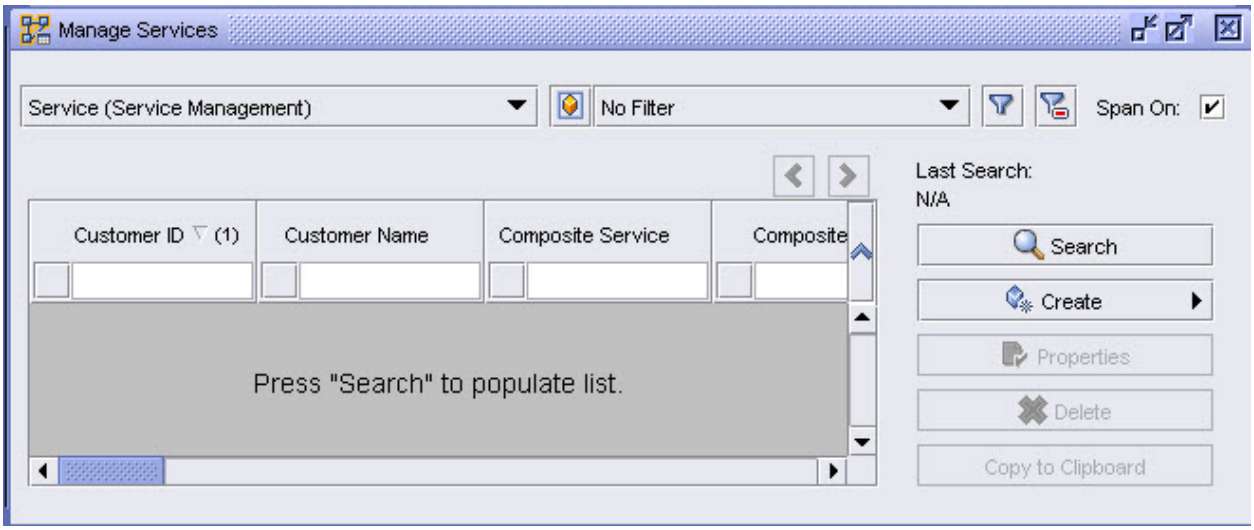


Figure 6: Auto populate warning

Additions to Listing Forms

A number of design changes requests submitted by customers to include additional columns in certain list forms were addressed in 9.0R5. These include:

- Listing access port missing state info
- Add port description column during SAP creation
- Add SW and Boot Version in Managed Equipment (DCR.499358 – R1)
- software versions on individual cards (R1)

In addition a "Does Not Contain" filtering option is available in 9.0R5.

Miscellaneous Usability Improvements

There are a number of additional improvements of the usability. This includes additional and adequately sized description fields.

A change of port types is allowed only, if there is no impact on Service Access Points, and vice versa, port descriptions are shown, when working on SAPs. This removes the need to jump from one screen to another, and avoids errors.

The tab names "Override" in scheduler policies are modified to "Override Policy Items" to clarify the scope of the override context.

In 9.0R5 the map has been extended with an option to expand only Link Groups with Highlights or Troubles.

Alarm Enhancements

Operators can select a number of alarms and get a consolidated list of current and historical alarms received in that timeframe (5 min. Before and after). This helps with troubleshooting by showing all alarms that may be related.

Since 9.0R3 an effort began to improve alarm documentation coverage. The alarmDetails.csv file contains an Applicable Nodes column. The intent is for that column to show all network elements that may raise this particular alarm. Adding content is an ongoing effort that will continue throughout the 9.0 release.

As of 9.0R5 the severity of an alarm is determined by the highest severity of all correlated alarms.

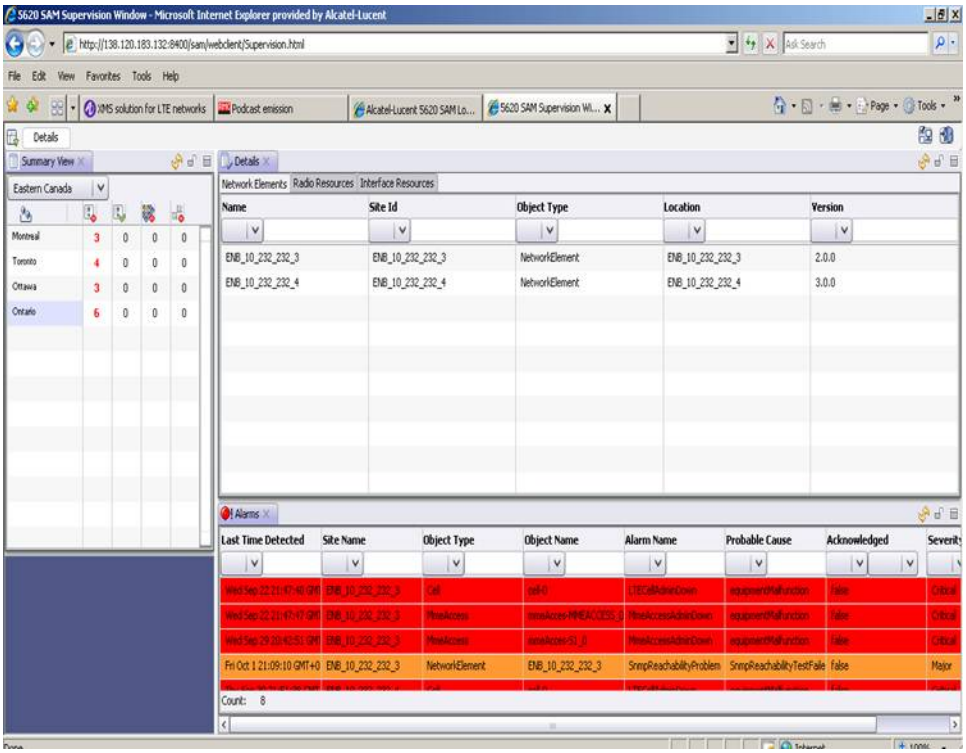
As of 9.0R5 users can enable/disable alarm correlation per alarm window. In previous releases this was done globally in the User Preferences for all alarm windows.

5620 SAM Supervision

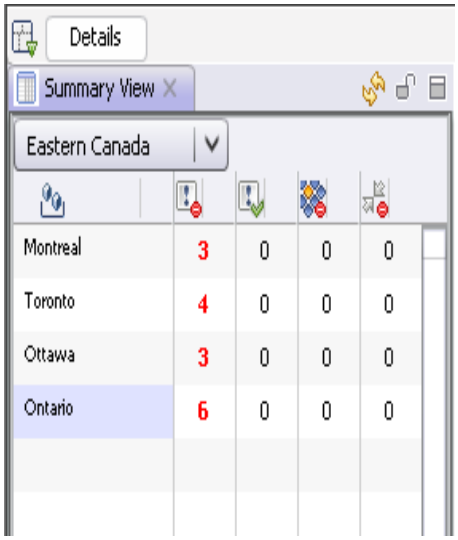
5620 SAM Supervision is a web-based tool that provides a user the ability to monitor alarms and object status of elements managed by a 5620 SAM.

The GUI has three components:

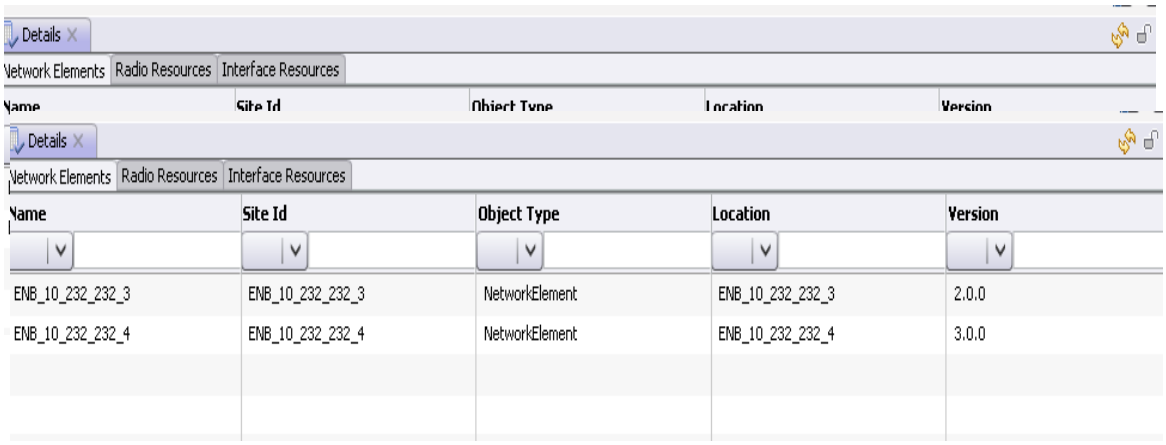
- Summary View
- Tabular View
- Detailed Alarm View



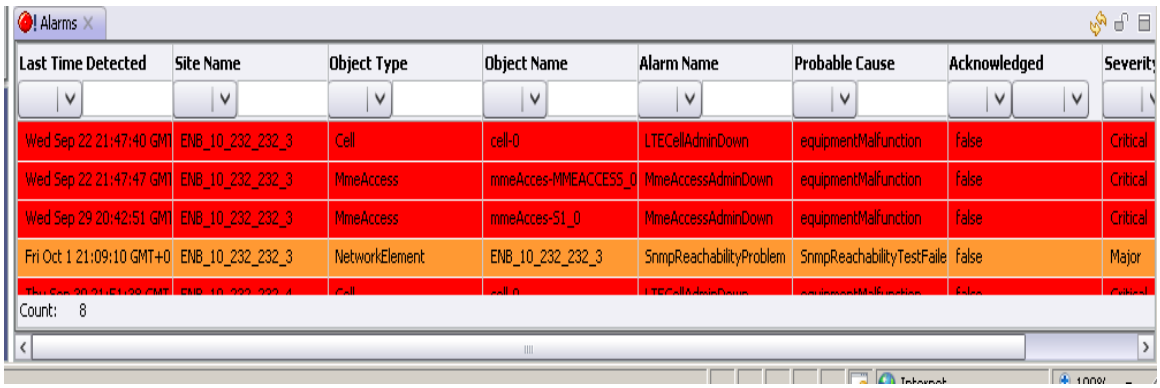
The Summary View allows supervising some key information of Groups of equipment, such as number of disabled cells, number of links disabled for the group. These Groups are configured in 5620 SAM.



The Tabular View displays the list of the equipments that are declared into a group and displays info such as operational state and administrative state.



The Detailed Alarm view displays the list of alarms for the list of the equipments that are declared into a group and displays the details of the alarms.



In addition of those supervision functions, the user can launch in context with single sign-on the associated properties form of the 5620 SAM in order to pass in one click from the supervision view to the classical 5620 SAM configuration view.

Horizontal Integration Protocol Support

5620 SAM introduces support for Horizontal Integration Protocol (HIP). This acts as an enabler for applications to integrate horizontally to 5620 SAM. Horizontal integration includes a common alarm feed (single northbound interface) and will provide the ability to navigate from 5620 SAM Supervision to the corresponding application's GUI interface.

Note: This is an enabler only. Requests to integrate applications into 5620 SAM must be presented to 5620 SAM Product Management as per normal feature request process as each requires additional test and possibly development work.

Display of PEM and fan trays in the equipment tree

PEM and fan trays are shown in the equipment tree as follows:

Shelf
|_Fans
| |_Fan Tray x
| |_Fan Tray y
| |_...
|_ Power Supplies
| |_Power Supply Tray a
| |_Power Supply Tray b
| |_...

1) Fan Tray node is shown in the format “Fan Tray - <ID>, <Fan speed>, <Fan device state>”
2) The Power Supply Tray is shown in the format “Power Supply Tray -<ID>, <assigned type>, <power entry module type>”
3) The power entry module attribute is not supported by all the nodes, hence this attribute will be visible to only those nodes which support power entry module.

They will be listed under "Shelf", the slot information will be added. If there are trays in different slots, they will be sorted according to the slot.

Reply Function to 5620 SAM Text Messages

The "Client ID" is added to text messages in 5620 SAM, in order to make sure that the sender of the text message can be uniquely identified. A reply function is taking that Client ID into account, so that an operator receiving a text message can send a response immediately.

Ethernet Layer Added to Bulk Change

LLDP Ethernet layer attributes are available now for bulk configuration change via the Bulk Change tool.

Script Management Enhancements

In 9.0R1 the following enhancements are available to the GUI builder:

- When renaming components that are target of an action, the GUI builder automatically updates the actions with the new name.
- The datetime property in scripting supports the definition of “Current Time”.
- In CLI scripts, the Result Manager displays results for the selected target. Before, the Result Manager displayed results for all targets regardless of the selection.

Release 9.0R5 adds support to schedule scripts. This includes all script types except Control Scripts. 5620 SAM retains a maximum of 100K scripts results in its database. Any individual result is truncated if it exceeds 4K.

Release 9.0R5 provides the ability for scripts to be bound to contextual menus of equipment and service components. This provides users to quickly launch scripts that they use often.

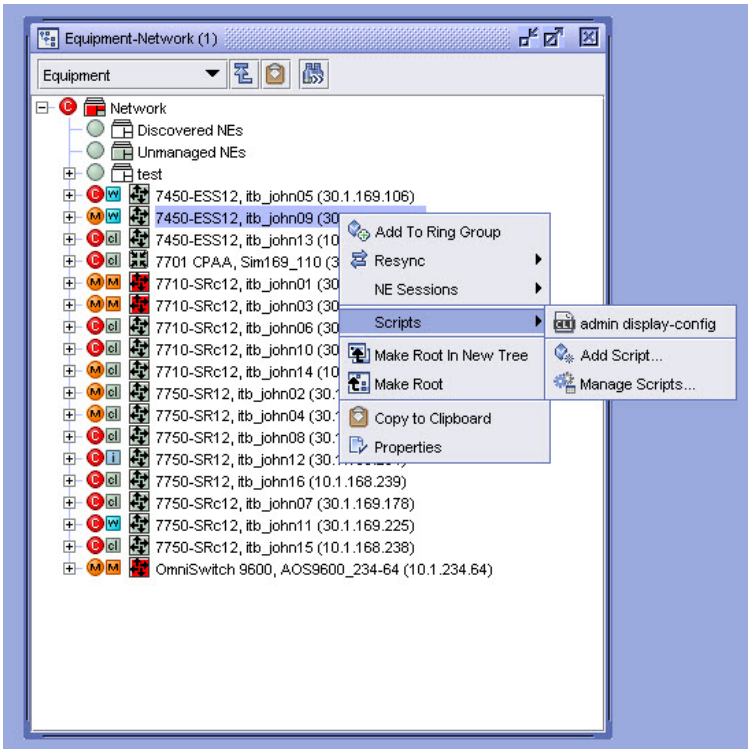


Figure 7: Script Binding

Release 9.0R5 substantially increases the power of 5620 SAM's Script Management with support for Cascading

Cascading provides an ability to produce a customize workflow for operators.

Capabilities include:

- A series of scripts/templates can be defined to run in sequence to deliver the operator workflow
- Flow control logic to be written to orchestrate scripts execution. For example: If a Script-X results in this, then run Script-Y, otherwise run Script-Z.
- Script execution results can be part of the input parameters for subsequent script invocations based on logic written into control scripts.
- User can be prompted for input during an execution of a workflow.
- Script Bundle manages scripts belonging to the same workflow.
- Script Bundle provides backup, installation and update management of scripts.

Common Use Cases that can be covered by this feature:

I want my operators to provision services via a standard, uniform, template and then run some diagnostics on the service.

I want to be able to chain configuration scripts together.

Contact your Alcatel-Lucent representative for more information or to obtain assistance creating these workflows.

Switch User Account without Stopping the 5620 SAM Client

A new menu item is added to the Application menu named "Switch User". When this menu option is selected, the existing GUI is closed and a new one is opened for the user to relogin.
The user can be switched quickly without the need to restart the client.

Enhanced Channelization Support

Enhanced Channelization Support now includes:

- Creation of DS0 sub-channels and the assignment of time slots.
- Consolidated view of the assignments of timeslots to DS0 sub-channels.

Confirmation for ACL Filter Re-ordering

When re-ordering the Ids of ACL filter entries, a confirmation pop-up dialog will be invoked before the change is implemented. This is consistent with most other windows/forms in 5620 SAM application.

Create All Channel Support for APS Groups (DCR.607110)

This feature extends the support of Create All channels to APS & MC-APS ports.

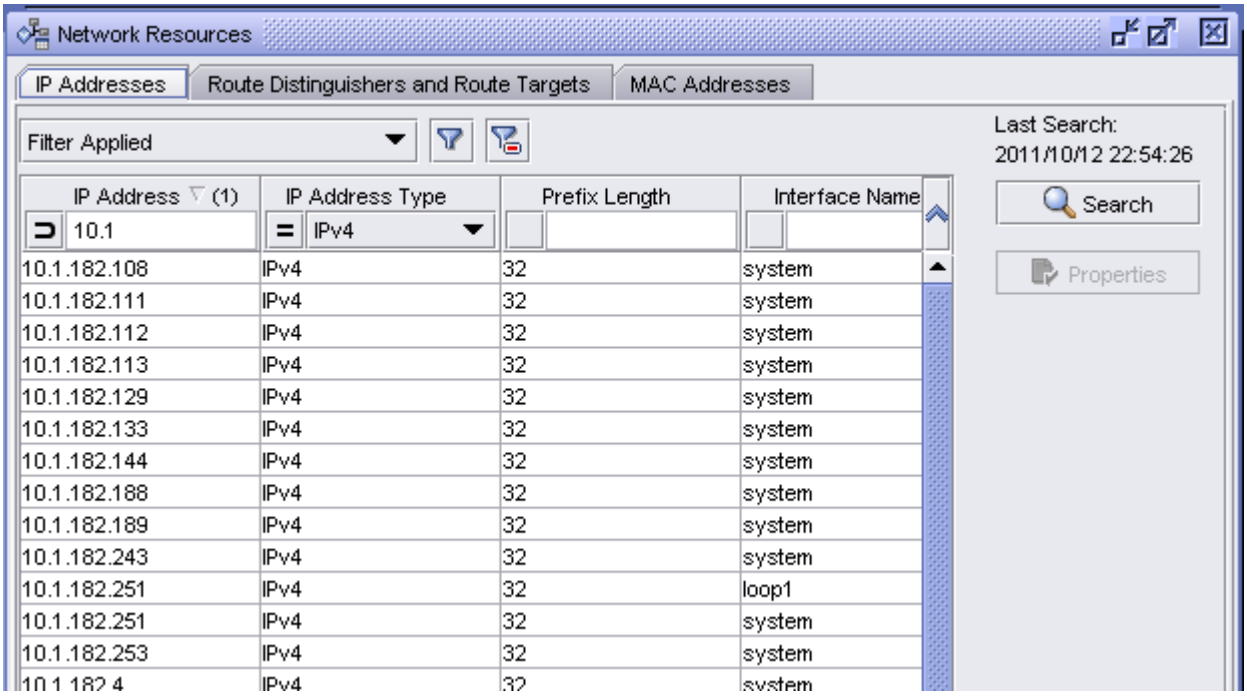
Update the Discovery Rules Limit to 25000 (DCR.614051)

This feature increases the maximum number of discovery rules in 5620 SAM from 5000 to 25000.

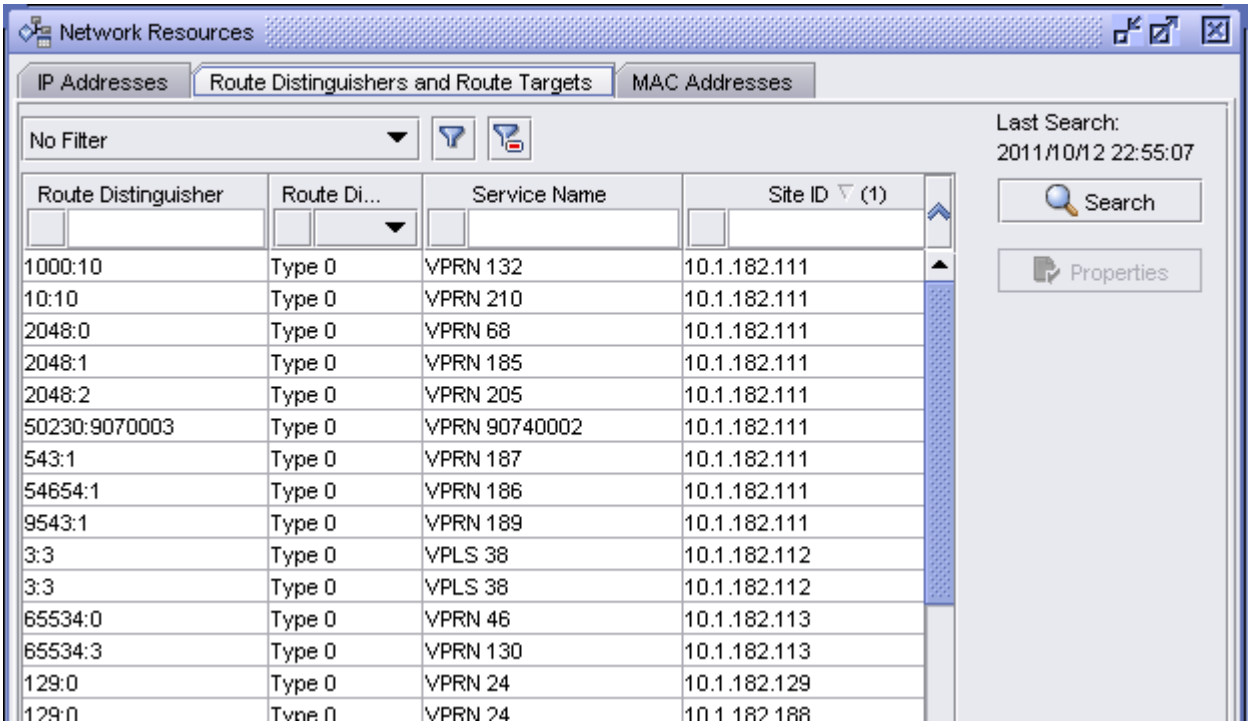
Network Resources Listing

SAM 90R5 provides a global listing/sorting of certain network resources. The objects could be IPv4/v6 addresses, RD, RT for both VPRN and BGP/BGP-AD VPLS, MAC addresses of ports, VPLS access interfaces, B-VPLS service instance, etc. The operator should be able to navigate back to the object(s) that is currently using the resource (by double-clicking on the selected entry). The application can be invoked from Tools->Network Resources.

For example, listing IPv4 addresses in the subnet 10.1.0.0/16



Another example, listing of RD based on type (Type 0 or 1).



For RT, the RT values hidden in the policy are also retrieved along with the possible static RT configuration for that Service Site. Also the import RT and export RT are display in different entry.

The owner of the Network Resources:
IP Address:

rtr.NetworkInterface
ies.L3AccessInterface
vprn.L3AccessInterface
vprn.NetworkInterface
vprn.IPsecInterface
vpls.L2ManagementInterface
ies.IPsecInterface
ies.SubscriberInterface
vprn.SubscriberInterface
service.RedundantInterface
service.VideoIfAttachment
rtr.MultiHomingInterface

RD and RT:
- VPRN Site
- B-VSI and VSI

MAC Address:
-Chassis
-Port
-SAP
- the PBB MAC for B-VSI

Result paging is a stretch goal and will not be supported in this release. Standard way of limit control is used. If the returned result reach the pre-defined limit (by default 50000 entries), an error is popped up to warn the user to refine the filter.

Also, for listing SAM operators can now, for a given object type; use the attributes of the children objects in searching criteria. To be specific, when open AccessInterface ListManager form, the operator can configure the filter based on IP address/prefix to find all interfaces that match the configured filter.

Unmanaged NE Group

As of 5620 SAM Release 9.0 R5, an Unmanaged NE group resides in the Physical and Tunnel topology maps to contain Unmanaged Network Elements. The purpose of this group is to accept newly discovered Unmanaged Network Elements until the user decides where they will best fit their topology layout. Unmanaged Network Elements can be dropped in and dragged out in the same manner as the Discovered NE group.

Unmanaged Network Elements that get created when unmanaging a Network Element are not be placed in into this group as the Unmanaged Network Element is replacing an existing Network Element and it is not typically a user's desire to modify the existing layout.

Existing Unmanaged Network Elements are not be placed into the Unmanaged NE group upon upgrade as this would modify existing topology layout.

There is a maximum of 500 network elements (managed or unmanaged) per topology group so this feature helps to contain this.

Platform Applications

x86 Blade Perf Comparison (HP blade vs. Oracle Rack Mount)

Comparison performance testing showed no significant performance differences between comparable Oracle Rack Mount Servers and HP Blade Servers.

For more information, please refer to the *5620 SAM Planning Guide*.

Auto Database Reinstantiation

During 5620 SAM Server install, there is an option for

1) Automatic Re-instantiation (either on or off (default)) for _DB failover only_.

2) A delay time before kicking off the auto-reinstantiation (the default 60 minutes)

These parameters can be reconfigured at any time by re-running the server installer [‘config’ option].

On the 5620 SAM GUI Client, the three parameters are shown on the System Information form as read-only:

1) "Auto Re-instantiation Enabled"

2) "Delay Time"

3) "Next Auto Standby Reinstantiation Attempt Time"

After a database failure and the 5620 SAM server is back online, the auto re-instantiate delay timer starts and the Standby Re-instantiation State will be set to Pending. Once that time has expired, 5620 SAM will determine if it can connect to the standby DB proxy. Then the following happens:

IF 5620 SAM can connect to the standby DB proxy, it will initiate a re-instantiation. Once the re-instantiation is complete, it will be tagged as such. However, if the re-instantiation fails, it will be tagged as Failed and will not be attempted again.

ELSE, if 5620 SAM can't connect to the standby DB proxy, then the Standby Re-instantiation State will be set to Failed, the timer is re-started, and 5620 SAM will try again at the end of the next delay time. The 5620 SAM will continue to try to connect to the standby DB proxy at the end of each interval. Once 5620 SAM can connect to the standby DB proxy, an auto re-instantiation is launched. Once the re-instantiation is complete, it will be tagged as such. However, if the re-instantiation fails, it will be tagged as Failed and will not be attempted again.

If a manual re-instantiation is In Progress, the auto-reinstantiation will not be launched and the "Next Auto-Standby Re-instantiation Launch Time" will be cleared in the GUI. While an auto-reinstantiation is In Progress, the manual Re-instantiate the Standby button in the 5620 SAM GUI will be disabled.

An automatic standby DB re-instantiation will NOT be triggered:

Following a 5620 SAM DB installation or upgrade, an auto re-instantiation will not be launched. This feature is for DB failovers only.

A DB archivelog gap on the standby will not cause an auto re-instantiation.

Shutting down the standby DB or server and re-starting it again, will not cause an auto re-instantiation

A server or DB switchover will not cause an auto re-instantiation.

There is no 5620 SAM-O support.

Security DCRs

The security enhancements within the Oracle database include the following:

- The minimum allowed sqlnet logon version will be set to 10 or higher;
- Monitoring of DBMS access control bypass will be enabled;
- PUBLIC access to restricted packages will be removed; and,
- Oracle minimum object auditing will be enabled.

Security Improvements

The provided improvements of security include a minimum number of characters for the user name, the ability of the security administrator to force a user to change his password at next log-in.

Furthermore, the risk of accidental deletion of services will be reduced by assigning a service priority (low, medium or high). While the handling of services with a low service priority is exactly as it was so far, ensuring that there is no impact on current provisioning procedures unless really wanted, services can be explicitly protected.

When an operator wants to delete a set of services including a service of priority “medium” or “high”, it is required to confirm the deletion by typing in the highest priority level. This ensures that the operator does not just blindly tick the confirmation box, but has to check the priority level of the services about to be deleted and to confirm awareness of the implications. Services of protection level “high” can be removed only by operators with a specific access right. This prohibits unintended removal of business-critical services.

Search for Users Not Logged in Yet (DCR.610672)

The feature includes users who did not yet login to the system at all in the search for inactive users. It is shown for how many days they were inactive for all users matching the search criteria.

Automated SSL/SSO Configs for Upgrades

When a 5620 SAM server/client is installed, the set of parameters that are needed to configure SSL/SSO will be collected through the installer software and stored in a data file that will be backed-up and restored across software upgrades.

If, in moving from one release to another, additional changes to information are required, the information will be collected through the installer, and the data file will be updated. The data file

would then be used by the installer post-upgrade to re-instantiate SSL/SSO configuration on 5620 SAM server. The end-user will not need to go through the process of reconfiguration across an upgrade.

To make 5620 SAM more secure, the installer has only two options: enable SSL for all communication channels between 5620 SAM components; or disable SSL for all channels. This includes the interface between 5620 SAM-O and OSI applications. Individual channel configuration for SSL is unsupported starting from Release 9.0 R1.

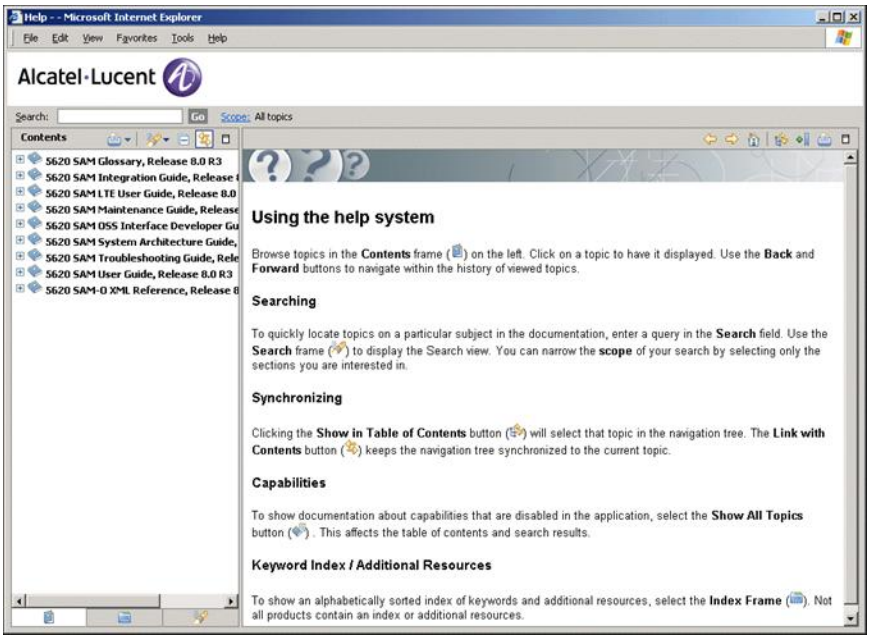
If, prior to Release 9.0 R1, the system configuration had only selected channels enabled for SSL, the installer for subsequent 9.0 Rloads will overwrite the option by enabling or disabling all channels for SSL as specified by the user.

Infocenter for User Documentation

5620 SAM will move to an Infocenter paradigm for user documentation in Release 9.0 R5. Infocenters allow operators to:

- Import their choice of 5620 SAM docs
- Import their own custom docs, links, videos
- Search across all docs

The Info-center is triggered in the same way the current documentation is. A user selects Help from the main menu in 5620 SAM.



Compression of Backup Files via tar/gzip

From the Database Manager Configuration form, users can now enable the compression the 5620 SAM database. Based on the selection, the backup files will be compressed using tar and gzip. Only the compressed files will be kept. Upon restoration, the files will be restored to their original format before starting the restore process.

Use logToFile for Performance Statistics

5620 SAM-O interface provides two methods to retrieve statistical data from the network: registerLogToFile and findToFile. registerLogToFile method is recommended to maintain an up-to-date view of statistics; and, findToFile method is recommended for infrequent statistics queries. In 5620 SAM Release 9.0 R5, registerLogToFile is now extended to support Performance Statistics.

The accounting and performance statistics export can generate a large number of files that consume disk space. Two parameters control file management based on the statistics type: file retention and file rollover times. The minimum value can be set to 5 minutes and the maximum to 600; the default value is 15 minutes. The file retention and rollover times can be configured by users using Administration->System Preferences configuration form.

Please note, since the original configuration parameter "timeToKeepFile" in the nms-server.xml file is deprecated and not used, users will have to adjust the parameters manually (if necessary) from the System Preferences configuration form after an upgrade from releases prior to Release 9.0 R5. Starting from 9.0 R5, both configuration parameters will be maintained across upgrades.

TCAs for MIB-Based Performance Statistics

Network operators typically ask the following questions about their networks:

- Which links in my network are reaching a specific % capacity based on real traffic?
- Which links in my network have an excessive traffic drop relative to my overall traffic?
- Which links in my network have an excessive error rate based on my overall traffic?

Starting from 5620 SAM Release 9.0 R5, network operators can setup TCA Policies to raise alarms based on rules with thresholds set on any mib-based performance statistics and on Server Performance statistics. Depending on the conditions, users can proactively be notified before network congestion or a critical event might occur.

5620 SAM can monitor Performance Statistics using two algorithms: threshold crossing based on absolute values; and, threshold crossing using values from previous collection interval (relative thresholds).

For example, when a network operator is interested in an alarm when traffic capacity reaches 80Mps, an algorithm based on absolute values is used. When the network operator is interested in an alarm when traffic capacity changes by 10% from the previous statistics interval, an algorithm based on relative thresholds is used. In a TCA Policy, users can create rules using either a single algorithm or both.

To illustrate the calculation of a threshold crossing based on absolute values, the following example can be demonstrated. An alarm can be raised based on the following condition.

If (counterA @ T1) > 80, raise an alarm,
Where,
counterA: mib-based statistics counter, like Received Total Octets Periodic;
T1: is the collection interval.

To illustrate the calculation of a threshold crossing based on relative values, the following example can be demonstrated. An alarm can be raised based on the following condition:

If ([(counterA @ T2) – (counterA @ T1)] / (counterA @ T1)) * 100 > 10, raise an alarm,
Where,
counterA: mib-based statistics counter, like Received Total Octets Periodic;
T1: is the collection interval at a specific collection time
T2: is the collection interval at the collection time right after T1.

To accommodate a condition for relative thresholds where the previous statistics counter value is zero or the change in the value is too small to be of significance to the user, the user can set "Delta Tolerance" parameter as a squelch mechanism to suppress unnecessary alarms.

For example, let's consider a physical port with 1 GB traffic capacity. Let's also assume that the user is interested in notification when the traffic profile changes by more than 10%. In addition, let's assume that the traffic profile is observed according to the following.

Note: for illustration purposes in this example, statistics counters are represented in units of rate. However, the actual statistics counters might use different units.

(counterA @ T1) = 10kbps
(counterA @ T2) = 20kbps

[(counterA @ T2) – (counterA @ T1)] / (counterA @ T1) * 100 > 10, raise an alarm

[20kbps – 10kbps] / 10kbps * 100 = 100 > 10%

A TCA alarm will be raised since the traffic change was observed to be 100% more relatively to the previous interval. If the user were to decide that the traffic change is insignificant until traffic reaches at least 1000kbps capacity, the user can set "Delta Tolerance" parameter to 1000kbps to suppress the generation of the TCA alarm.

For common network objects, 5620 SAM provides pre-configured TCA policies. Port Utilization TCA Policy is an example of pre-configured policy. Port Utilization TCA Policy can monitor %utilization, %drop and %error thresholds. Users can setup specific rules for each type of statistic to generate alarms.

Custom TCA Policies are used to monitor any other mib-based performance statistics.

To setup Custom TCA Policies, TCA Profiles need to be created first where users can specify the statistics counters with mathematical operations to be performed on the counters. Then, TCA Profiles are used within specific TCA Policies, either custom or pre-configured.

When the threshold values within TCA Policies are set too low for a large number of network objects, 5620 SAM might raise too many TCA alarms. The raised alarms might overflow the existing alarms. A configuration parameter exists within System Preferences to control the rate of alarms raised by TCA monitoring mechanism. If the system raises alarms at a rate greater than the configured system preference, 5620 SAM will stop the alarm generation and notify the user of too many TCA alarms. Threshold crossing monitoring will resume at the next interval.

TCA Policies can be setup independent of the Performance Statistics Collection Policies. However, for the threshold crossing monitoring to work, the user has to enable related statistics for the monitored objects.

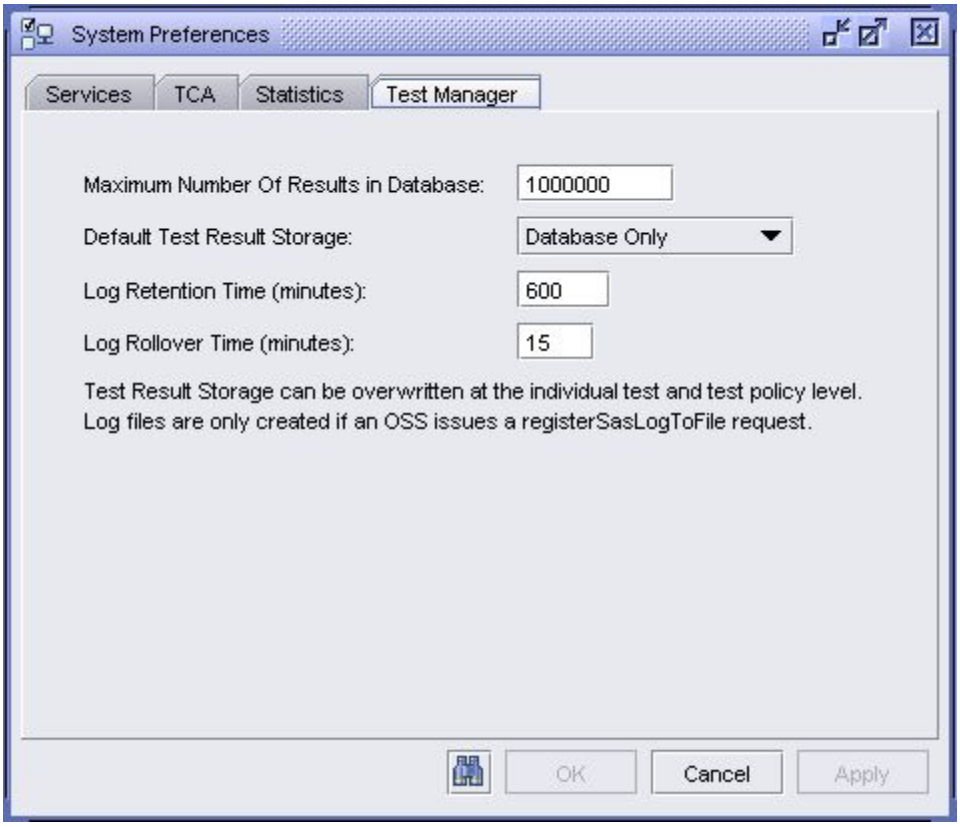
FN2717 logToFile for STM Results

To increase the rate of test results to be read from the NE's, SAM offers the option to write the directly results to text files. With SAM 90R5, SAM operators are able to select one the following options per test suite or per individual test:

1. Log to file
2. Log to database
3. Log to both

The options are available via OSSI and GUI.

The default option can be defined using Administration->System Preferences



Log to file is only applicable for tests and test suites with accounting files. For tests and testsuites without accounting files, the only applicable value is Log to Database.

The behaviour of STM Log to File feature is based on the existing Stats Log to File function. That means the test results for all test executed from an NE are stored in the files specifically for that NE. The logfile has the same format and information as the find to file.

The directory and the number of workers can be configured using nms-server.xml config file.

Increase JMS Filtering Flexibility

In Release 9.0R5 a new topic is added for JMS subscribers to register to that provides increased filtering opportunity upon subscription for OSS' to help reduce the number of messages being sent from the SAM server to the OSS. Prior to 9.0R5 elements found in the header were the only ones 'filterable".

See the 5620 SAM OSS Developer's Guide for more information.

NODAL FEATURES

7x50 Support

7x50 Mixed-Mode Chassis Support Phase 2

In Release 8.0 support for a new capability was introduced on the 7450 ESS-7 and ESS-12 platform to support 7750 (SR) functionality through the support of 7750 IOM3-XP and MDAs or 7750 IMMs. This provides 7450 customer greater flexibility in the services they can offer namely a seamless transition to scalable IP services within existing 7450 footprints.

In 9.0, mixed mode is being extended to the 7750 so that IPv6 can be enabled on a 7750 chassis in chassis mode B without having to upgrade the entire chassis. This is done by selectively upgrading only the slots with network ports and those ports requiring IPv6 support to IOM3-XPs or IMMs.

Target Applications
There are a large number of customers with 7750 system populated with a mixture of IOM1, 2 and 3, upgrading these systems to replace all IOM1s so that the chassis mode can be changed to mode C or higher is cost prohibitive.

The intent of this feature is to use the mixed mode mechanism to allow 7750 chassis to be selectively upgraded with IOM3-XPs or IMMs to allow certain features (namely IPv6) to be supported on a 7750 chassis without upgrading the entire chassis to support a new level. In Release 9.0 the only feature to be supported is IPv6 under mixed mode.

7750 Mixed Mode
The primary goal of this feature is to use the mixed mode mechanism to allow 7750 chassis to be selectively upgraded with IOM3-XPs or IMMs to allow certain features (namely IPv6) to be supported on a 7750 chassis without upgrading the entire chassis to support a new level.

When the mixed mode state is enabled on a 7750 chassis then IPv6 can be configured without replacing existing IOM1s or changing the chassis mode level for the system. However all IPv6 interfaces will restricted to ports on the 7750 IOM3-XPs or IMMs.

Basic Constraints
- In order to place a chassis into mixed mode all network interfaces must be on IOM3-XP and associated MDAs or IMMs
- The MDAs must match the IOM type (i.e. 7750 MDAs/MDA-XPs with 7750 IOM3-XPs & 77450 MDAs/MDA-XPs with 7450 IOM3-XPs)
- IPv6 support is the feature supported via this mechanism in 9.0
- All access interfaces with IPv6 interface may only reside on slots with an IOM3-XP or IMM

Hardware Support
This feature should be supported on all existing and future CFM/CPM. Only 7750 IOM3 and MDAs or IMMs will be supported in a 7450 (Not supported on ESS-6)

Note: Mixed mode is not applicable to the 7750 SR-1, 7450 ESS-1, 7710 SR-c4, 7710 SR-c12, 7750 SR-c4 or 7750 SR-c12

7750 MDA support in a 7450 mixed mode chassis
An additional part of this feature in 9.0 is to add support for additional 7750 MDAs in a 7450 chassis running in mixed mode. These should include:
- Any remaining Ethernet MDAs
- POS (SONET/SDH) MDAs
  - 7750 - 16/8 x OC-3c/OC-12c/STM-1c/STM-4c POS MDA
  - 7750 – 2/4 x OC-48c/STM-16c POS MDA
  - 7750 – 1x OC-192c/STM-64c POS MDA (SR, IR & LR optics)
- ATM MDAs
  - 7750 - 4 x OC-3c/OC-12c/STM-1c/STM-4c ATM MDA
  - 7750 – 16 x OC-3c/STM1c ATM MDA
- ASAP MDAs
  - 7750 – 12/4 x chDS3 ASAP MDA
  - 7750 – 4 x chOC-3/chSTM-1 ASAP MDA
  - 7750 – 1 x chOC-12/chSTM-4 ASAP MDA
- CES MDAs

Support of OC-48 POS ROHS (4-port only), 16-port OC-3 and 4-port & OC-12 ATM ROHS, OC-3/12 POS ROHS (16-port only) MDAs

The main driver for the Portugal SONET/SDH MDA is due to the “Rhine Framer” utilized on the Spain, Alberta MDA’s and Orophin CMA has become obsolete. Hence an in-house FPGA SONET/SDH Framer based MDAs have been introduced which will supersede the “Rhine Framer”, these would enable a new generation software selectable POS, and ATM MDAs.

The Portugal MDA’s will provide the 7710 SR, 7750 SR, 7750 SR-c4/c12, and 7450 ESS Platforms with higher performance, and functionality, as well as significant investment protection.

This generation of SONET/SDH MDA’s will focus on the higher density port counts for product introductions, reducing the overall number of SONET/SDH MDA’s going forward.

Support of 3-port 40GE (possibly oversubscribed) Magma-based QSFP IMM

This is a second phase of 40G Line Card for the 7x50 SR/ESS Family. This Line Card will be based on the 100G baseboard with a new daughter card PCB that would ideally support (3) 40G ports and will occupy one IOM slot in the 7x50 SR Family.

This generation of IMM would require a smaller optics package/technology (QSFP) as opposed to the CFP form factor specified by the IEEE. This would enable a single 7x50 slot to accommodate 3 ports, as CFP is too large to fit/power/cool. QSFP is a package believed to be feasible offering a low cost 40G solution that consumes less power and is small enough to accomplish the product goals.

The target application for this is aggregation of 40g trunks at the core, providing PE to PE, and or P to PE trunks for short reaches inside the building. It could be noticed that a PE-facing 7x50 with many 40G

ports designed to aggregate other 7x50's, hence a single port QSFP version of the IOM3-XP based 40G IMM is inevitable to directly interoperate with this line card in 7x50 systems higher up the food chain. The reaches that shall be made available are 2km, 10km, and possibly 40km for this QSFP package. This is a standard serial 1550nm wavelength over SMF, and would be used also to interconnect to OTN boxes such as the OND 1870.

One application is to leverage 40G for cost sensitive high speed trunks. It is also possible that 40G shall have a place in applications such as GE aggregation in the metro space. In this case 40G will offer a more cost effective, stat-mixed function for east-west trunk connections. In this space, 100G may not be affordable for next few years, hence future platforms shall utilize 40G uplinks, thus requiring IMM's in the systems further up the food chain to collect these interfaces.

The next generation Integrated Media Module (IMM) for 7x50 ESS/SR platforms provide high scaling of services with support for multi-core CPU on the IMM.

Support of IOM3-XP with MultiCore CPU

The 2nd Generation of the IOM3-XP product is being designed to deploy a multi-core Cavium processor to provide additional on-IOM processing for expected SW enhancements in the near future. This product will leverage the same basic board design, except for the addition of the Cavium multi-core NP. This device will carry a new 3HE part number.

The basic network design/use cases are unchanged. However, the addition of the multi-core NP offers the hope of positively affecting a number of functional areas such as:

- BFD sessions/timers/performance/scale
- Mobile ISM Features
- Staticstics collection/processing
- Convergence/FIB updates
- PPP Sessions
- Boot time
- IEEE 1588v2

Support Configuration Rollback Alarms

CLI Rollback provides the ability to 'undo' configuration and move back to previous router configuration states while minimizing impacts to services (i.e. no reboot). This feature gives the operator better control and visibility over their router configurations and reduces operational risk while increasing flexibility and providing powerful recovery options.

The ability to rollback to a previous configuration is provided. Rollback is useful in case configuration changes are made but the operator later decides to not keep the changes (e.g. for experimentation, or when problems are identified in the configuration during actual network operation). The change of configuration is performed with minimal impact on the services being provided by the SR (i.e. without a reboot).

A history of changes is preserved allowing rollback to different points (checkpoint ids), as well as examination of changes made.

Without the rollback feature, the best we can do with SR-OS in previous releases is either:

1. Reboot to any config, or
2. Operator manually creates a 'forward' script of desired changes, along with a 'backout' script that would undo all the changes.

With rollback, the operator can smoothly revert to previous configurations.

Important Note: In 5620 SAM Release 9.0 R5, 5620 SAM just would process the special traps / events that would get generated during rollback those are,

tmnxSysRollbackStarted	*- A rollback revert was initiated*
tmnxSysRollbackStatusChange	*- A rollback revert has finished*
tmnxSysRollbackSaveStatusChange	*- A rollback save has finished*

The 5620 SAM would process those traps / events and would generate an alarm named "ConfigurationRollBackStatus" with severity as "Info" with the following details, with appropriate state based on the trap received.

```
Details of the Alarm
Name:                   ConfigurationRollBackStatus
Defined in package:     netw
Raised on class(es):    NetworkElement
Alarm type:             configurationRollBackAlarm (103)
Default severity:       SEVERITY_INFO
Default probable cause: configurationRollBackOperationPerformed (1422)
All probable causes:    configurationRollBackOperationPerformed (1422)

Additional properties
Implicitly cleared:     false
Applicable nodes:
                        Alcatel-Lucent 7450 ESS 9.0.0
                        Alcatel-Lucent 7710 SR 9.0.0
                        Alcatel-Lucent 7750 SR 9.0.0


Description:
            The alarm is raised when a configuration rollback operation is
            performed. And as aj additional information this alarm will also
            indicate the check point that has been rolled back.
```

Support of Multicore CPU-based 48-port GE TX IMM (KrakaCyprus2), Multicore CPU-based 48-port GE SFP IMM

The basic network design and use case are similar to that for the original IMMs, However, the addition of the multi-core processor on the card is expected to have a positive impact on specific functional areas as well as for overall services:

- BFD #sessions/timers/performance/scale
- Mobile gateway features
- Use of large number of shapers
- Convergence timing
- #of PPP sessions
- Boot time
- IEEE 1588v2
- Other areas deemed necessary by engineering

Note: SR has moved the release of the above IMMs to future releases, but as per our earlier plan, the 5620 SAM has provided the support for the same, which will not have any impact now. Once node releases these MDAs, the 5620 SAM support would get enabled automatically.

Service Size Reduction

Prior to 9.0, service sites of the same triplet [type, NE service-id, and customer-id] are put into one 5620 SAM service. In a number of deployments, the number of service sites of the same triplet could be in the range of hundreds and their (M-)SAPs could be in the millions range. Also, a large 5620 SAM service can be connected to other services to form a big composite service with thousands of sites and connections. This feature enables the formation of multiple 5620 SAM services with service-sites of the same triplet. It also allows manual fragmentation of a SAM service into multiple SAM services while retaining the service-site id, i.e. the triplet. The "break-up" shall have no effects on NE configurations. The operator can also create a composite 5620 SAM service in this manner if the composite service automatic discovery toggle is on.

When a large service is discovered, the operator is able to move the sites from the discovered SAM service to other SAM services while maintaining the service type, NE service-id, and customer-id. This technique is used in case where the service has been provisioned directly via CLI before SAM is deployed. There are no effects to the network configurations when the service sites are moved from one SAM service to another.

Services and Composite Services Management Enhancements

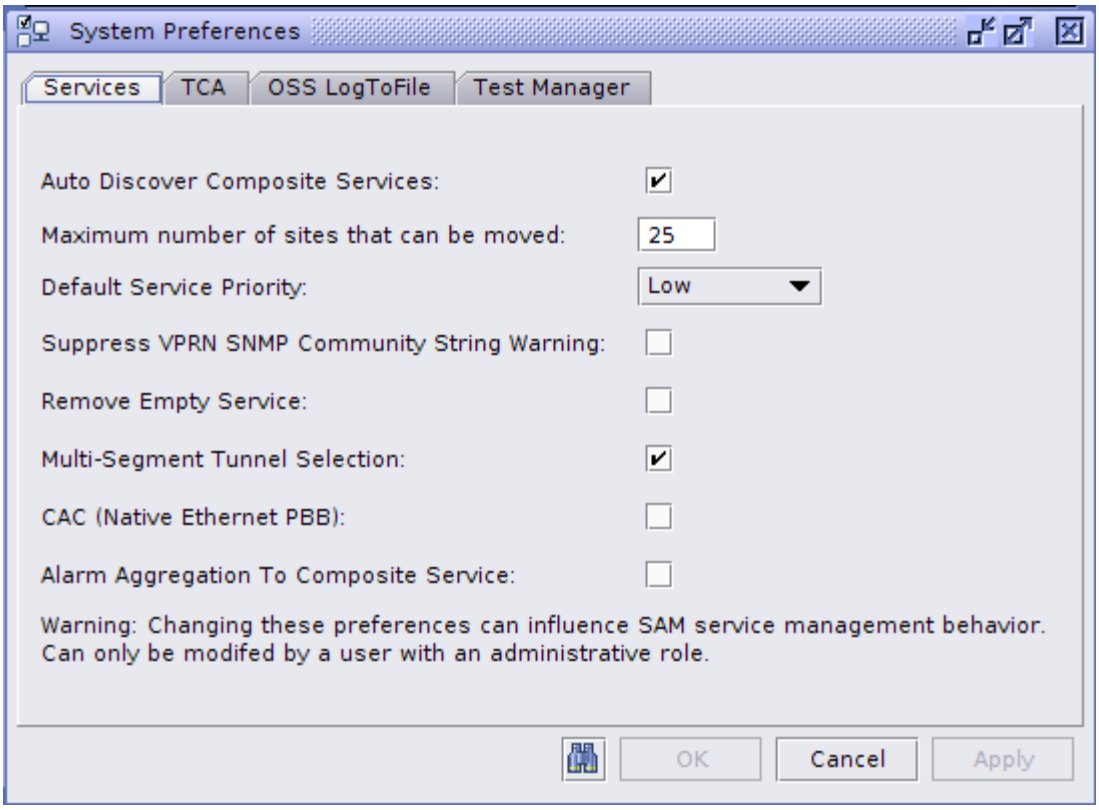
1. Create and add services/service-sites from the composite service flat map - The service connectors and the spoke/mesh SDP bindings between the service sites/SAPs/Interfaces can also be created from the flat map.

2. System wide service specific behaviour can now be configured by the admin(s) (GUI and OSSI). Four of the properties are available in 90R1: autodiscovery of composite service (default ON), default service priority (for deletion only - default is LOW), VPRN community alarm enabled (default is TRUE), maximum number of service sites can be manually moved from one service to another).

Auto Provisioning of Multi-Segment PW (Path Search)

The feature speeds up and increase the usability of the provisioning for service connections that span over multiple PE’s, i.e. a connection between two service instances that require one or more switching epipe(s) in between.

In order to use this functionality, "Multi-Segment Tunnel Selection" must be enabled under Administration->System Preferences:



It is possible to create a Spoke SDP Binding from any object that supports a Spoke SDP Binding into any object that supports a Spoke SDP Binding. These objects are:

- (M-)VPLS Site
- (M-)VPLS I-Site
- (M-)VPLS B-Site
- VLL Site
- IES L3 Access Interface
- VPRN L3 Access Interface
- VLL Endpoint
- VPLS Endpoint

When creating a Spoke SDP Binding, if a Termination Point is specified, the Spoke SDP Bindings and return Spoke SDP Bindings will be created.

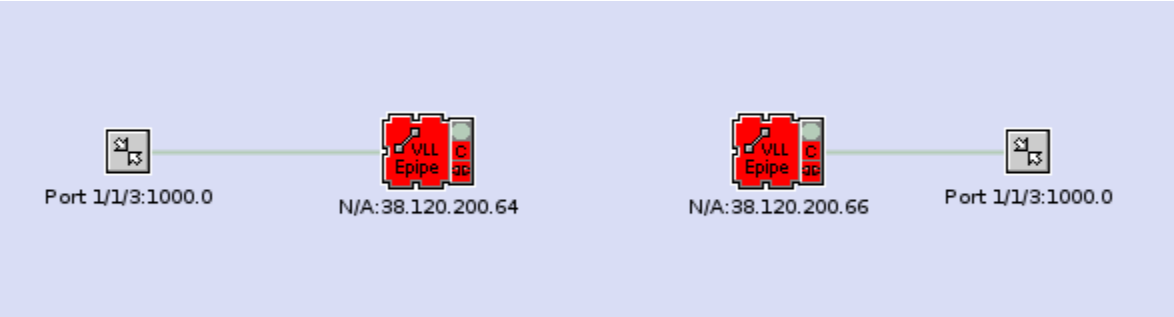
Switching sites will be created as follows:

1. If the Spoke SDP Binding is being created on a VLL, the switching sites will be created on the VLL service.
2. If the selected Termination Point is on a VLL service, the switching sites will be created on the VLL service.

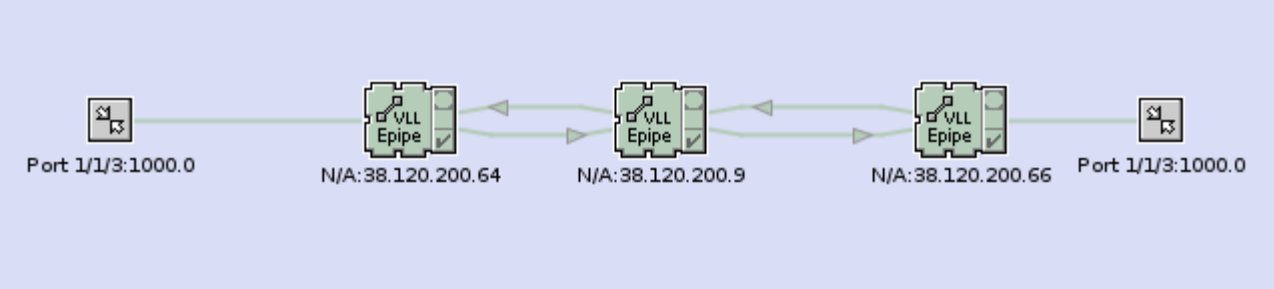
3. If neither end is on a VLL service, a new EPIPE service will be created. The svcComponentId will be auto-selected by 5620 SAM. The subscriberId will be that of the service on which the spoke is being created. All other parameters will be the default value.

In order to use this functionality, a Tunnel Selection Profile must be selected when auto-creating the Spoke SDP Bindings. The "Multi-Segment Tunnel Selection" property must be enabled on the TSP:

This functionality is supported when creating a Spoke SDP Binding on a VLL Service. Starting with a base EPIPE service with two sites



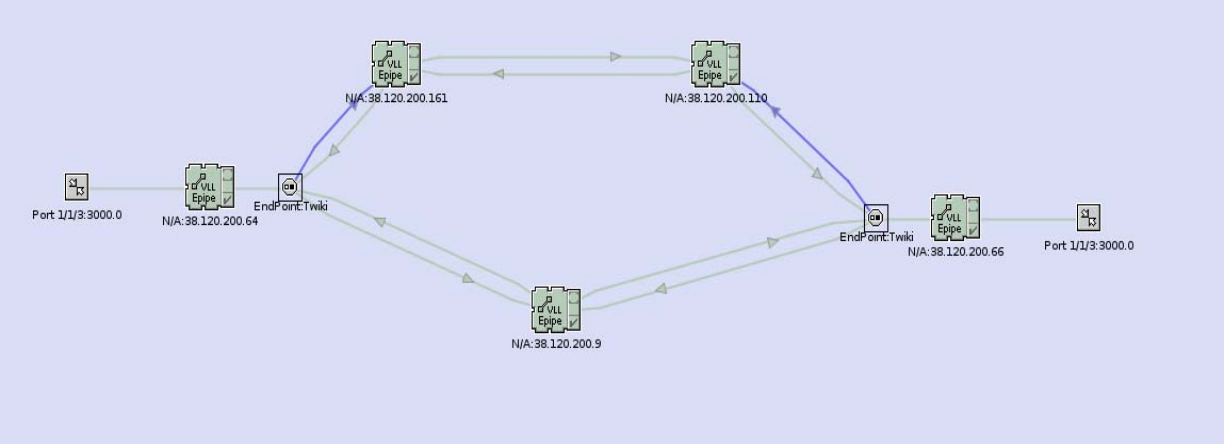
If a valid path is found between the two terminating sites, the Spoke SDP Bindings and switching sites will be created:



It is also possible to use this functionality when creating a VLL service.

For example, create an EPIPE service with two terminating sites. At the service level, enable "Automatic SDP Binding/PBB Tunnel Creation". Select the TSP with "Multi-Segment Tunnel Selection" enabled:

On the tunnel selection profile, if the "Redundant Path Selection" property is enabled, a redundant path will be created. This property can only be enabled if the "Multi-Segment Tunnel Selection" property is enabled.



The process from a VLL service is similar to that from the configuration without a redundant path, with the exception being that the TSP must have "Redundant Path Selection" enabled.

From a VLL Service, Endpoints on the Terminating sites that do not have SAPs or Spokes are used for the auto-created Spokes. If multiple Endpoints exist on a Terminating Site, the Endpoint without any SAPs is used. If multiple viable Endpoints are available, an error is raised by 5620 SAM and the operation fails. If there are no Endpoints available, an Endpoint is automatically created with all default values except:

Name: Endpoint_Service-*NodeServiceId*
Description: Auto-created by 5620 SAM

The precedence of the Spoke on the primary path will be set to 0; the secondary will be set to 1.

Templates are used as follows. The 5620 SAM will use the following logic to find a SDP Binding Template in the following order:

1. If the SDP Binding Template is populated in the TSP it is used when creating the Spoke SDP Bindings. This is not a change in behaviour from previous versions of 5620 SAM that support the TSP.

2. If the Site that the SDP Binding is being created on has a site template associated to it than an attempt is made to find a Spoke Template in that template. If **one** is found it is used to auto-create the Spoke SDP Bindings. If two or more are found then 5620 SAM will create the SDP Binding with default properties. If none are found continue on to step 3.

3. If the Service is associated to a Template then an attempt is made to find a Spoke Template in that template. If **one** is found it is used to auto-create the Spoke SDP Bindings. If zero or two or more are found then the automatically created SDP Bindings will be created with default properties.

Tunnels that fail to meet the following criteria are rejected:

- The operational MTU of the tunnel must be greater than or equal to the larger of the operational MTU of the terminating sites
- The tunnel must be operationally up
- The tunnel must pass the steering parameters specified in the tunnel selection profile

Tunnels are selected based on the following criteria:

1. If the metric value is specified for any of the SDPs along the path, the selected path will have the lowest sum of the metric property for all SDPs along the path

2. If no metric is specified for any of the SDPs along the path, the selected path will have the fewest number of SDPs (hops)

If two paths or SDPs are equal based on the selection criteria above, the selected SDP/path will have the lowest load factor (number of services using that SDP).

When using this functionality, SDPs will only be selected. No SDPs will ever be created.

FN2693 – Test Suite for Composite Service

This feature is about the support of Composite Service by TestSuite, i.e. composite services can be periodically end-2-end tested based on a predefined test template (or policy). Only L2 composite services are supported, i.e. a composite service can only consists of epipes and vpls's.

Retain Customized Test Attributes with Regenerating Tests

STM auto test generation function based on test template(s) and service topology is generic for all test entities. In certain applications, when there is a need to delete unnecessary tests or modified certain tests of the auto-generated tests. Prior to 9.0 R5, after the tests of a given test entity have been deleted and/or modified, when the auto generation test function is invoked again, STM would recreate the (deleted) tests. With 5620 SAM Release 9.0 R5, such modifications will survive subsequent Test Suite's auto test generation execution.

A new flag at the test entity level to help differentiate entities with modified/deleted tests and unmodified entities. The flag is set only when a test, MEP or NE MEG has been deleted. The flag can be manually set/reset from the Test Suite's test entity list. Note that when a test entity topology is changed, one or more tests of that test entity will be affected (existing behaviour); the flag for that entity will not be set.

Shared Domain Id

There is a need to have the same 802.1ag/Y.1731 Maintenance Domain Id (MD Id) in various parts of a

network. Note that there are three MD Ids that need to be differentiated: SAM MD Id, Network Equipment's MD Id, and standard E-OAM MD Id (level, type, and name if applicable).

Prior to 5620 SAM Release 9.0 R5, if the specified MD Id is already used in the NE by another MD, then SAM will assign the next available Id on the NE for the being created MD. That means the NE MD Id is not used to decide whether a NE MD belongs to a 5620 SAM (global) MD or not. Only the standard E-OAM Id used to see if an NE MD (or local MD) belongs to a global MD.

With Release 9.0 R5, 5620 SAM has a new option to auto assign NE MD Id (as pre 9.0 R5) or to specify the value when creating a Global MD. If the value is specified, then the configuration would fail at the NE's where the specified value is already used.

To maintain backwards comparability, 5620 SAM will discover MDs the same way it does in pre-9.0 R5, i.e. the standard E-OAM MD Id defines the uniqueness and the local NE MD Ids can be different. When using multiple MD's of the same "standard E-OAM MD Id", 5620 SAM should be used for the configuration of MD network wide.

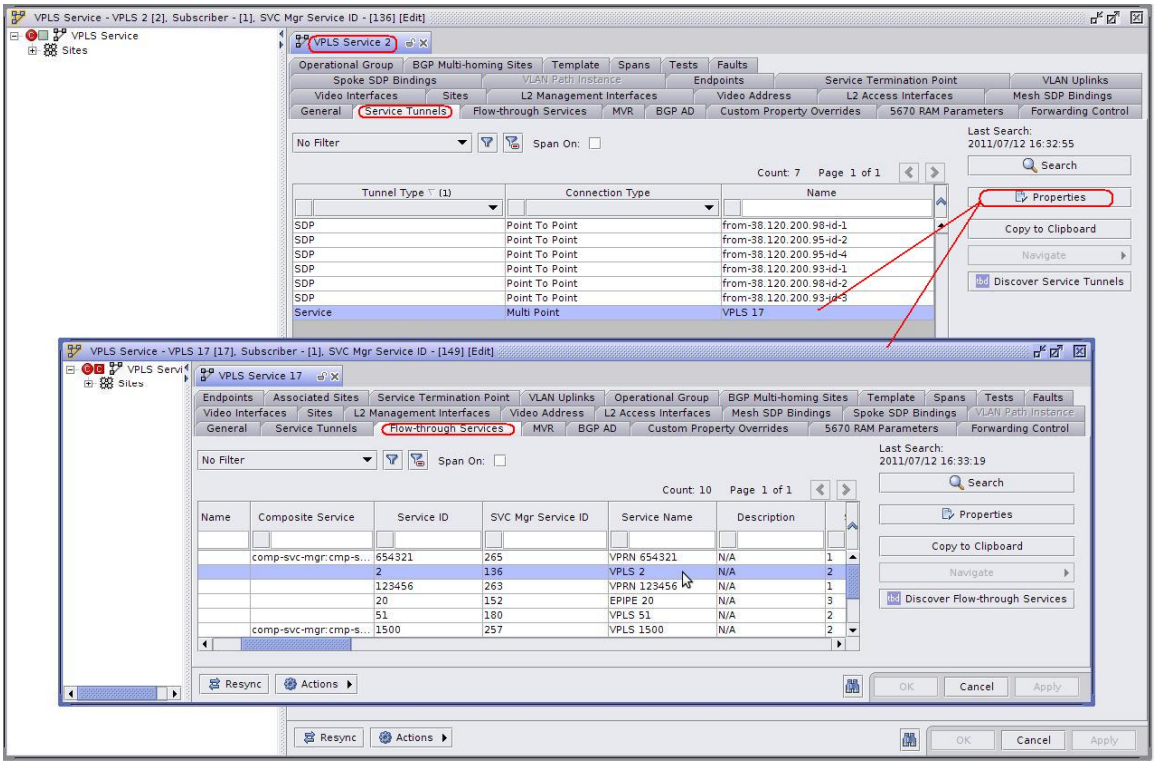
Upgrade script will modify pre-existing global Domains to have MD Id = 0 (auto assign when distributed).

OMNI nodes the local MD Id must be set to auto assigned as OMNI NE's do not have local MD Id.

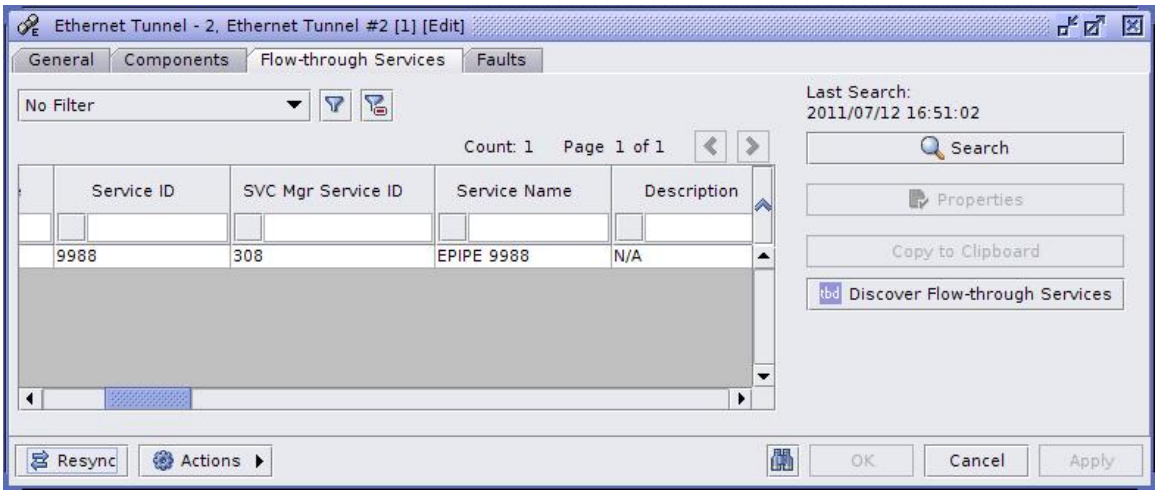
FN2906 Tunnels for Services

A service data path can ride on one or more service tunnels. A service tunnel is not just a unidirectional SDP, but could also be another service (B-VPLS, Optical Transport Service, MPR Transport Service, etc.), a G.8032 ring or G.8031 Ethernet Tunnel. To assist trouble shooting such as alarm correlation between those hierarchical services or finding the dependencies among those services/service-tunnels, this feature broadens the concept of service tunnel and to provide the relationship of the services.

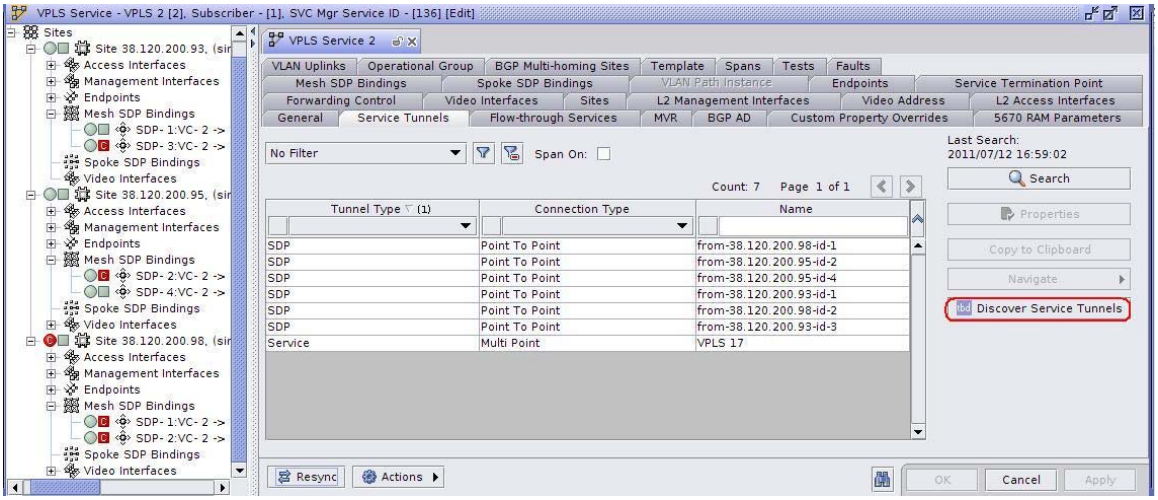
A new Tab called "*Service Tunnels*" shall be added to the Service Display Manager to list all currently used service tunnels. A second Tab called "*Flow-through Services*" shall be added to the display manager of all tunnel objects that are considered a service tunnel (such as Service, Ethernet Ring/Tunnel) to list all services that are currently using that specific service tunnel.



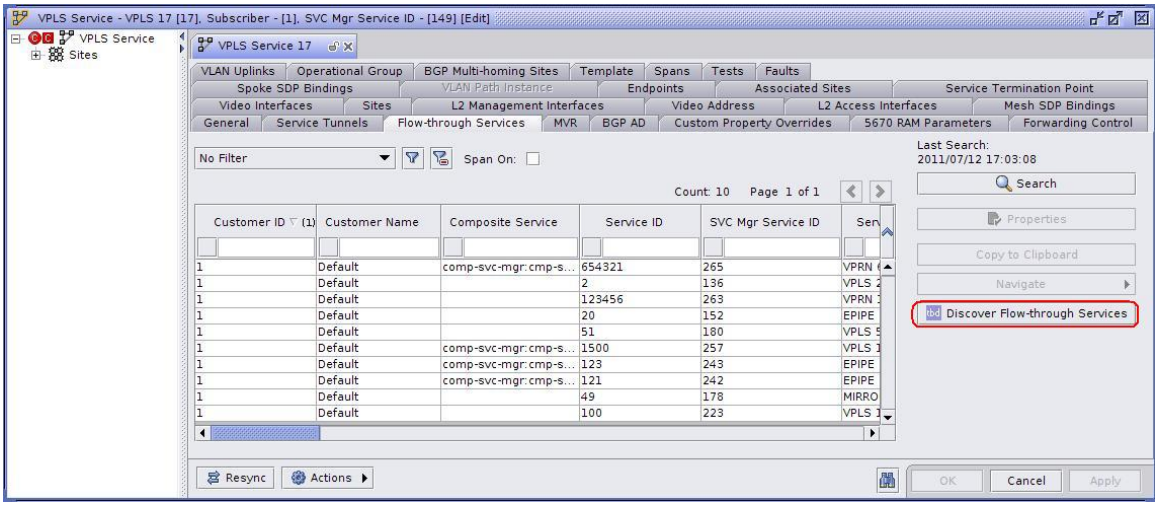
The following diagram illustrates the "*Services*" tab on the Ethernet Tunnel display manager where services currently using this Ethernet Tunnel are listed.



An operator shall be able to discover service tunnels on demand for any given service. An action button called, "*Discover Service Tunnels*" shall be added to the new '*Service Tunnels*' tab. This action removes any previously discovered service tunnels on the service and triggers the manual re-discovery of service tunnels based on direct usage and current service configurations. This action can be used on existing services after a SAM upgrade and shall be available through OSS.



An action button called, "*Discover Flow-through Services*" shall be added to the new *'Flow-through Services'* tab. This action removes any previously discovered Flow-through services on the service tunnel and triggers the manual re-discovery of Flow-through services based on direct usage and configuration. This action can be used on existing service tunnel after a SAM upgrade and shall be available through OSS.

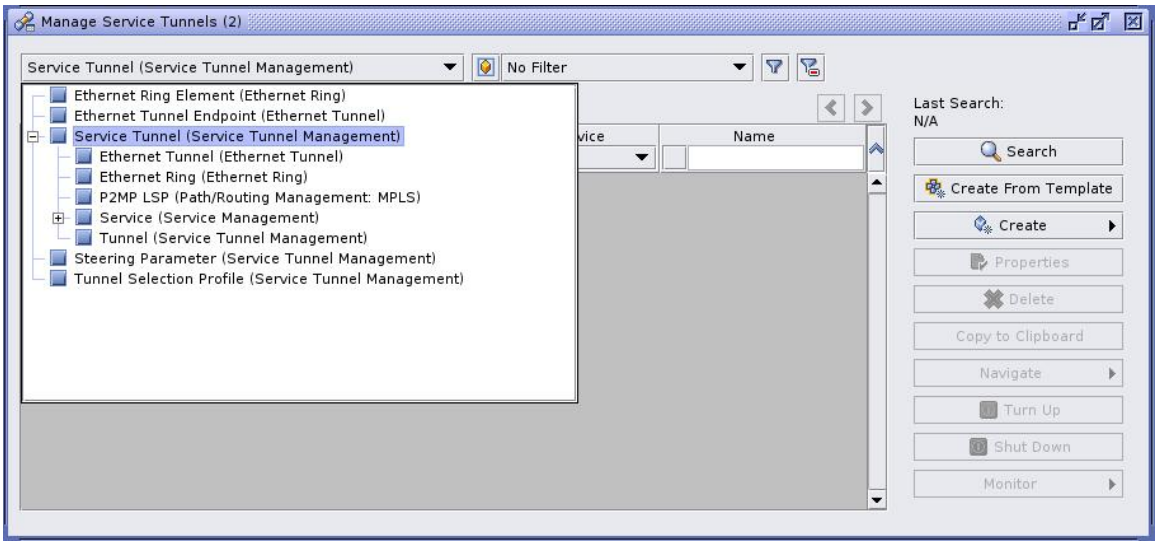


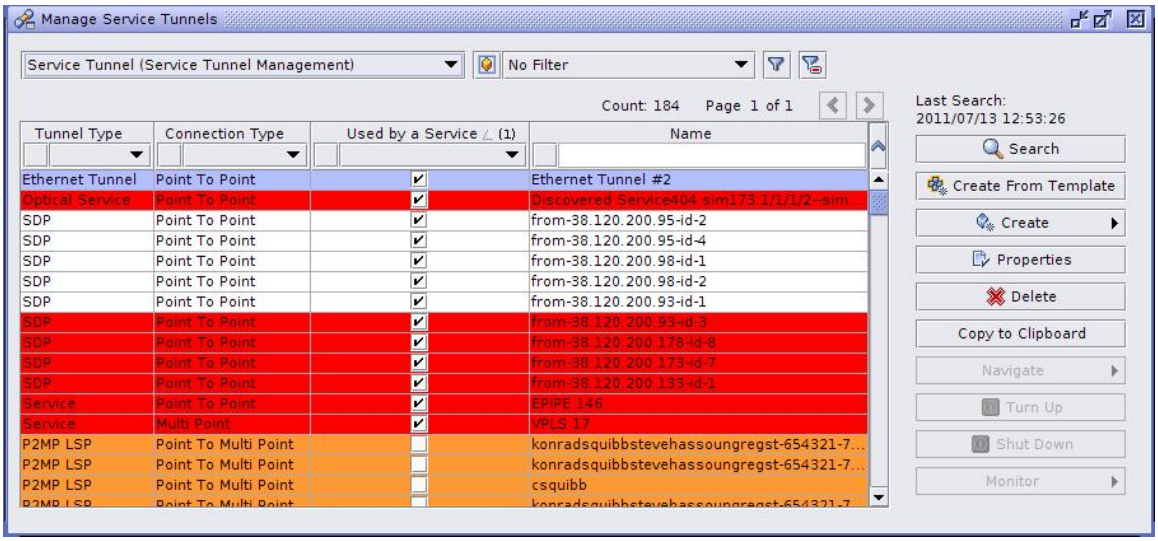
The following table is the "Service Tunnel Discovery Matrix" in order of priority and supported SAM release.

Service Tunnel	Supported Services	Priority	SAM Release	Discovery
Tunnel (SDP)	L2 & L3 VPN	P1	9.0 R5	Yes
Service to Tunnel Association	L2 & L3 VPN	P1	9.0 R5	Yes
Ethernet Tunnel	I/E-PIPE, I/B/VPLS	P1	9.0 R5	Yes
Ethernet Ring	I/B/VPLS	P1	9.0 R5	Yes
PBB	EPIPE, I/M/VPLS	P1	9.0 R5	Yes
P2MP RSVP LSP	VPRN	P2	9.0 R5	Yes

Optical Transport Service	L2 & L3 VPN	P1	9.0 R5	Yes
MPR Transport Service	L2 & L3 VPN	P1	9.0 R5	Yes
IPSec	VPRN, IES	P2	TBD	No
L2TP Tunnel	VPRN	P2	TBD	No
Carrier Supporting Carrie (CSC)	L2 & L3 VPN	P2	TBD	No

The current Service Tunnel listing window shall be enhanced to include 'Service Tunnel' category where all service tunnel objects can be listed. Although the list contains services, it only lists those services that are being used as service tunnels and this depends on the on-demand discovery of service tunnels where a service is discovered to be used by another service as a tunnel. Also, since the discovery is on demand; therefore, the list of services may not be up-to-date.





There shall be no alarm aggregation as this can amount to a very large number of alarms. However, a new alarm relation of "*association*" type shall be added between service tunnels and service in order to propagate the object (service tunnel) alarms to the service level. These alarms as they are association alarms shall be displayed on the 'Related Alarms' under the 'Faults' tab. This is a one way

association relation which means no service alarms are to be propagated to the service tunnels that it is currently using.

Increase max number of mesh bindings per VPLS

With this enhancement, VPLS full mesh with 100 service instances (sites) can be created from SAM in one step. The provision of full mesh bindings can be done via SAM-O, the service map, or the service configuration form.

FN2699 Composite Service Alarm

The use of composite service for business VPN services is quite popular. Prior to 9.0 R5, alarms from the component services and their child objects are not visible at the composite service. A new property called "Alarm Aggregation to Composite Service" shall be added to the Service Preferences to enable/disable service alarm aggregation to composite service. When enabled, all component service alarms shall be listed under the 'Aggregated Alarms' tab under the Faults tab of the Composite Service. This property is 'Disabled' by default.

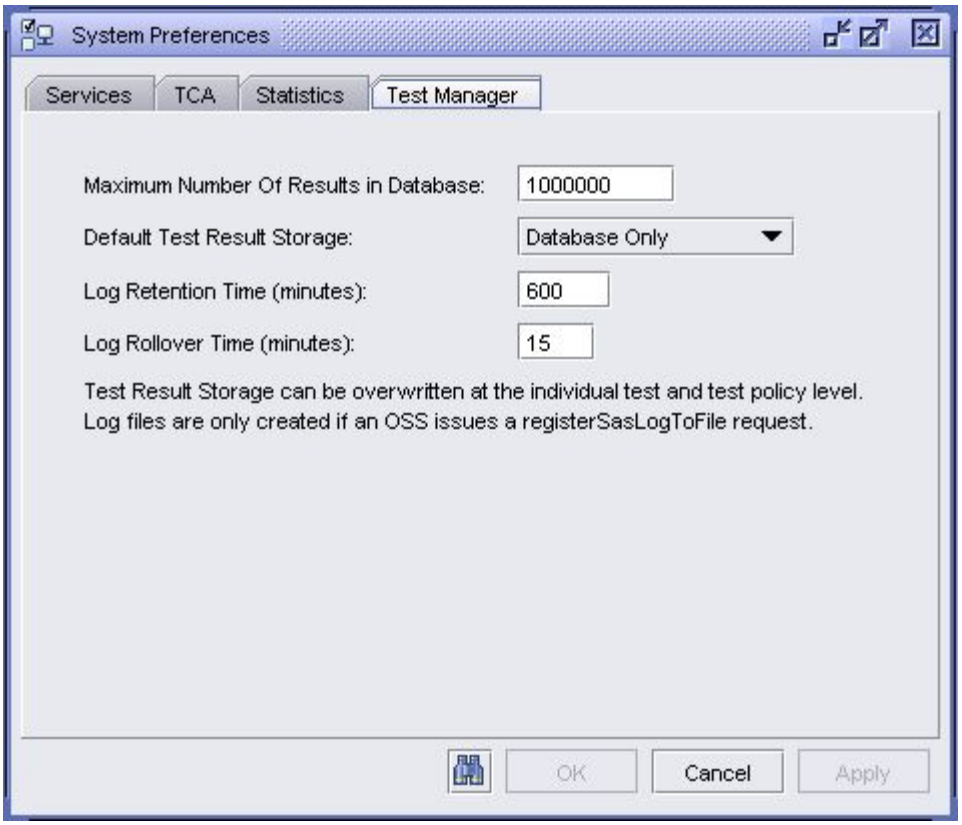
LogToFile OAM Test Results

To support 200K test results per 10 minute interval, SAM 9.0R5 offers the option to write the directly results to text files. With SAM 90R5, SAM operators are able to select one the following options per test suite or per individual test:

1. Log to file
2. Log to database
3. Log to both

The options are available via OSSI and GUI.

The default option can be defined using Administration->System Preferences



Log to file is only applicable for tests and test suites with accounting files. For tests and testsuites without accounting files, the only applicable value is Log to Database.

The behaviour of STM LogtoFile feature is based on the existing Stats Log to File function. That means the test results for all test executed from an NE are stored in the files specifically for that NE. The logfile has the same format and information as the findToFile.

In order for the log files to be created, there must be a request from a JMS client.

The number of threads (workers) and the location (directory) of the log files.

FN2831 Accounting File and Continuous Execution Specification for Individual E-OAM Test

The Continuously Execution option shall be configurable on each individual NE Schedulable CFM test.

For individual test configuration:

- By using the CLI commands, the AccountingFile option could be configured for each individual test. The ContinouslyExecution and the AccountingFile options are intended to be configured together to achieve the best execution rate performance.

- The AccountingFile option shall be configurable during the creation of one individual NE Schedulable test. The test configuration form shall display the AccountingPolicy name if the Test Result Accounting Policy exists on the node, or an error message indicating that no Test Result Accounting Policy could be found on the node.

- AccountingFile option and Trap configurations are mutually exclusive. If the test already has accounting option, then removing this option, will set the trap configuration on the test, and vice versa. This behavior is supported from OSSI

- The ContinuouslyExecuted and AccountingFile options are independent from each other.

The GUI operator will be able to execute the test once it has the Continuously Executed option configured by clicking the Execute button. While the test is continuously executed, the Execute button greys out, and the Stop button becomes read-writable.

A test with Accounting File option can only be added to a Test Suite using Accounting File. A continuously executed test can only be added to a Test Suite with continuously executed option on. If the test is currently running, it will continue to run when being added to the test suite regardless the execution states of the test suite's tests. If the test is not running when being added to the suite, it will assume the execution state of the test suite.

FN2552 SR MS-PW Routing

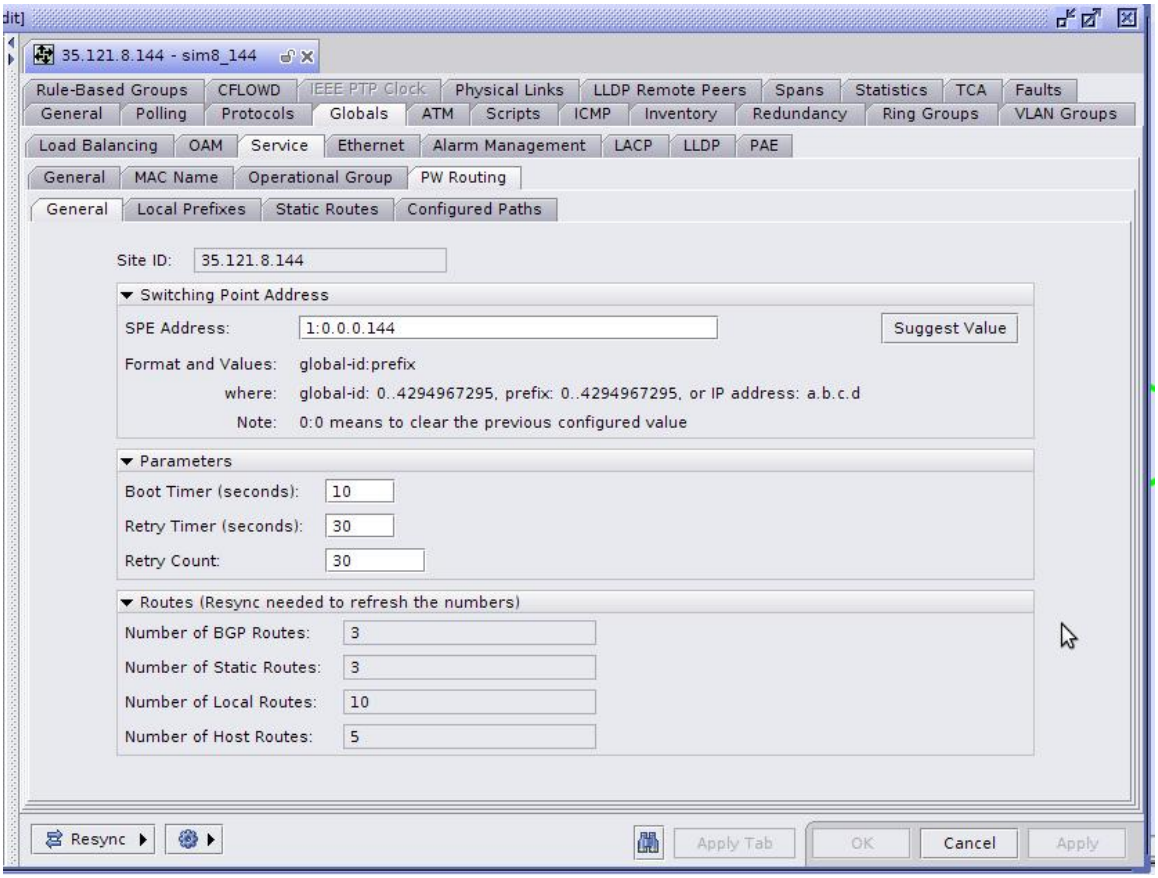
Prior to Release 9.0, the Alcatel-Lucent 7x50 provided Inter-domain Services for VLL through the use of VLL spoke switching (5620 SAM 6.0), which allows to create a VLL service by cross-connection two spoke SDPs. This was achieved by statically configuring the PW Switching Points at the gateway S-PEs between domains.

5620 SAM Release 9.0 R5 service manager greatly speeds up and improves the multi-segment PW provisioning (see Path Search feature). That feature also supports end points from 7210 and 7705 and any SR versions. Besides, the MS-PW can be created between various service instance types and not restricted to epipe. The key advantage of using this BGP based MS-PW SR feature is service path protection is accomplished by routing while the existing PW service path protection is either explicit (with endpoint object) or by MPLS layer.

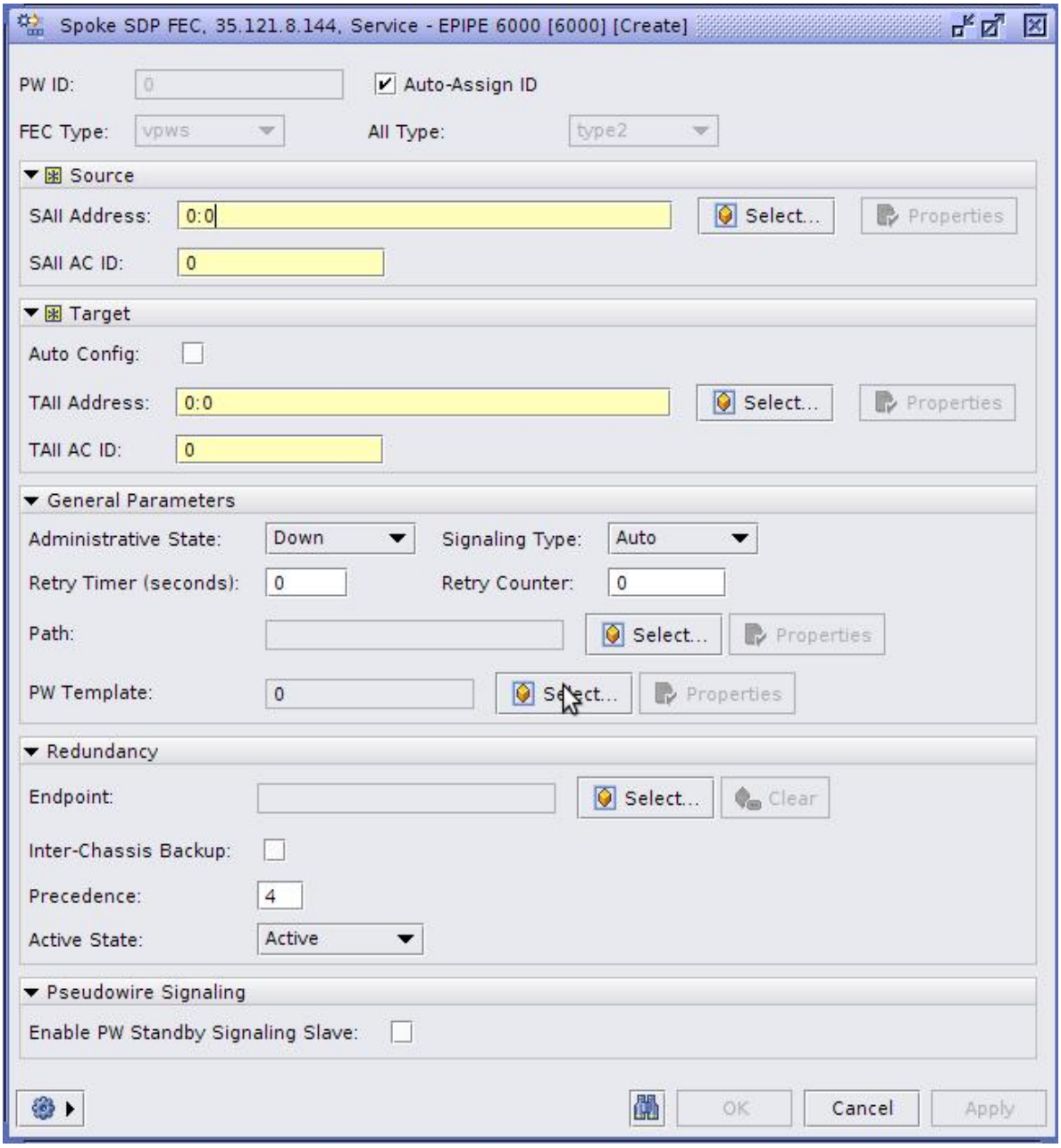
The following simplified procedure gives an overview of the SR feature.

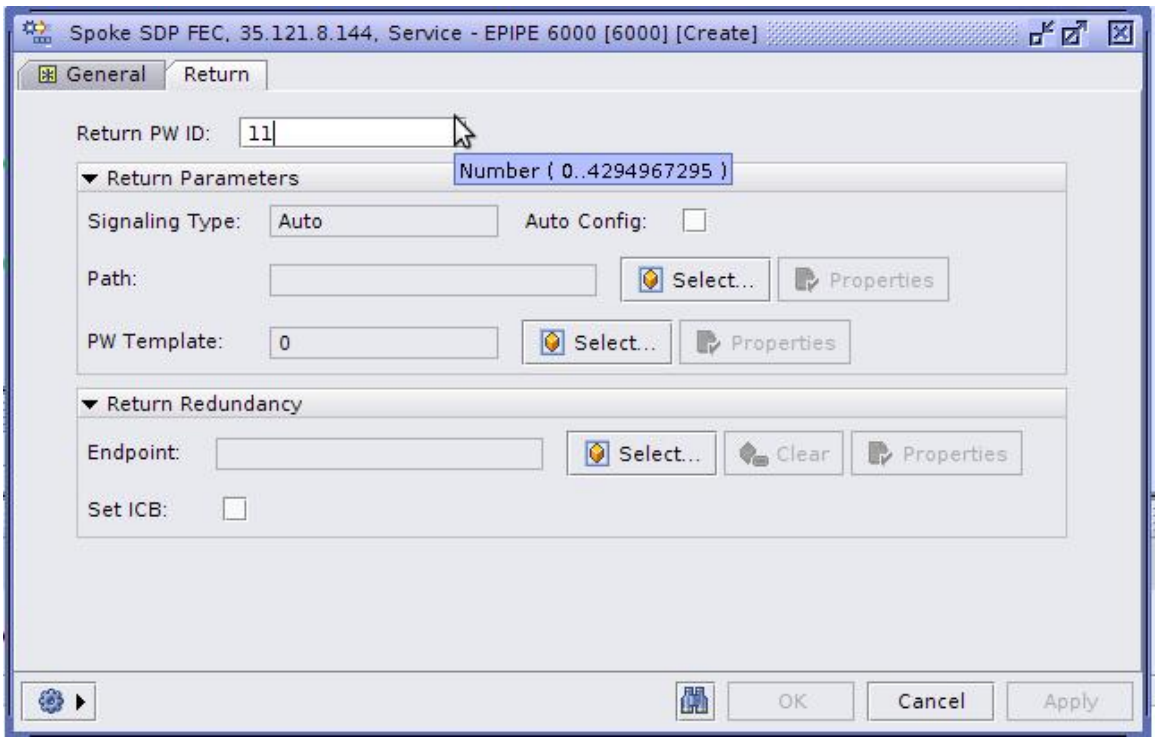
Network Commissioning Procedure

Step 1: BGP family needs to include **MS PW** and IPv4.
Step 2: Configure a routing policy having family including MS PW, and if path diversity is needed for primary/standby MS-PWs, multiple policy entries are required.
Step 3: If there are ASBRs, or if all T-PEs and S-PEs are within the same AS extra configuration is needed.
Step 4: Configure PW routing parameter at the NE level.



To create a MS-PW spoke one would need to create a spoke FEC, a new tab in the service form. The return spoke FEC is supported in the same fashion as T-LDP spoke.


Spoke SDP FEC, 35.121.8.144, Service - EPIPE 6000 [6000] [Create]
PW ID:
0
Auto-Assign ID
FEC Type:
vpws
All Type:
type2
Source
SAII Address:
0:0
Select...
Properties
SAII AC ID:
0
Target
Auto Config:
TAII Address:
0:0
Select...
Properties
TAII AC ID:
0
General Parameters
Administrative State:
Down
Signaling Type:
Auto
Retry Timer (seconds):
0
Retry Counter:
0
Path:
Select...
Properties
PW Template:
0
Select...
Properties
Redundancy
Endpoint:
Select...
Clear
Inter-Chassis Backup:
Precedence:
4
Active State:
Active
Pseudowire Signaling
Enable PW Standby Signaling Slave:
OK
Cancel
Apply



OMNI Support

The following table shows features of the OmniSwitch family of products supported by 5620 SAM releases.

Functionality	SAM 6.0 R1	SAM 6.0 R3	SAM 6.1 R1	SAM 7.0 R1	SAM 7.0 R3	SAM 7.0 R4	SAM 8.0 R1	SAM 8.0 R3	SAM 8.0 R5	SAM 9.0 R1	SAM 9.0 R3	SAM 9.0 R5
OmniSwitch Equipment Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stack Configuration[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ethernet Port Configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VLAN Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
QoS Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NE Maintenance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AAA Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Port Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protocols – Static Routing, IPv4 Multicasting (switching & routing)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

IGMP Snooping	-	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
Notifications – Traps & Alarms	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
Ethernet Interface Statistics	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
OSSI	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
OAM – ICMP Ping & Trace	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
Full Spanning Tree management	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫	∫
UDP Relay/DHCP Snooping[3]	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
Switch Health Monitoring	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
Ethernet OAM – Connectivity Fault Management	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
CPE Node Head Test[2]									∫	∫	∫	∫
Y1731[2]									∫	∫	∫	∫
SAA interval									∫	∫	∫	∫
LAG – Link Aggregation Group	-	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫
LLDP - Link Layer Discovery Protocol	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
Service Templates	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
Scheduling	-	-	-	∫	∫	∫	∫	∫	∫	∫	∫	∫
Routing Protocols: OSPF,RIP, PIM[3]							∫	∫	∫	∫	∫	∫
MVRF-Multiple Virtual Routing & Forwording[3]							∫	∫	∫	∫	∫	∫
MPLS, LDP support [3]							∫	∫	∫	∫	∫	∫
VPLS support [3]							∫	∫	∫	∫	∫	∫

Table 5: Supported OMNI Features

[1]Stack Configuration is not supported for the OS 6855 6.3.2 and OS6900
[2] Supported only for OS6250M starting with AOS 6.6.2
[3] Applicable to AOS9000E nodes in 8.0 R1/R3.
[4] UDP Relay/DHCP Snooping is not supported on AOS9000E nodes in 8.0 R1.

The 5620 SAM Release 8.0 supports the following OS6250 Chassis types:

Chassis Type	Description
OmniSwitch OS6250-8M	8 copper GigE Ports, 2 Fiber/Copper GigE combo ports, and 2 fiber ports for stacking.

OmniSwitch OS6250-24M	24 copper GigE Ports, 2 Fiber/Copper GigE combo ports, and 2 fiber ports for stacking.
OmniSwitch OS6250-24MD	24 copper GigE Ports, 2 Fiber/Copper GigE combo ports, and 2 fiber ports for stacking. internal DC power supply
OmniSwitch OS6250-24	24 copper GigE Ports, 2 Fiber/Copper GigE combo ports, and 2 fiber ports for stacking.
OmniSwitch OS6250-P24	24 copper PoE Ports, 2 Fiber/Copper GigE combo ports, and 2 fiber ports for stacking.

Table 6: Supported OS6250 Chassis Types

The 5620 SAM Release 8.0 supports the following OS9000E Chassis types:

Chassis Type	Description
OmniSwitch OS9700E	The OmniSwitch 9700E is a high performance switch offering eight slots for Gigabit Ethernet and/or 10-gigabit Ethernet Network Interface (NI) modules. Additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs). The OmniSwitch 9700E supports a maximum of three power supplies.
OmniSwitch OS9800E	The OmniSwitch 9800E is a high performance switch offering 16 slots for Gigabit Ethernet and/or 10-Gigabit Ethernet Network Interface (NI) modules. An additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs). The OmniSwitch 9800E supports a maximum of four power supplies.

Table 7: Supported 9000E Chassis Types

The OS9000E series share a family of common Network interfaces for 10 Gigabit Ethernet and Gigabit Ethernet connectivity:

NI Module	Description
OS9-GNI-C24E	Network Interface with 24 Ports 10/100/1000 with RJ-45 support
OS9-GNI-U24E	Network Interface with 24 Ports 1000Base-X with SFP/MiniGBIC support
OS9-XNI-U2E	Network Interface with 2 Ports Unpopulated 10Gigabit Ethernet with XFP support
OS9-GNI-P24E	Network Interface with 24 Ports 10/100/1000 with RJ-45 support with Power over Ethernet support

Table 8: Supported OS9000E NI Modules

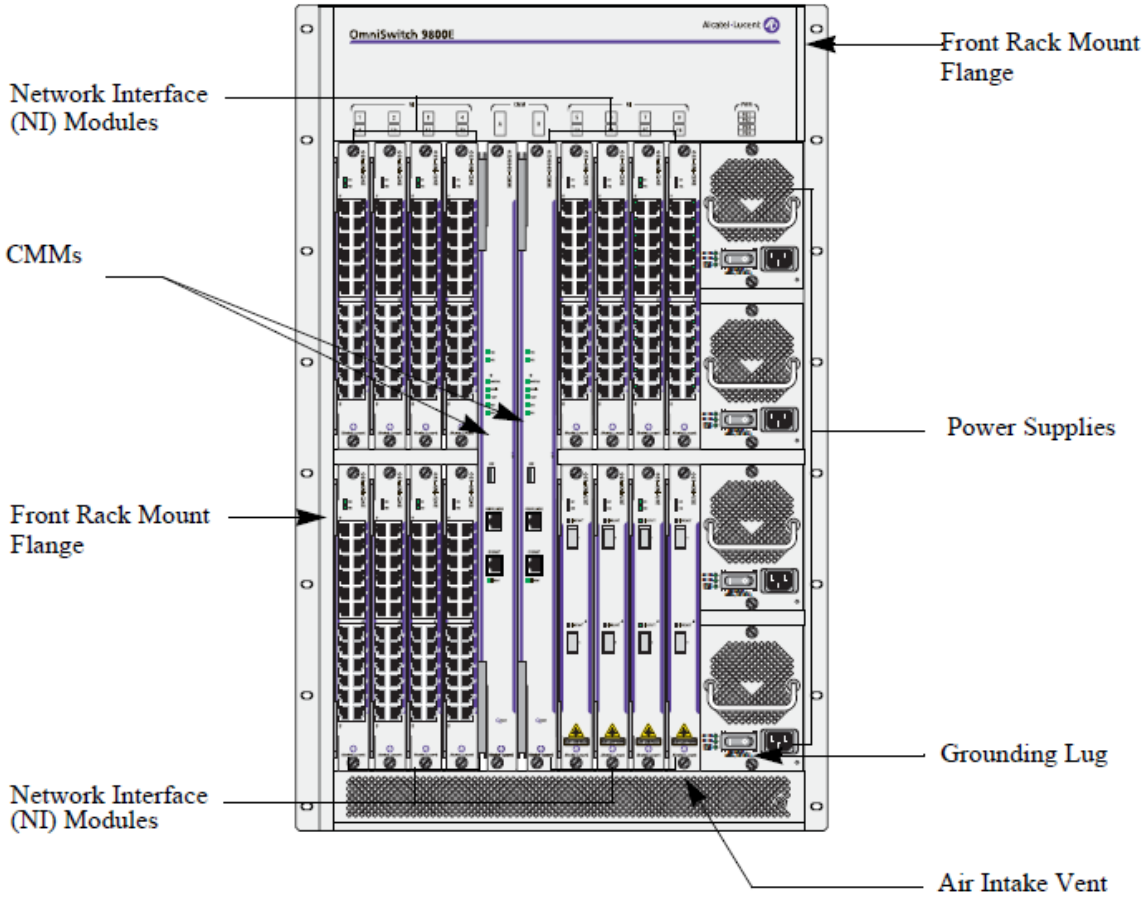


Figure 8: OMNISwitch OS9800E

In 8.0 R1, OSPFv2, RIP, and PIM protocol support is introduced only for AOS9000E nodes.
The maximum number of OS9800E nodes supported by a 5620 SAM is 1000.

The 5620 SAM Release 9.0 R1 supports the following OS6850E Chassis types:

Chassis Type	Description
OmniSwitch OS6850E-24 OmniSwitch OS6850E-P24	Gigabit Ethernet L3 fixed configuration chassis with 20 RJ-45 10/100/1000 BaseT ports, 4 combo ports, and two 10GigE CX-4 ports. The CX-4 ports can be used as stacking ports or as connectors for the OS6-XNI-U2.
OmniSwitch OS6850E-24X OmniSwitch OS6850E-P24X	Gigabit Ethernet L3 fixed configuration chassis with 20 RJ-45 10/100/1000 BaseT ports, 4 combo ports, 2 SFP+ 10GigE ports, and two 10GigE CX-4 ports. The CX-4 ports can be used as stacking ports or as connectors for the OS6-XNI-U2 .
OmniSwitch OS6850E-48 OmniSwitch OS6850E-P48	Gigabit Ethernet L3 fixed configuration chassis with 44 RJ-45 10/100/1000 BaseT ports, 4 combo ports, and two 10GigE CX-4 ports. The CX-4 ports can be used as stacking ports or as connectors for the OS6-XNI-U2.
OmniSwitch OS6850E-48X OmniSwitch OS6850E-P48X	Gigabit Ethernet L3 fixed configuration chassis with 46 RJ-45 10/100/1000 BaseT ports, 2 combo ports, 2 SFP+ 10GigE ports, and two 10GigE CX-4 ports. The CX-4 ports can be used as stacking ports or as connectors for the OS6-XNI-U2

OmniSwitch OS6850E-U24X	Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with 22 SFP GigE ports, 2 combo ports, 2 SFP+ 10GigE ports, and two 10GigE CX-4 ports. The CX-4 ports can be used as stacking ports or as connectors for the OS6-XNI-U2.

Table 9: Supported OS6850E Chassis Types

The 5620 SAM Release 9.0R1 supports the following OS6900 Chassis types with AOS 7.2.1R01 with node Equipment level at this release.

Chassis Type	Description
OmniSwitch OS6900-X20	10Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with 20 SFP+ ports, one optional module slot.
OmniSwitch OS6900-X40	10Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with 20 SFP+ ports, one optional module slot.

Table 10: Supported OS6900 Chassis Types

The 5620 SAM Release 9.0R5 supports the following OS10K Chassis types with AOS 7.1.1R01 with node Equipment level at this release. The Chassis configurations below are available with DC power Configuration and are supported by SAM 9.0 R5.

Chassis Type	Description
OmniSwitch OS10K8-RCB-A	OS10K redundant bundle with AC power and SSL (DES,3DES,RC2,RC4). Redundant bundle includes 1 x OS10K Chassis, 2 x Fan Trays, 4 x OS10K-PS-25A power supplies, 2 x OS10K-CMM chassis management module, 2 x OS10K-CFM chassis fabric module and fully featured AOS software w/ advanced IP routing SW (IPv4/IPv6).
OmniSwitch OS10K8-CB-A	OS10K base bundle with AC power and SSL (DES,3DES,RC2,RC4). Base bundle includes 1 x OS10K Chassis, 2 x Fan Trays, 2 x OS10K-PS-25A power supplies, 1 x OS10K-CMM chassis management module, 1 x OS10K-CFM chassis fabric module and fully featured AOS software w/ advanced IP routing SW (IPv4/IPv6).

Table 11: Supported OS10K Chassis Types

The OS10K series share a family of common Network interfaces for 10 Gigabit Ethernet and Gigabit Ethernet connectivity:

NI Module	Description
OS10K-XNI-U32S	OS10K network interface card includes 32 unpopulated 10G SFP+ ports. Supports standard tables for L2, L3 and ACL policies
OS10K-GNI-C48E	OS10K Gigabit network interface card offers 48 wire rate RJ-45 1000Base-T ports. This Enhanced network interface card is MPLS ready, and provides large table support for L2, L3, and ACL policies.
OS10K-GNI-U48E	OS10K Gigabit network interface card offers 48 unpopulated wire rate 1000BaseX SFP

	ports. This Enhanced network interface card is MPLS ready, and provides large table support for L2, L3, and ACL policies.

Table 12: Supported OS10K NI Modules

7210 SAS Support

This section describes the key 7210 SAS node features supported by 5620 SAM in 9.0 releases.

Access Uplink Support in 7210 SAS-M Platforms

5620 SAM Release 9.0 provides support for the 7210 SAS-M platforms running in access uplink mode (Pure L2 Ethernet switching mode without MPLS capability). Below section describes the brief details of the platforms which can have this capability & the feature.

7210 SAS-M Platforms

7210 SAS-M is capable of line-rate switching across all its ports and is targeted for use as a CPE device or for use in aggregation in small access aggregation networks.
It is available in three variants as listed below:

- 7210 SAS-M 24F – support 24 100/1000 SFP Ethernet interfaces
- 7210 SAS-M 24F 2XFP – supports 24 100/1000 SFP Ethernet interface and 2 x 10G XFP interfaces
- 7210 SAS-M 24F 2XFP ETR – supports 24 100/1000 SFP Ethernet interface and 2 x 10G XFP interfaces and supports extended operating temperature ranges

Additionally, all the above platforms have an expansion slot and can support the following MDAs:

- 4 x T1/E1 CES MDA (Currently this MDA is not supported in Uplink mode)
- 2 x 10G XFP Ethernet MDA

All the platforms support SyncE and 1558v2 (hardware ready, software support in a future release), allowing these devices to be used in mobile backhaul networks.

Access Uplink Support in 7210 SAS-M

Access uplink support on 7210 SAS-M provides the capability to deploy 7210 SAS-M in L2 networks using QinQ uplinks. Operators who are agnostic to deploy MPLS to the edge prefer to use either QinQ/802.1ad or PBB/802.1ah in the access aggregation networks. With Access uplink (QinQ links) support, operators can use 7210 SAS-M. With the support of access uplink on 7210 SAS-M platforms, operators who want the 10G Ethernet interface have an option to deploy these devices.

With the introduction of the access uplink feature, operators intending to use L2 access networks can use the 7210 SAS-M variants where operators have a requirement for the 10G Ethernet interfaces and the additional capabilities (e.g. Y.1731 hardware timestamp, SyncE, 1588v2) of the 7210 SAS-M platform.

BFD for FRR (Bi-Directional Forwarding Detection for Fast Reroute)

5620 SAM Release 9.0 provides support to manage BFD sessions on the RSVP interfaces in 7210 SAS-M & SAS-X platforms. This would enable the use of bi-directional forwarding (BFD) to control the state of the

associated RSVP interface. This causes RSVP to register the interface with the BFD session on that interface.

BFD (Bidirectional Forwarding Detection)

Bidirectional Forwarding Detection (BFD) is intended to be a light-weight low-overhead, short-duration detection of failures in the path between two systems. If a system stops receiving BFD messages for a long enough period (based on configuration) it is assumed that a failure along the path has occurred and the associated protocol or service is notified of the failure.

When a BFD session transitions to DOWN state, the following actions are triggered. For RSVP signalled LSPs, this triggers activation of FRR bypass/detour backup, global revertive, and switchover to secondary if any for affected LSPs with FRR enabled. It triggers switchover to secondary if any and scheduling of re-tries for signalling the primary path of the non-FRR affected LSPs.

MSTP (Multiple Instance Spanning Tree Protocol)

5620 SAM Release 9.0 provides support to manage MSTP support in 7210 SAS-M platforms, MSTP would enable individual STP per VLAN; this is supported in the similar way it is supported in SR nodes.

7210 SAS-D

5620 SAM Release 9.0 provides support for the 7210 SAS-D node. The 7210 SAS-D is a new device managed by 5620 SAM and has been modeled in 5620 SAM following the existing paradigm of management for 7210 SAS family of nodes. The configuration, provisioning will be inline with the existing 7210 nodes; a new license type for SAS-D has been introduced.

Note: Please refer the latest official roadmap / release notes / Compatibility Guide for the officially supported 5620 SAM release for 7210 SAS-D.

7210 SAS-D 6F4T & ETR

7210 SAS-D is an Ethernet demarcation unit with support for 4 x 10/100/100 Base-T ports and 6 x 100/1000 SFP ports. Operators typically will use it as a customer premise unit (CPE). It is expected to support line-rate switching on all the ports. It will primarily provide services to single customer on one or more ports OR provides services to a very small group of customers. It supports transport of service traffic primarily using Ethernet QinQ uplinks. It allows for service differentiation with support for QoS per service. Additionally it supports designing highly reliable and available networks with use of G.8032 based Ethernet APS. It supports a rich set of Ethernet OAM tools that allow for quick and centralized troubleshooting in case of any problems in the network minimizing truck rolls.

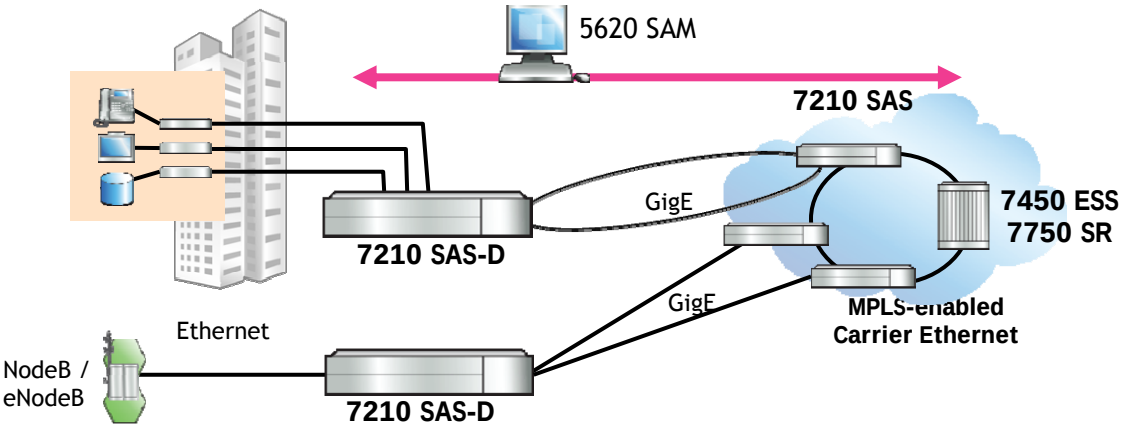
It will be available in two variants

- 7210 SAS-D supporting normal operating temperature range (i.e. 0C – 50C). Its primary application is for use as a CPE/demark unit in delivery of business services.
- 7210 SAS-D ETR supporting extended temperature range (i.e. -20C – 65C), is targeted for use in outdoor installations (e.g. mobile tower, etc.). This unit has a stratum 3 Oscillator to allow for support of syncE and 1588v2. Its primary application is in use for mobile backhaul. 7210 SAS-D ETR will be available in three options (power supply being different)
- DC unit supporting +48V DC power supply with an external backup power supply

- DC unit supporting +24V power supply with an external backup power supply
- AC unit with an external backup supply.

Target Applications

7210 SAS-D is an Ethernet demarcation device used for carrier Ethernet service delivery. It is targeted for use as a CPE device for use in business service delivery and mobile backhaul (the ETR version supports syncE and 1588v2). It supports service delivery with use of QinQ uplinks.



Ethernet Service Delivery Business and Mobile Backhaul using 7210 SAS-D

IP VPRN support in 7210 SAS M/X Platforms

IP VPRN RFC 4364 details a method of distributing routing information and forwarding data to provide a Layer 3 Virtual Private Network (VPN) service to end customers. Each Virtual Private Routed Network (VPRN) consists of a set of customer sites connected to one or more PE routers. Each associated PE router maintains a separate IP forwarding table for each VPRN. Additionally, the PE routers exchange the routing information configured or learned from all customer sites via MP-BGP peering. Each route exchanged via the MP-BGP protocol includes a Route Distinguisher (RD), which identifies the VPRN association. The service provider uses BGP to exchange the routes of a particular VPN among the PE routers that are attached to that VPN.

This is done in a way which ensures that routes from different VPNs remain distinct and separate, even if two VPNs have an overlapping address space. The PE routers distribute routes from other CE routers in that VPN to the CE routers in a particular VPN. Since the CE routers do not peer with each other there is no overlay visible to the VPN's routing algorithm. When BGP distributes a VPN route, it also distributes an MPLS label for that route. On a 7210 devices, a single label is assigned to all routes in a VPN. Before a customer data packet travels across the service provider's backbone, it is encapsulated with the MPLS label that corresponds, in the customer's VPN, to the route which best matches the packet's destination address. The MPLS packet is further encapsulated with either another MPLS label header, so that it gets tunneled across the backbone to the proper PE router.

In 4.0R1, The following support is available (For details please refer 7210 SAS User Guides):

- L3 SAP types of NULL, Dot1q and QinQ
- Service label per VRF

- Static spoke-sdp for PE to PE
- VRF export/import policies support
- QoS
    - SAP ingress classification using mac-criteria or ip-criteria (5-tuple and DSCP)
    - SAP Ingress per FC policing and per SAP aggregate policing (hierarchical policer)
    - 7210 SAS-X – SAP based egress queuing and port based marking (DSCP and dot1p bits)
    - MPLS EXP bits used for network side classification and marking for MPLS LSPs used to transport VPRN service packets
- ACLs/Filter, SAP ingress/egress ACLs (ip-criteria only)
- MP-iBGP protocol (vpn-ipv4 family only) for VPRN route exchange
    - 4-Byte ASN support available (enable/disable)
    - BGP route policy support (export/import policies)
    - Route reflector recommended (w/7210 as client only)
    - VPRN aggregate route support is available
- PE-CE routing protocol
    - Static routing with CPE-check connectivity
    - eBGP
    - MPLS LSP for VRPN data forwarding
    - RSVP-TE LSPs
    - LDP LSPs
- OAM Tools and Accounting
    - ICMP ping and traceroute applications available in VPRN context
    - vprn-ping and vrpn-traceroute OAM tools (SAA support available)
    - SAP ingress accounting records is supported
    - SAP egress accounting records is supported only on 7210 SAS-X VPRN service support is available only on 7210 SAS-M (network mode).

In 7210 SAS 4.0R1 release some of the features NOT supported please refer the node document for more details.

Port Loopback with MAC Swap (RFC 1544, No Traffic Generaion)

MAC swap enables us to swap the destination MAC and dource MAC over a sap when port is enabled for internal loopback. The purpose is to verify the SAP is intact and deliverable to customer in related to qos/acl/throughput/loss/latency etc., as defined in RFC 2544 tests before deployment. The swapping of MACs enables the packet to retrace back in the same path as it was over the MPLS cloud.

This feature is restricted to SAS-MX and SAS-X alone for 4.0R1, please refer the node document for other node support. In 7210 SAS-X, additional port is required to be configured as no service port using CLI "config system loopback-no-svcport port-id" to support loop back with MAC swap. Then loopback with MAC swap can be configured using CLI "config port <port-no> ethernet loopback internal service id sap id srcmac mac-addr dst-mac mac-addr", when this command is executed, the system enables PHY/MAC loopback on the specified port.

All the packets sent out of the port configured for loopback is received back by the system. On ingress to the system after the loopback, the node swaps the MAC addresses for the specified SAP and service. It only processes packets that match the specified source MAC address and destination MAC address, while dropping packets that do not match. It processes these packets as per the service configuration for the SAP. This is recommended for use with only VPLS and VLL services. This feature affects all the services and protocols configured on the port as the port loops back all of the packets, hence exercise extra care

when using this command. For more details and recommended procedure of usage please read the 7210 SAS user guide.

If multiple saps exist on loopbacked port, it is recommended to shutdown saps which are not configured for loopback. At a time, loopback can be enabled on only one sap. A internal loopback on the port is expected to be used with a external third-party Ethernet test device. They can be used to diagnose problems with the service provisioning or for testing endto-end performance metrics for the service.

G.8032 - Multi Chassis Support

Release 4.0R1 enhances Ethernet Ring Protection for 7210 SAS-X, to include support for dualconnected hierarchical rings and LDP VPLS access rings. Ethernet ring protection switching offers ITU-T G.8032v2 specification compliance to achieve resiliency and fast protection for native Ethernet Layer-2 networks. G.8032 (Eth-ring) is built on Ethernet OAM and is often referred to as Ring Automatic Protection Switching (R-APS).

Eth-rings are supported on VPLS SAPs (VPLS service only). VPLS services supporting Eth-Ring SAPs can connect to other rings and Ethernet services using VPLS SAPs. Eth-rings enable ring topologies for core network or access network resiliency. By utilizing rings and sub-rings, any flexible ring topology can be constructed. Support for dual-connected access rings to LDP VPLS enable inter-connection flexibility and the ability to interact with other protection mechanisms for overall service protection.

Eth-rings offer resiliency for Ethernet services optimized for ring topologies for any single link or node failure and the ability to manage traffic for both unicast and multicast services. By allowing multiple Eth-rings instances on the same physical topology, G.8032 can utilize all link resources in a ring.

In release 4.0R1, dual-connected ring support (i.e. G.8032v2) is available only for 7210 SAS-X.

Active / Standby Pseudowire Redundancy in VPLS

This feature provides the ability to use 7210 SAS devices acting as MTUs (Multi Tenant Unit Switch) to be multi-homed for VPLS to multiple PEs without requiring the use of mVPLS. In such configurations, the MTU has two spoke-SDPs to two PE devices. One is designated as the primary spoke and the other as the secondary based on configurable precedence. The secondary spoke is in a blocking state (both on receive and transmit) as long as the primary spoke is available. When the primary spoke becomes unavailable (due to link failure, PE failure, etc.), the MTU switches traffic to the backup spoke and starts sending/receiving traffic over the standby spoke.

Multi-chassis LAG (MC-LAG) in SAS M/X

Multi-chassis LAG (MC-LAG) is an extension to the LAG feature to provide not only link redundancy but also node-level redundancy. This feature uses a proprietary solution developed by Alcatel-Lucent. A proprietary messaging between redundant-pair nodes supports coordinating the LAG switchover. Multi-chassis LAG supports LAG switchover coordination: one node connected to two redundant-pair peer nodes with the LAG. During the LACP negotiation, the redundant-pair peer nodes act like a single node using active/stand-by signalling to ensure that only links of one peer nodes is used at a time.

Multi-chassis LAG is expected to be used primarily for supporting SAPs connecting to a VPLS and Epipe service with pseudowires on the network core side, so that MAC Flush messages can be used to ensure a loop-free and consistent end-to-end topology. ICB (Inter-Chassis Backup) spoke-sdp is supported for use with Epipe service in a MC-LAG configuration.

Note: Using MC-LAG for dual homing is not possible in ring topologies in the access network. The solution for such network configurations is not part of this feature. The solution is not usable for VPRN and IES SAPs. Multi-Chassis Synchronization is an Alcatel-Lucent proprietary mechanism to synchronize dynamic state information (7210 supports only synchronization of IGMP snooping information) between redundant pair nodes (inter-node state synchronization). This mechanism is not a standalone feature, but rather a mechanism required to provide a solution for redundant access (dual homing) Multi-chassis LAG. This mechanism requires that the involved nodes are running at the same system times (NTP/SNTP). It is also required that the local service configuration of the involved nodes is similar.

Split Horizon Group Support

In release 4.0R1, port-based split-horizon feature is available on 7210 SAS-X platform. Traffic arriving on an access or a network port within a split horizon group is not copied to other access and a network ports in the same split horizon group (but will be copied to an access or network ports in other split horizon groups if these exist within the same VPLS). Since split horizon is a per port feature in 7210 SAS, all SAPs associated with the port becomes part of split horizon group configured on that port.

In release 4.0R1, service-based split-horizon feature is available on 7210 SAS-X. Use of this feature is mutually exclusive to use of mesh-sdps in the same service. Only a single splithorizon group per service is available for use. Traffic arriving on a SAP or spoke-sdp configured in a service and is configured in the same split horizon group is not copied to other SAP or spoke-sdp in the same service. It can be used to disable local switching on the 7210 SAS. A loop-free topology can be achieved using split horizon on 7210 SAS switches.

Support G.8032 MEPs with 100mS CCM Timers (HW based)

This enhancement is applicable only to 7210 SAS-X. Prior to release 4.0, in 7210 SAS-X G.8032 MEPs were supporting 100ms CCM timers but implementation was in software. With release 4.0, hardware implementation of 100ms CCM timers is available for use with G.8032 only. In order to use this functionality operator needs to reserve a VLAN-ID for use with only G.8032 MEPs. No data services or control SAPs can use this VLAN-ID. More details are available in the 7210 SAS-X Services user guide.

PBB

IEEE 802.1ah draft standard [IEEE802.1ah], also known as Provider Backbone Bridges (PBB) defines an architecture and bridge protocols for interconnection of multiple Provider Bridge Networks (PBNs). IEEE defines PBB as a connectionless technology based on multipoint VLAN tunnels. MSTP is available for use as the core control plane for loop avoidance and load balancing.

The IEEE model for PBB is organized around a B-component handling the provider backbone layer and an I-component concerned with the mapping of Customer/Provider Bridge (QinQ) domain (e.g. MACs, VLANs)

to the provider backbone (e.g. B-MACs, B-VLANs): i.e. the Icomponent contains the boundary between the Customer and Backbone MAC domains. PBB encapsulates customer payload in a provider backbone Ethernet header, providing for Customer MAC hiding capabilities. With PBB, 7210 devices can be used for tier-2/3 aggregation, encapsulating customer service frames in PBB, allowing the PE-rs devices deployed in the metro core to be aware of only provider MAC addresses and for metro service scaling.

Only 7210 SAS-M (network mode only) and 7210 SAS-X devices support PBB Epipe/ELINE service (for point-to-point connectivity) and VPLS/ELAN service (for multipoint-to-multipoint connectivity). Different transport options are supported for PBB ELAN and ELINE services:

- A dedicated tunnel (one-to-one model) where one service is mapped to one backbone tunnel
- Shared tunnel (many-to-one model) where many services are sharing one backbone tunnel.

The PBB implementation supports the following capabilities for resiliency:

- management VPLS (M-VPLS) with STP
- Multi-Chassis LAG (MC-LAG).

Some of these features may be used to provide support for a number of access resiliency options towards a customer edge (CE) device or a QinQ network:

- MC-LAG offers a simple scheme where just LAG (no STP) is required on the access device
- All STP protocols are supported – e.g. RSTP, Provider/Enterprise MSTP – for compatibility with deployed customer or provider QinQ protocols

On the backbone side (B-Domain), the following options are available for tunnel resiliency:

- M-VPLS provides comprehensive loop-avoidance with load-balancing for any kind of topology through the localized, controlled use of RSTP/MSTP/PMSTP.
- Standard-based Provider MSTP is available for loop avoidance
- MC-LAG (no STP required)

Other VPLS features are also inherited by the PBB implementation: VPLS Management (FIB and SAP), L2PT, BPDU translation, filters, mirroring and QoS capabilities.
The following features are not available (This is not complete list):

- PBB-VPLS (i.e. use of SDPs in PBB service is not supported)
- Split-horizon groups (service-based)
- IEEE 802.1ak (MMRP)
- CFM (802.1ag) / Y.1731 OAM
- G.8032 and G.8031
- Black-hole avoidance mechanisms in case of MC-LAG
- B-SAP on LAG ports
- l2pt, BPDU translation across B-Domain is not supported.
- I-VPLS STP BPDU's are not transmitted over B-VPLS.

For more details please refer the 7210 Services user guide.

Default (*.*) QinQ SAPs for EPipe and PVLS in SAS-M / D

Default QinQ SAPs (notation - *.*) are used in ring ports to avoid the need to configure services on all the intermediate nodes in the ring which are transiting the service. Only one epipe service with default QinQ SAPs can be created for transit traffic on access-uplink ports. Default QinQ SAPs are allowed only on access-uplink ports and access ports. It can co-exist with 0.* SAP on an access-uplink or access port. A default QinQ SAP accepts only tagged packets. Untagged packets or Priority tagged packets are not accepted on default QinQ SAP. When using an epipe service for transit traffic in a ring deployment, no

protection mechanism (example: STP or G.8032) is supported for Default QinQ SAPs. The upstream or head-end node on which the service originates must ensure the correct path on the ring is selected using either G.8032 or STP.

Default QinQ SAP is available for use only in an Epipe and a VPLS service created with svcsap-type parameter set to "null-star". Default QinQ SAP can be configured along with other SAPs allowed in the same service (i.e. service with svc-sap-type parameter set to "null-star"). Default QinQ SAPs in a VPLS service does not support any loop-avoidance mechanisms such as STP or G.8032. It is not recommended for use in a topology where Layer-2 loop exists. It must be used carefully and is typically helpful to aggregate a set of VLANs into a service towards an upstream node in a hub-spoke network topology without Layer-2 loops.

Default QinQ SAPs is supported only on 7210 SAS-D and 7210 SAS-M (access-uplink mode). Following features are available for use with Default QinQ SAPs configured in Epipe and VPLS service (unless otherwise explicitly called out below listed features are applicable for both Epipe and VPLS service):
For Default QinQ SAPs on either access ports or access-uplink ports:

- MAC learning and aging is available for use in a VPLS service
- Per SAP Mac limit is available for use in a VPLS service
- Mac-move detection and Mac-pinning is available for use in a VPLS service
- Discard-unknown and discard-unknown-source is available for use in a VPLS service
- CFM and Y.1731 is not available for use
- STP (and all its different flavors) is not available for use
- G.8032 is not available for use
- IGMP snooping is not available for use
- L2PT and BPDU translation is not available for use
- IP interface in a VPLS service is not available in a service using this SAP.

For Default QinQ SAPs created on Access-uplink Port:

- SAP ingress qos policy is available for use
- Egress qos policy applied on an access port is available for egress shaping, scheduling and marking.
- SAP Ingress ACLs is available for use
- SAP egress ACLs is not available for use
- SAP Ingress Meter counters, SAP Ingress received count and
- SAP Egress forwarded counter are available for use (appropriate accounting records can be used)

24V Power Supply Support in SAS-M

7210 SAS-M and all variants supports +24V power supply. This allows users the choice of using a +24V DC power source to power the node. Users can use two +24V power supplies in a redundant configuration. DC power source failure detection is supported.

AC power supply use along with DC (+24V or -48V) power supply is supported from 3.0R6 release.

Configured DC power supply type (+24V or -48V) is displayed using snmp MIB object tmnxChassisPowerSupplyAssignedDCType"

Note: A mix of +24V DC and -48V power supplies must not be used together in the same chassis.

Line Timing of Ethernet Ports Using Sync-E with SSM Support

In 7210 SAS 3.0R6 release, 7210 SAS-D ETR provides support for Synchronous Status Message (SSM) also known as ESMC) for Synchronous Ethernet. SSM provides a mechanism to allow the synchronization distribution network to both determine the quality level of the clock for a given synchronisation trail and to allow a network element to select the best of multiple input synchronization trails.

Synchronization Status messages have been defined for various transport protocols including SONET/SDH, T1/E1, and synchronous Ethernet, for interaction with office clocks, such as BITS or SSUs and embedded network element clocks. SSM allows equipment to autonomously provision and reconfigure (by reference switching) their synchronization references, while helping to avoid the creation of timing loops. These messages are particularly useful to allow synchronization reconfigurations when timing is distributed in both directions around a ring.

In Synchronous Ethernet, SSM uses an Ethernet OAM PDU that uses the slow protocol subtype. For a complete description of the format and processing, see ITU-T G.8264. Copper interfaces can be used only for timing distribution. They are not recommended for use as timing references

SNMP Dying Gasp (Beta Only)

In release 4.0, 7210 SAS-D and its variants support generation of SNMP dying gasp trap on power failure. By default, the system generates EFM OAM dying gasp message. The user needs to explicitly configure the system to send out an SNMP trap on loss of power to the node.
Generation of SNMP dying gasp trap is mutually exclusive to use of EFM OAM dying gasp message. For details, please refer to the 7210 SAS-D/E System Management Guide.

This feature is not supported in 5620 SAM 9.0R5 release.

IP MTU Support on IES Interfaces

This feature allows the user to set the IP MTU to use for an IES IP interface. IP MTU ensures that the IP packets sent out of the IP interface are less than the IP MTU specified. Users configure IES IP interface on access-uplink ports for in-band management of the node. With this feature operator can specify the IP MTU to use for CPU generated IP packets (e.g. SNMP, FTP, etc.), making it possible to use different MTU (possibly smaller MTU value than the port MTU) for management traffic and service traffic that share the same port. It is available for use on 7210 SAS-E, 7210 SAS-D and 7210 SAS-M (access-uplink mode only).

Configurable Period for Writing Accounting Records to Flash

With this enhancement, users have an option to configure the collection-interval for different accounting records supported in 7210. The collection-interval determines how frequently the system polls for counters to generate accounting records that are written to flash. Users can configure values other than the default value based on the how frequently they need to gather performance statistics for different service entities. Use of bigger value for collection-interval, can reduce the number of writes and frequency of writes to the flash. It is available on all 7210 platforms.
This feature is not supported in 5620 SAM 9.0R5 release.

Enable / Disable of Management Console Ports

In release 4.0, 7210 devices support the capability to disable console. In remote deployments,this provides the operator with additional security measure. Operator can disable the use of console to prevent access to the box by a malicious user. Use of console access is not available only when the Timos image is booted. It is always available for use when the bootloader image is executing. It is available on all 7210 platforms.
This feature is not supported in 5620 SAM 9.0R5 release.

Storing of SAA results in Flash

OAM SAA test results can be saved in a file on the compact flash card, and the standard available file policy can be used to define how long the file is open/closed when 5620 SAM is informed to retrieve the file, similar to how accounting works. SAA TCAs and ad-hoc (non scheduled/non-cron) results are sent as usual. Once the OAM SAA test results are put on the compact flash card and the file is closed, a trap is sent to the SNMP trap receiver that may then opt to obtain the file and process it as desired. This feature is available on 7210 platforms.

This feature is not supported in 5620 SAM 9.0R5 release.

9500 Support

5620 SAM R9.0 R1 support the WTD 9500 MPR R3.00.00 load mobile back haul transport system load. Support includes the full node feature set with the potential exclusion of STM card support which is currently a stretch feature. In addition, the release extends support for MPR sync features introduced in previous ANSI / ETSI R2.X releases. The 5620 SAM Release 9.0 R1 likewise supports the following MPR loads from prior releases: 9500 ETSI 1.03.01E, 1.04.00E, 2.01.01E & 9500 ANSI 1.02.00A, 2.02.00A, 2.02.01A

5620 SAM adds support for the WTD 9500 MPR R3.01.00 and R3.02.00 loads. All features are supported with the exception of ERPS which is committed in the 9.0 R7 load. All existing platform versions from SAM 9.0 R1 are likewise supported in 9.0 R5.

The 5620 SAM also improves the overall mobile back haul solution with the following NMS content in this release.

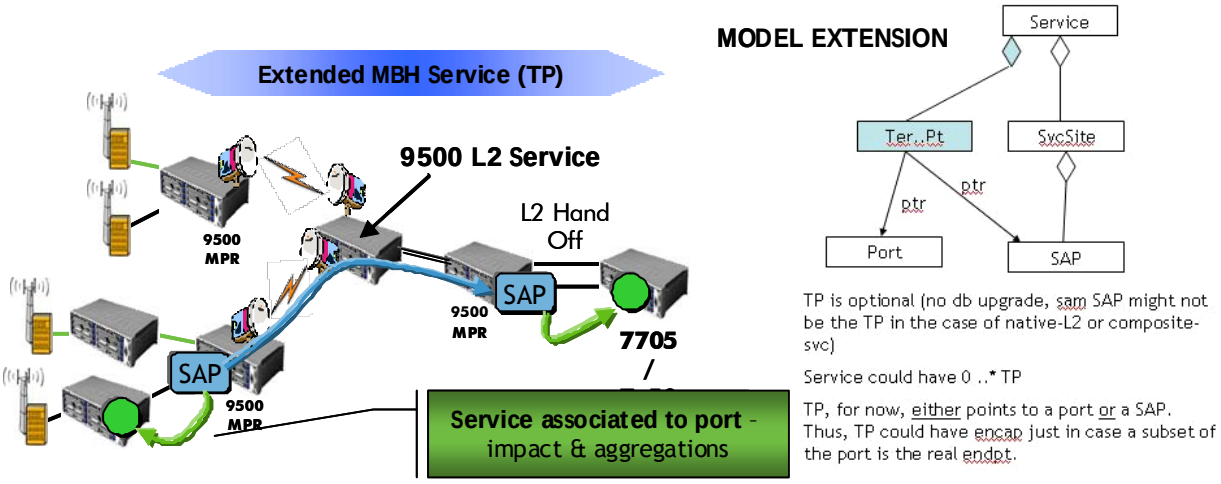
Port Segregation Usability

5620 SAM shall support admin up/down changes in the 9500 R3.X code base to make admin state IETF compliant. Note that this feature is 100% dependent on WTD committing the fix in the R3.00.00 time frame.

Extended Back Haul Service

The extended back haul service evolves existing powerful service-in-service features to be more in line with 5620 SAM evolution in the optical management space. This is done by adding a termination point to the service level that points at a far end port / near end port/sap. Termination points make it easier for a MBH service event to be correlated back to upper layer objects on other NEs such as a 7705 enhancing the overall solution as follows:

- 5620 SAM provides a service termination point (TP) associated with a far side device port such as 7705 port. Service TPs are automatically discovered as a side effect of configuring the physical port between a 9500 and IP/MPLS equipment like the SAR family.
- 5620 SAM provides support for both services terminating on 9500 or on a remote node like 7705. In cases where 9500 is the service termination a TP will point at the local service port.
- 5620 SAM correlates 9500 service faults to remote port side objects as a result of the new TP feature; eg. a service failure will correlate to port level protocols in the 5620 SAM correlation hierarchy.
- 5620 SAM service forms will display the termination end point making it easier to understand the potential impact of disabling a back haul service on microwave transport.
- 5620 SAM Release 9.0 R5 extends service-in-service by discovering the association between the 9500 back haul transport service and upper layer IP/MPLS services in the SAR family. As a result of discovery service faults in either layer are cross correlated in 5620 SAM. *Note that existing manual mapping is still provided for forward compatibility and to cover some complex corner cases.*



dot1Q VLAN Service

The 9500 R3.00 and R3.01 loads provide full 802.1Q bridging features for the delivery of Ethernet transport. The dot1Q VLAN mode generally replaces the existing ePIPE service in most common deployments of the 9500 MPR MSS4 and MSS8. The 5620 SAM fully models the dot1Q VLAN service as an end to end service that includes full radio paths. Work flows follow the existing approach of SAM with full support of service templates, components, state management and so on. Similarly all deployments are based on the SAM VLAN path construct allowing automated management of VLANs and dot1Q cross connections end to end. The dot1Q vlan service may be deployed in multi site or dual site – eg. as an epipe – modes.

9500 QoS Configuration

The 9500 MPR MSS 4/8 supports MIBs to configure QoS objects in 3.02. Specifically the MPR family will support QoS settings for the following common configurations:

- Scheduler Setting
- Mapping 802.1p or IPv4/IPv6 DiffServ Code Points
- Mapping of TMN-RF to queues
- Radio Queues Size Setting

The 5620 SAM provides policy based QoS configuration on the MPR 9500 MSS 4/8. The QoS configuration supports a single policy that manages the global scheduler and mapping settings that will include a view of the read only QoS config values. All policies will be in the SAM policy framework as 9500 based QoS and will support audits, distribution, policy IDs and so on in the normal SAM manner. An additional enhancement unqiue to 9500 is provision for QoS *bundles*.

A QoS bundle groups schedules, 802.1p / Diffserve mappings, and queue settings into a common deployment. The intention for policy bundling is to allow a customer to build a number of 'gold' standards for QoS deployment. For example, one bundle could be applied to sites with four radios in slot 1/1-1/4 and 16K queues wheras another might be for a lower capacity site with two radions in slot 1/1 and 2/1 and queus of 8K. *Customers can use the bundle to update or configure a site in 'one shot' for all the related QoS policies reducing configuration errors by enforcing consistency.*

SAP/XC Physical Link

The 5620 SAM shall enhance existing port work from 8.0 R5 that protected service instances when 9500 is terminated by a 77xx network port via a physical link. In this release extended back haul service will accommodate the access – network connection and will preserve service instances on the 9500 access port. This feature is delivered in conjunction with the extended back haul service.

Redundant Links

The 9500 adds multiple redundant link models as 1+1, N x 1+1, VCL and XPIC. The 5620 SAM adds support for discovery of redundant links, correlation of alarms across redundancy relationships, and notification to the SAM physical MAP. For example, 1+1 protected radio links are represented in the map as a link group with colouring based on the fault status. Similalry in the path layer a switch to protection is registered as an impact (on protection) with correlation up to all services associated to that end to end path. Note that some redundancy models – eg. N x 1+0 and L1 LAG – will require that the link ID be unqiue so that SAM can unambiguously associate links on both sides of a PPP-RF connections between 9500 MPRs. The recommended format of the Link ID field on the port should be LINKGROUP:LINKMEMBER in hex where LINKGROUP is the first character and LINKMEMBER are the following members. Please see the user guide for additional information on redundant links within SAM.

L2 LAG

The 9500 adds SNMP discovery support for L2 LAG in 3.01 release and then enhances LAG with configuration and assurance features in 3.02. The general intention of LAG deployment in 9500 MPR MSS is to increase radio capacity through the use of L2 or L1 LAG (3.04). The 5620 SAM supports LAG by mediating the 9500 MIBs into the standard IEEE based LAG structures achieving a common management look and feel and OSS interface with existing features. Likewise LAG is supported as a target for service paths as a VLAN path for both hop types of L1 LAG or L2 LAG. All existing SAM end to end path,

service, and assurance work flows are identical to the existing 9500 MPR features when LAG is employed making it easy to add LAG to an existing operations or OSS work flow.

Note that for SAM LAG a function to work it is critical that the links be discovered so that dot1Q configurations are properly deployed to the LAG. Therefore all radio based L1 or L2 LAG must use a unique link ID pair between 9500s so that SAM can discover link adjacency properly. The recommended format of the Link ID field on the port should be LINKGROUP:LINKMEMBER in hex where LINKGROUP is the first character and LINKMEMBER are the following members. Please see the user guide for additional information on redundant links within SAM.

Path Management: Auto Tunnel & Redundant Path Creation

The 5620 SAM supports MBH transport path creation as a VLAN path in Release 7.0 and 8.0. Paths are constructed hop by hop and may then be re-used during service creation on the 9500 MPR platforms. The 5620 SAM path record is very similar to LSP records recording a hop-by-hop path for the service. In this release, the 5620 SAM will extend path management to automate the process of creating VLAN paths for service management:

- Creation & discovery of redundant paths for 1 x (1+1) redundant links and listing of the paths that can be created for selection. Manual path management now will permit configuration of paths as an over ride of the auto path feature.
- Filtered listing of redundant paths for the VLAN group being managed as well as standard filtering.
- Creation support for 1+1 paths with improved hop by hop selection and UI filtering; eg. only appropriate candidates are presented in 1+1 cases.
- Creation of paths as a mesh or tree with multiple hub sites. Paths may be constrained by maximum hop count and bandwidth cost. Future releases will add constraint by link colouring.
- Support for 1+1 in the physical map by indicating active links and 1+1 state.

9500 Support for Channelized Automation

The 5620 SAM supports automated flows to make it easy to rapidly configure multiple channels on a channelized card. In this release the SAM supports this automated work flow for all channelized cards on the MPR in loads 3.00 or later.

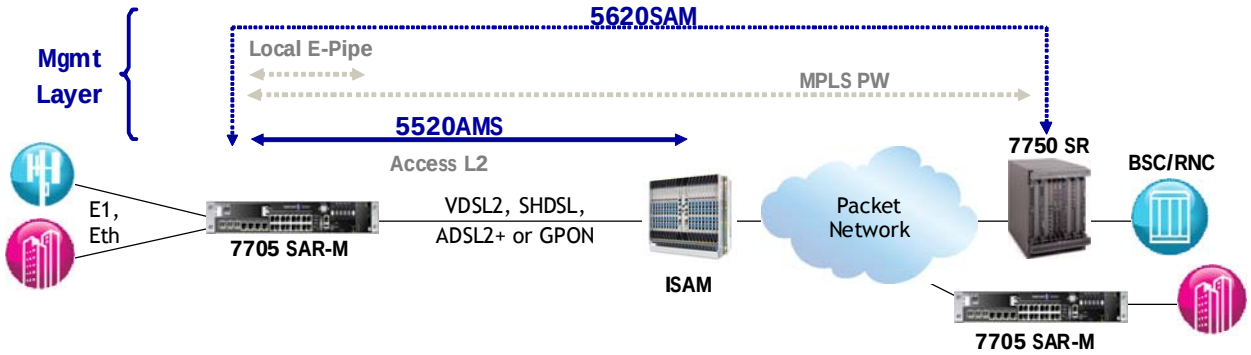
7705 Support

The 5620 SAM R9.0 R1 support the 7705 SAR R4.0 R1 load for SAR-F, SAR-8 and SAR-18 families of mobile back haul routers. Support also includes beta level content in 4.0 R1 that is hardened in the SAR 4.0 R2 load set. Note that the 5620 SAM currently excludes support of the new alarm TCA model delivered in the SAR-18 alarm model using the old alarm card model instead. Future loads of 5620 SAM will support the new card's model for TCA.

In addition to nodal feature support the 5620 SAM extends three NMS features into the mobile back haul environment.

7705 SAR-M Support

5620 SAM 9.0 R5 adds support for 7705 SAR-M R1.0 at SAR R4.0 level of capability. As such the SAR-M base chassis is discovered and managed as a SAR-M fully in SAM equipment managers, trees, and on the MAP. However all software features are managed at the same functionality as SAR 4.0 R4 or earlier; eg. one can configure, see faults and manage 4.0 R2 service features but wil have no access to R1.0 R1 features. SAR-M GPON and xDSL daughter cards are expected to be managed by AMS and, hence, in SAM 9.0 R5 the management model is as shown below. The SAM managed the IP/MPLS services and infrastructure whereas AMS manages the L2 interfaces and protocols in the network.



Full management of the SAR-M R1.0 R1+ software feaures and the GPON / xDSL hardware modules will be provided in SAM 9.0 R7. Likewise the 5620 SAM will support upgrades from the 9.0 R5 support level to 9.0 R7.

802.1ab LLDP Support

In addition to standard 5620 SAM 802.1ab LLDP support, the 5620 SAM platform accommodates the special nature of mobile back haul services via a 9500 transport. In such cases the 9500 back haul service represents a lower level link discovery that interacts with the edge-to-edge LLDP that may exist between SAR and SR family routers. Whenever a physical link exists between a 7705 running LLDP and a 9500 node the discovery process is modified for LLDP to avoid MAP clutter and to better represent the actual connectivity.

- The 5620 SAM discovery process is enhanced to re process LLDP adjacencies whenever a physical link exists between 7705 and 9500 ports.
- The MAP will not show edge-to-edge LLDP TPMR adjacencies treating them like ‘non-TPMR’ adjacencies; e.g. edge-to-edge adjacencies are dotted and hidden by default avoiding significant MAP clutter.
- The MAP is enhanced to show via link colouring that a 7705 – 9500 link has both the port level adjacency and edge-to-edge LLDP adjacency present when so discovered.
- The MAP allows highlighting of the LLDP adjacency by listing ‘Upper Layer Adjacency Links’ which results in a list of LLDP sessions that can be highlighted across the physical map. Highlights will traverse both 7705 and 9500 links.
- The MAP allows highlighting of the LLDP adjacencies via the menu system as well.

Service Re Targeting

5620 SAM 8.0 offered the ability to re target – eg. re groom – services from one SAR port to another port or even between ports on different SAR. Re targeting provided an easy UI for such grooming activities and was based on the SAP copy – move features within SAM. SAM 9.0 R1 extended service re targeting from ePIPE (8.0 R5) to cPIPE. Likewise in SAM 9.0 R7 re targeting will be extended to the aPIPE, fPIPE and hPIPE service features offered in 5.0 R1 and later.

DCR 00597975 SAR Support for Channelized Automation

The 5620 SAM supports automated flows to make it easy to rapidly configure multiple channels on a channelized card. In this release, the 5620 SAM extends the automation feature to the channelized cards on the SAR platform such as the STM line card. User may now easily create common channel configurations across a card in a small number of selections just as is supported for 7710/7450/7750

Generic Network Element (GNE) Support

This feature provides a simple mechanism to extend the service and composite service to include GNE service objects, namely, GNE service instance (or GNE service site, GNE UNI and NNI service interface). A new service site type called GNE site, and a new SAP type called GNE service interface, are introduced. GNE service interfaces are specific to GNE sites. GNE sites can be part of most types of services. The service map and the composite service flat map now include GNE service sites and GNE service interfaces.

GNE sites and GNE SAPs are manually created in 5620 SAM. Note, these objects are created in 5620 SAM only, they are not actually deployed to the GNE node. Using scripts is still the only way to configure the objects from 5620 SAM to the node.

In addition to the existing scripting functionality provided in the *'Scripts'* tab, there is a separate feature currently underway in 9.0 R5 to enhance the scripting functionality by allowing scripts to be associated with a specific object type. Thus, the user can associate scripts to the GNE site or a GNE service interface.

The service manager automatically creates a VLAN uplink between the GNE site and a SR site based on the existence of the physical connection (LLDP or manual) between the two NE's, the service type, and the SAP configurations between the two sites. If the sites are configured in different services, then a composite service can be formed with a SCP-to-SCP connection (made possible by another 9.0 R5 feature).

There is no operational or admin states applied to the newly introduced objects. The operational state shall be shown as unknown on the GUI form and service map.

No new alarms are introduced. No existing alarms are applicable. As a result, there won't be any alarms raised for the GNE sites and the GNE SAPs. In Release 10.0, 5620 SAM GNE trap mapping could be enhanced to have service alarms associated with the service instance or interface (instead of the GNE).

Services associated with a GNE node will be listed in the new *'Services'* tab on the Network Element configuration form. This tab is only displayed when the network element is a GNE. Note, this is a very low priority requirement.

Since the GNE service instances and the GNE SAPs are 5620 SAM-only objects, they will be removed if a GNE node is unmanaged.

Supported Services

GNEs are supported in the following types of services:

- all VLLs (Epipe, Apipe, Fpipe, Ipipe, Cpipe)
- all MPR VLLs (Cpipe, Apipe, Epipe)
- VPLS, M-VPLS
- VPRN
- IES
- VLAN (OMNI mode only, the 9500 is not supported)

The GNE support is excluded from the mirrored services, the optical transport services, and the 9500 VLANs.

Provisioning Procedure Example

Configuring a GNE site in a VPLS service with one SR site

1. Scripts are created for the GNE site and the GNE SAPs.
2. Discover the GNE node. Discover the SR node. Add a cable between the SR and the GNE (could be done automatically with LLDP if available).
3. Create a VPLS service in 5620 SAM, add the SR as a VPLS site, create a SAP from a port connected to the GNE.
4. Add the GNE as a GNE site, create a GNE NNI service interface on the port connected to the SR. At this point, the VLAN uplink should be created between the two SAPs.
5. The user can now configure the service objects on the GNE via scripts by selecting the right script(s) from the service site or interface.

ESM

The 5620 SAM allows the creation of NAT static port forwarding entries via two methods, a synchronous method that will respond directly to the XML request and an asynchronous method that will convey the result of the XML request via JMS.

5620 SAM maintains the NAT static port forwarding entries in its DB and also provides a method to synchronize these entries between two nodes. This can be done individually via an XML method or in batches via the GUI only.

ESM over ATM (PPPoA/PPPoEoA)

The 5620 SAM supports configuration of ESM and MSAPS on ATM interfaces in Routed CO. Subscriber sessions will be PPPoA or PPPoEoA over ATM interfaces. These sessions will be visible in SAM. SAM also supports configuration of PPPoE policy for pre 9.0 R4 SR routers and the generic PPP policy for all PPP type sessions for post 9.0 R4 SR routers

SRRP Enhancements for PPPoE Redundancy

5620 SAM supports the configuration of SRRP enhancements (support for rate sharing, route policy enhancements for SRRP state advertisements) to support PPPoE redundancy.

Multicast Traffic Replication on Subscriber Interfaces

The 5620 SAM supports configuration of IGMP redirection and replication on subscriber interfaces.

DS-Lite

5620 SAM supports the configuration of DS-Lite entries.

NAT44 Enhancements (Network Address Translation)

1. Provisioning Static Port Forwards (Carrier based, L2 Aware, DS Lite) via SAM /OSS (functionality not available via CLI)
2. Synchronization of Static Port Forwards to redundant nodes

DHCPv6 Server

1. Ability to specify IPv6 address pools in 5620 SAM.

Residential IP Transit Subs: Static Subs (CLI/SNMP)

In many cases it is not possible or practical to implement application assurance at the edge of the network – either because the edge router does not support the AA-ISA, or because sparse subscriber density makes it commercially impractical to deploy the AA-ISA at the edge.

As of 9.0 R1 the AA-ISA supports 'residential transit subscribers', which allows the AA-ISA to be deployed one-hop-back from the edge.
This feature is added to support residential transit subscriber policies, transit subscriber policing and transit subscriber accounting.

Application Assurance

RFE 99246: ISA-AA Scale Config

An AA VPN policy is generally administered using a per-site (aa-subscriber) policy attribute assignment (ASO override), as opposed to a service profile based model commonly used for residential services. Due to this, the number of attributes and values of ASOs that can be needed in an AA VPN service will be much larger than ASO scale needed for residential uses.
On the other hand, the number of AA subscribers needed per node and per ISA is much smaller for VPN services, and the size of each in bandwidth is generally much larger than residential.
This feature is added to place an AA-group into a mode optimized for VPN scale requirements

- Max # AA subs per ISA = 8k
- ASO characteristics / partition = 128
- ASO values / partition = 1000
- ASO characteristics / group = 3000

- ASO values / group = 20000

In the default residential mode, the limits are unchanged from previous releases.

AA Policer Resource Alarms

In some situations an AA policer may not be instantiated so network & service behaviour will not be as intended. This feature allows 5620 SAM to capture alarms about this condition and reflect it as a warning alarm within the Alarm Manager.

App Performance Statistics for VoIP/Video/Audio

As part of the application assurance function in 9.0 R1, the MS-ISA, is capable of providing performance and quality of experience measures for RDP/UTP voice/video and audio applications via cflowd.

This Application Performance Stats features allows the configuration of the flow sample, rate at an AA group level, as well as enabling/disabling cflowd publication for specific RTP/UDP applications and application groups at an AA partition level.

RFE 91494: TLS Certificate Expression Matching

The feature allows the configuration of app-filter expressions that string match on the TLS certificate Subject Name.

Improved Overload Handling

A mechanism is required protect against potential AA VPN discards when resources are exceeded on the ISA card

This feature allows configuration of AA-ISA traffic cut-through on a per-ISA group basis. There are two states of overload cut-through affecting AA traffic:

1. Normal operation – no cut-through
2. All traffic cut-through on subscriber context with default subscriber policy applied.

When enabled the WA-shared-buffer-wmark threshold values used for alarming will also be used to trigger overload cut-through.

ISA Capacity Information

This feature allows improved visibility of ISA capacity by providing new ISA loading statistics to allow operational planning of ISA overload monitoring and mitigation. The table below shows previously supported, as well as new for 9.0 R1, ISA capacity loading metrics.

Parameter	Current	Average(I)	Peak(I)
active flows	existing	existing	existing
flow setup rate	existing	existing	new
traffic rate	existing	existing	new
Packet rate	new	new	new
active subs	existing	existing	new
downloaded subs	existing	existing	new
flow resources in use (3M - #free flows = active flows + wildcard flows + …)	new	n/a	n/a
ISA AA sub Stats count allocation	new	n/a	n/a
ISA Capacity cost	existing	n/a	n/a

In addition to the total flow threshold event currently supported (flow count threshold), the node is to raise traps when the current load exceeds configurable capacity thresholds (high and low watermarks) for:

- per-ISA total flow setup rate
- ISA traffic volume

RFE 101156: AA VPN Partitioned Group Scale Increases

The node has implemented new scale limits for objects related to AA VPN partitions. The feature in 5620 SAM is to ensure previously enforced limits are re-aligned.

Customer Level Apdex/MOS Thresholds

This features allows thresholds to be defined on a per business customer basis for MOS scores and Apdex scores independently. These thresholds, when used in conjunction with AA application performance reporting (TCP, and RTP/UDP respectively) allow the Apdex scores and MOS scores, collected by 5670 RAM, to be processed into an application state. The applicable states for Apdex and MOS scoring are detailed in the table below:

Apdex	MOS
Excellent	Excellent
Good	Good
Fair	Fair
Poor	Poor
Unacceptable	Bad

Business IP Transit Subs: Static Subs (CLI/SNMP)

In many cases the network toplogy does not support (physically or commercially) the placement of AA-ISA at the edge closest to the VPN site:

- The edge node does not support AA-ISA
- The subscriber density does not justify an AA-ISA at the edge
- The VPN site is on a different network

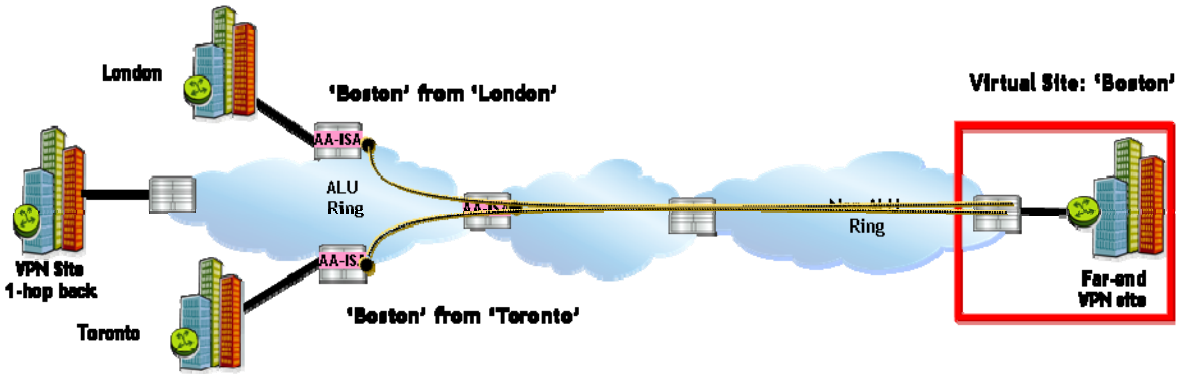
As of 5620 SAM Release 9.0 R5, the AA-ISA supports 'business transit subscribers', which allows the AA-ISA to be deployed one-hop-back from the edge.

This feature, consistent with the existing AA transit subscriber feature, is added to support transit subscriber policies, transit subscriber policing and transit subscriber accounting for business transit subscribers.

Business IP Transit Subscriber Aggregation

In scenarios where the VPN site exists on the far side of the network, not directly accessible by AA-ISA, usage data can be collected by instantiating business transit subscribers on the relevant AA-enabled local nodes. In order to put together a more complete view of traffic in and out of the 'virtual VPN site' it is necessary to aggregate usage data from each of the transit subscribers that represents this site.

This feature allows multiple tranist subscribers to be identified as part of a single logical application assurance entity.



DCP Summarization Groups

In support of 5670 RAM, this feature allows for the creation and management of summarization groups.

The function of 5670 RAM DCP is to collect and analyze cflowd records produced by the AA-ISA for the purposes of enabling application performance analysis. Summarization groups optimize the benefit of this feature by enabling complete flexibility in how terms of how DCP will summarize data.

In 5620 SAM Release 9.0 R5 operators can enable DCP summarizatio on AA-enabled services. As this occurs two service-wide groups will be created:

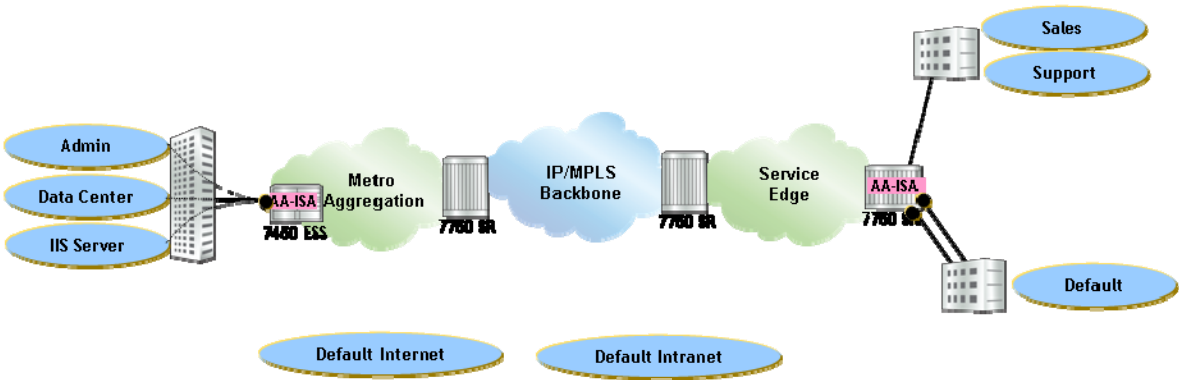
- Internet
- Intranet

With no further action all cflowd records will be sorted into either 'Internet' or 'Intranet' based on RFC 1918: Address allocation for private internets.

Operators may also define custom groups for the services. Custom groups are explicitly associated to a business AA subscriber (SAP, Spoke, or business transit subscriber). Operators also define the IPv4 membership rules for a specific group in the form of:

- IP address range
- IP subnet

5670 RAM uses this information to aggregate, and ultimately report on application performance data in the form of 'local group' to 'remote group'



Usage-Based Billing Attributes

This feature extends aspects of the AA policy specifically to extend the application assurance capability into felxible usage based billing:

Within the AA policy operators can define a 'Charging Group' to each application and each application group. There are eight charging groups in total. By default every application and application group is associated to charging group 1.

Within the AA policy operators can define a quota and three thresholds (low, medium and high) per charging group within the app-profile. Also within the app-profile operators can define a billing reset date as an integer between 1 – 28. Subscriber association to an app-profile defines the specific service tier criteria required to faciliate usage based billing.

Usage based billing attributes are not pushed to the node, but are available to northbound applications (like 5670 RAM) via 5620 SAM-O.

Runtime Attributes

In support of 5670 RAM this feature adds specific attributes to be used by the reporting system.

- Standard/subscribed app profile: Associated to an ESM AA-sub, a text field intended to be populated by the app-profile most generally associated to the sub.
- Current app profile: Associated to an ESM AA-sub, a text field intended to be populated by the current app-profile. This is used to identify subscribers that went over their quota limit (and were subsequently assigned a new app-profile)
- SAP class. Used to identify SAPs of a particular class for batch reporting
- SAP-type description: Used to classify SAPs for batch-reporting
- SAP total upstream bandwidth
- SAP Total downstream bandwidth

- Per class-of-service (COS) upstream traffic (to support 4 COS)
- Per class-of-service (COS) downsteam traffic (to support 4 COS)
- SAP Site name: friendly name for the SAP for use in reporting
- SAP/Service/Customer: friendly name for the customer for use in reporting
- Application type: for use in reporting
- Application group: for use in reporting

Runtime attributes are not pushed to the node, but are available to northbound applications (like 5670 RAM) via SAM-O.

Support for AA on 7750 SR-c12

This feature enables hardware and policy support for application assurance running on 7750SR-c12.

Optical Node Management

Release 9.0 R3 Optical Support – At a Glance

Supported Network Elements

- 1830 PSS-32/16 Release 2.5 and 2.5.1, 3.5, 3.5.1, 3.5.2
- 1830 PSS-4 Release 1.5
- 1830 PSS-1 GBEH Release 2.5, 2.5.1, 2.7
- 1830 PSS-1 MD4H Release 1.5, 1.7
- 1830 PSS-1 AHP Release 1.0

Optical NMS features

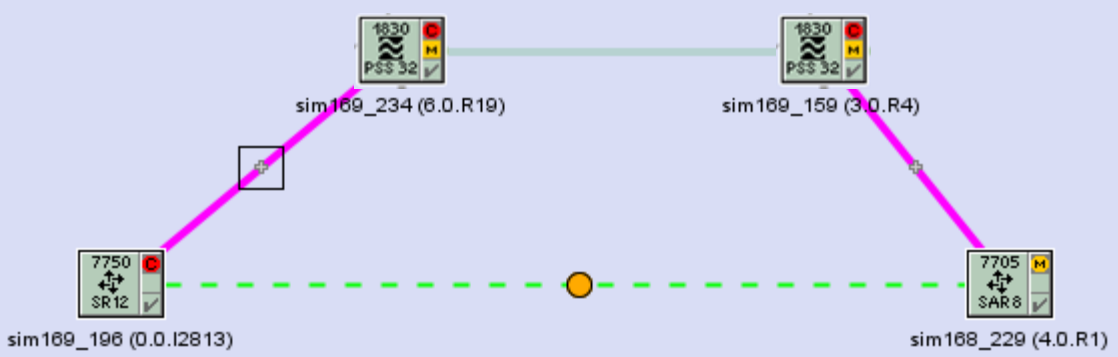
- Discovery and Provisioning of Optical Transport Services
- Provisioning of optical transport services terminating on IPD routers
- Support for Span of control on optical network elements and optical transport services
- Support for physical map display of optical and IP network elements and links
- Support for alarm management of optical alarms
- Support for statistics collection and display
- Support for optical power graph of all measurement point on an optical transport service
- Support for optical power graph of all channels on an optical port
- Support for automated launch power management for optical transport services with dangling transponders on SR routers

Optical Platform

Physical Topology Map

The physical topology map will display 1830 PSS network elements.

If there are Ethernet adjacencies discovered between IP ports then the topology will look as follows:



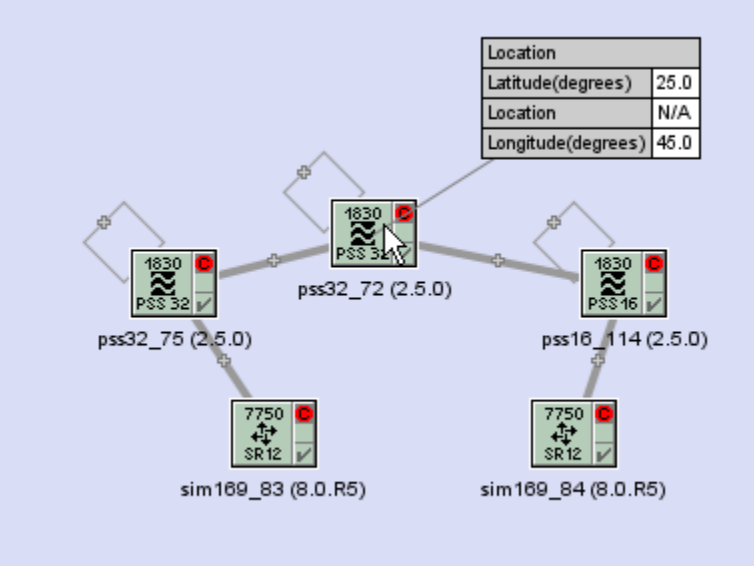
Links between 1830's (inter node) and links on 1830's between cards (intra-node) are manually provisioned from 5620 SAM or on the node. The latter can be discovered by the 5620 SAM if they are provisioned onto the node during the commissioning phase. The typical scenario is for the intra-node links to be configured during the commissioning phase. Links configured on the NEs will be discovered by 5620 SAM. There is no link layer discovery protocol supported on the network elements.

Links that have at least one end (or both ends) on an 1830 are called Optical links. They are modeled, listed and managed as separate objects to Physical links which exist between routers. Fiber links internal to the network element are also shown as Optical links and look like a loopback on the network element.

Optical links between 1830's and routers are manually provisioned from 5620 SAM.

By default, the 5620 SAM physical topology map show routers and 1830's with physical and optical links. Using map filters the map can be changed to show only routers with the links between them or only optical NE's and the optical links with attached routers.

Info boxes with permanent or mouse over display are supported on the map for 1830 PSS network element.



Span of Control

Optical NE management uses the 5620 SAM scope and span rules.

Optical NE's can be placed in a Router Span to restrict access and visibility to assigned user groups.

Optical transport services can be placed in an Optical Service span to restrict access and visibility to assigned user groups.

Other supported span classes such as scripts continue to be supported as before.

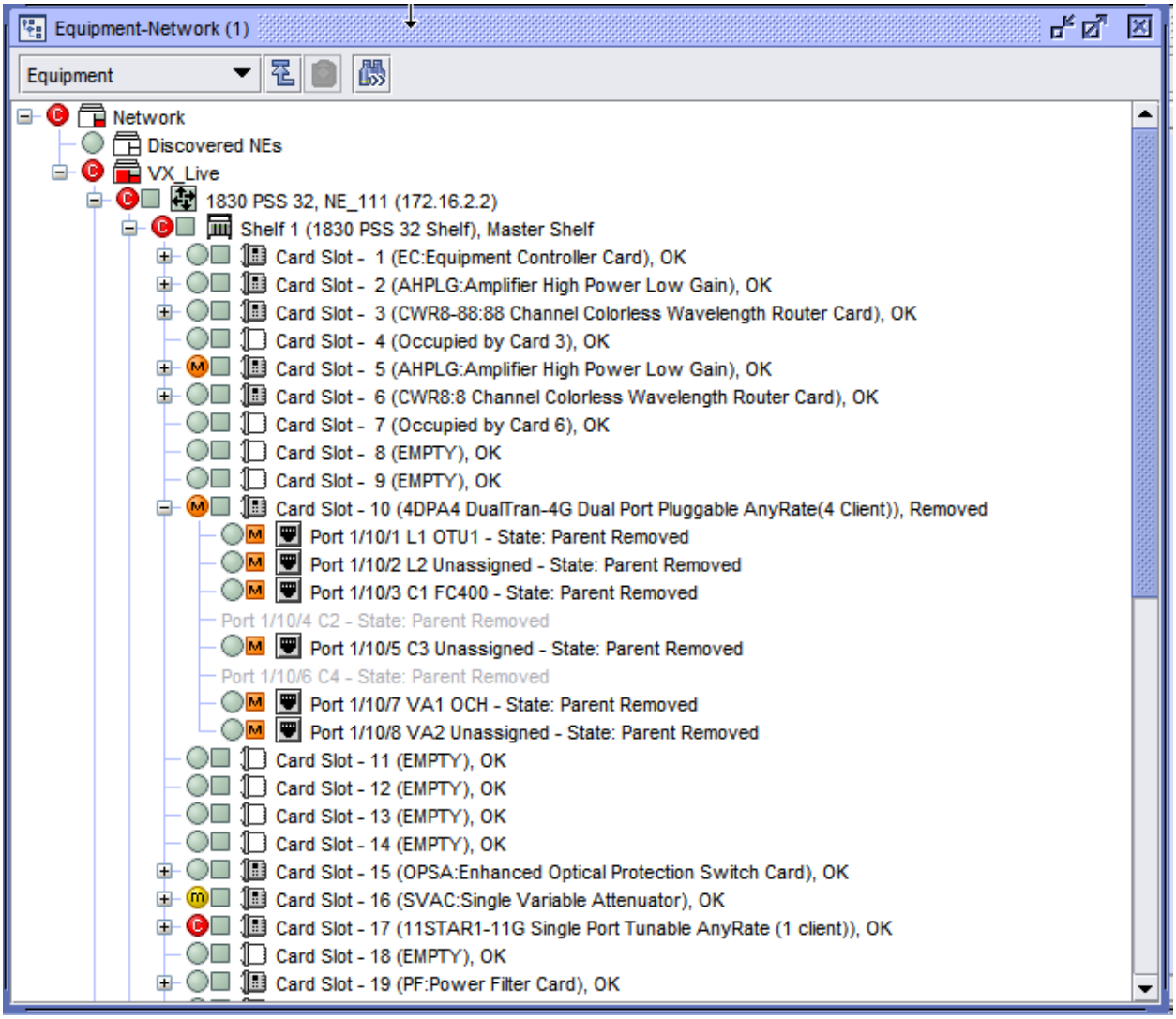
Optical Equipment Management

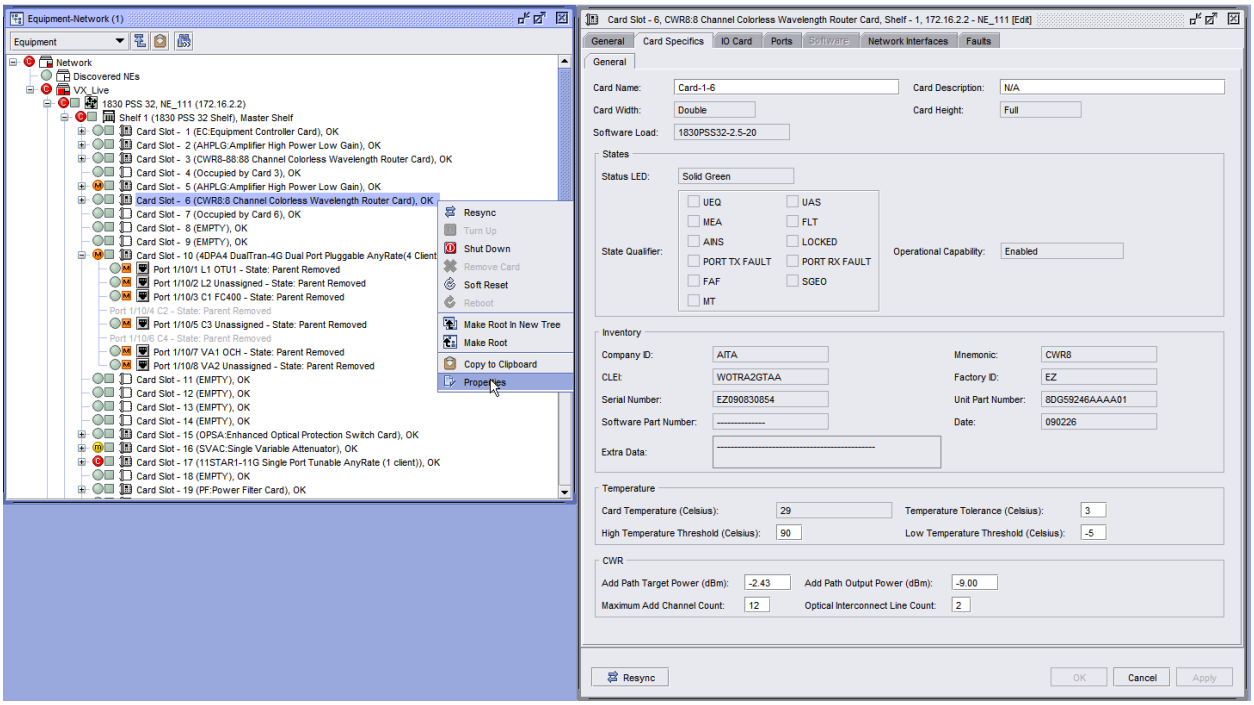
Network Element Discovery

The 5620 SAM discovery rule has been extended to discover supported 1830 PSS network elements. Discovery behaviour and placing discovered NE's on the physical topology map and in the equipment tree is unchanged from previous 5620 SAM releases.

Network Element Configuration

1830 network element shelves, cards, ports and sub ports can be viewed and configured from the 5620 SAM.


Equipment-Network (1)
Equipment
Network
Discovered NEs
VX_Live
1830 PSS 32, NE_111 (172.16.2.2)
Shelf 1 (1830 PSS 32 Shelf), Master Shelf
Card Slot - 1 (EC:Equipment Controller Card), OK
Card Slot - 2 (AHPLG:Amplifier High Power Low Gain), OK
Card Slot - 3 (CWR8-88:88 Channel Colorless Wavelength Router Card), OK
Card Slot - 4 (Occupied by Card 3), OK
Card Slot - 5 (AHPLG:Amplifier High Power Low Gain), OK
Card Slot - 6 (CWR8:8 Channel Colorless Wavelength Router Card), OK
Card Slot - 7 (Occupied by Card 6), OK
Card Slot - 8 (EMPTY), OK
Card Slot - 9 (EMPTY), OK
Card Slot - 10 (4DPA4 DualTran-4G Dual Port Pluggable AnyRate(4 Client)), Removed
Port 1/10/1 L1 OTU1 - State: Parent Removed
Port 1/10/2 L2 Unassigned - State: Parent Removed
Port 1/10/3 C1 FC400 - State: Parent Removed
Port 1/10/4 C2 - State: Parent Removed
Port 1/10/5 C3 Unassigned - State: Parent Removed
Port 1/10/6 C4 - State: Parent Removed
Port 1/10/7 VA1 OCH - State: Parent Removed
Port 1/10/8 VA2 Unassigned - State: Parent Removed
Card Slot - 11 (EMPTY), OK
Card Slot - 12 (EMPTY), OK
Card Slot - 13 (EMPTY), OK
Card Slot - 14 (EMPTY), OK
Card Slot - 15 (OPSA:Enhanced Optical Protection Switch Card), OK
Card Slot - 16 (SVAC:Single Variable Attenuator), OK
Card Slot - 17 (11STAR1-11G Single Port Tunable AnyRate (1 client)), OK
Card Slot - 18 (EMPTY), OK
Card Slot - 19 (PF:Power Filter Card), OK



Statistics Collection

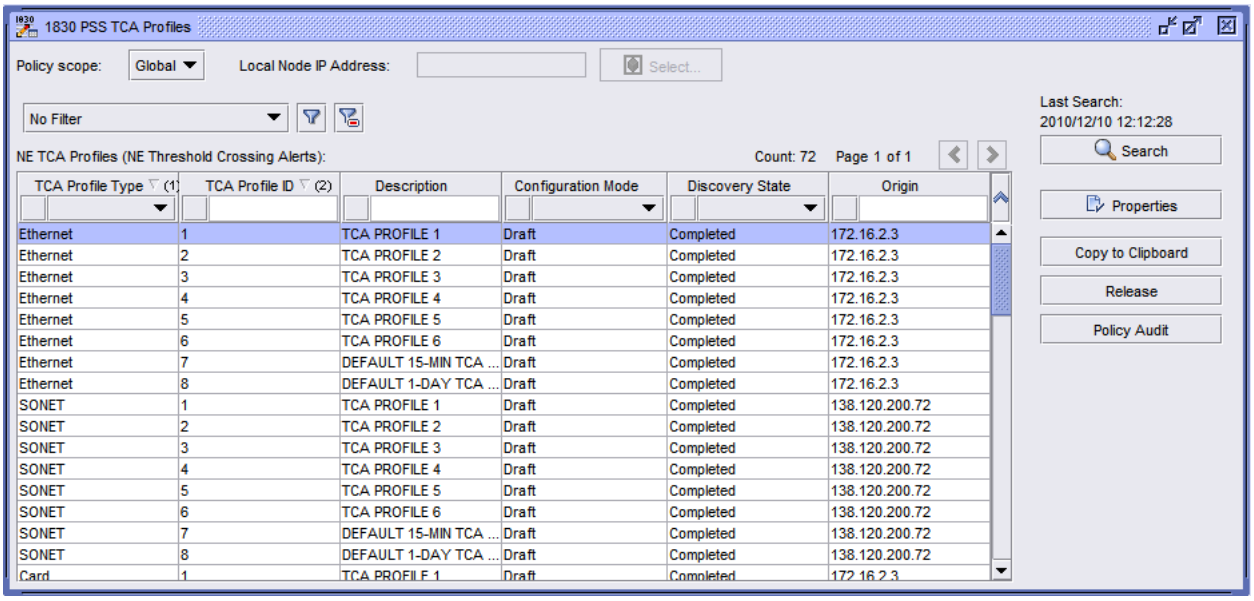
The 5620 SAM supports the collection and display of statistics counters from the 1830 PSS network elements.

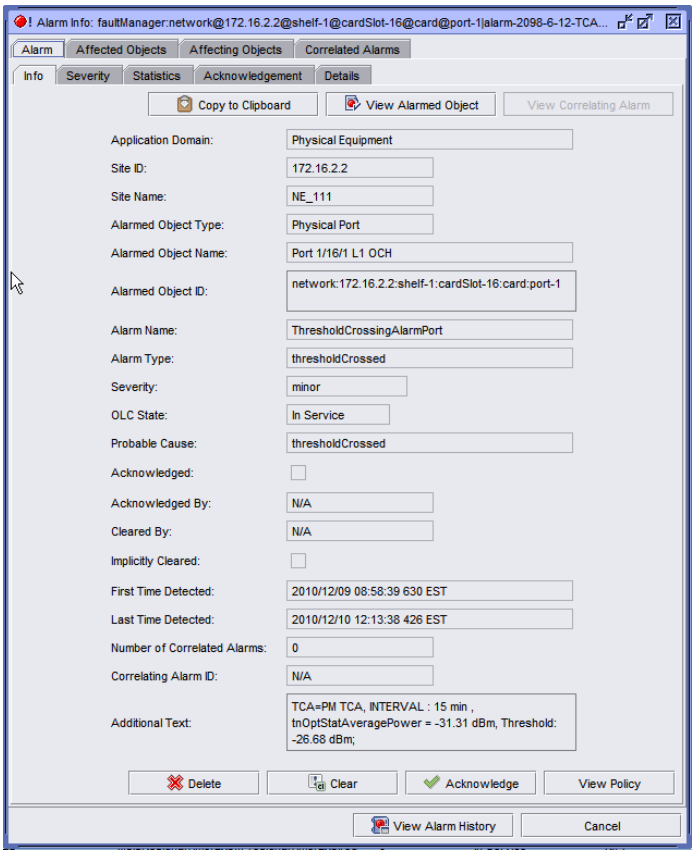
Statistics can be collected in one of three ways

- On demand – on a specific object by pressing the Collect button the specified counters are retrieved once from the network element
- Scheduled collection – using a collection policy the specified bins on the specified network elements are retrieved at the rate specified in the policy
- Real Time – the specified counters are polled and displayed on the plotter

Statistics can be collected from 15 minute and 24 hour bins that are accumulated on the network element.

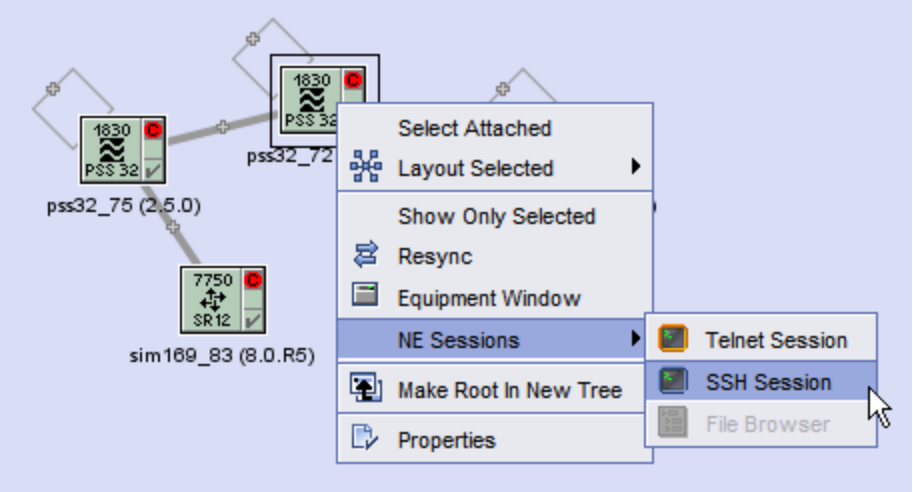
TCA (threshold crossing alerts) can be configured on the network element from 5620 SAM using the TCA policy configuration form. The TCA's appear as alarms in the 5620 SAM alarm window. The alarms are non self clearing and must be manually cleared.





Node Sessions

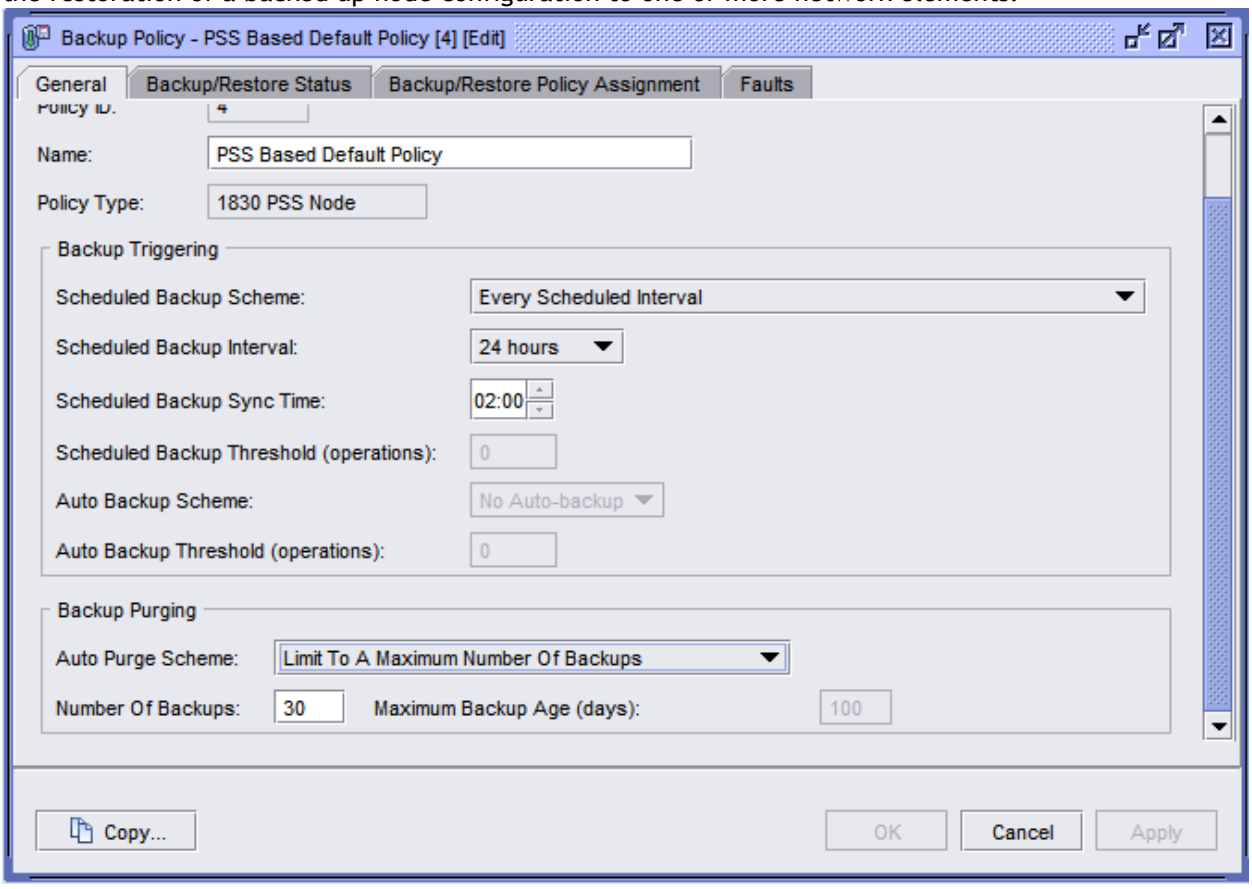
The 5620 SAM provides the capability to telnet/SSH into the node directly from various places such as from the equipment window and the map.



WebUI login is not provided directly from the 5620 SAM interface but can be achieved directly from an Internet Explorer browser.

Node Configuration Backup and Restore

The 5620 SAM supports the scheduled automated backup of 1830 PSS node configurations, as well as the restoration of a backed up node configuration to one or more network elements.



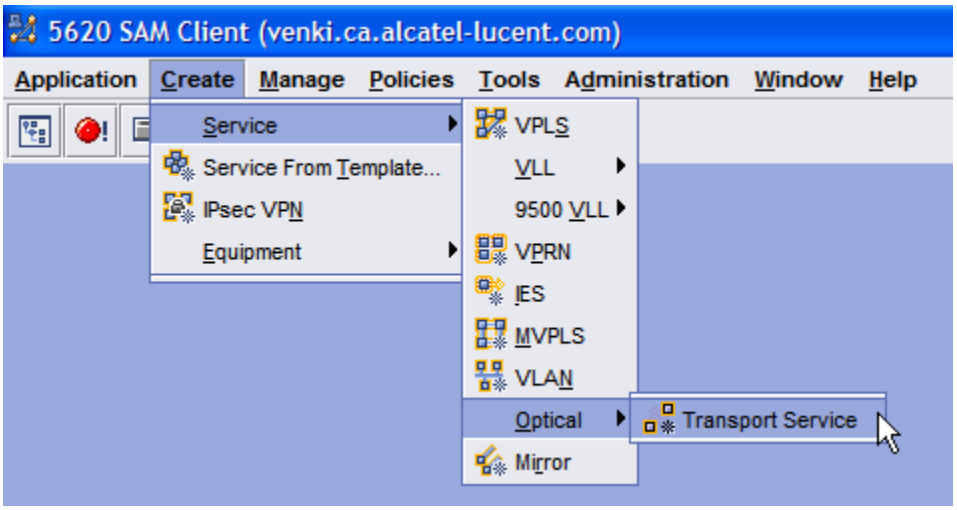
Dry Contacts

5620 SAM supports the configuration and reporting of Dry Contact alarms on the 1830 PSS family of network elements.

Optical Service Management

Service Provisioning and Discovery

The 5620 SAM supports the creation of Optical Transport Services. The workflow to create these services is very similar to the VLL service creation. Optical transport services are point to point services.



5620 SAM supports the provisioning of protected and unprotected optical transport services. Protection modes that are supported are:

- Y-Cable
- OPS

5620 SAM supports the provisioning of divers route services. In this case user specifies only the endpoints and 5620 SAM will provision two unprotected services with diverse routes.

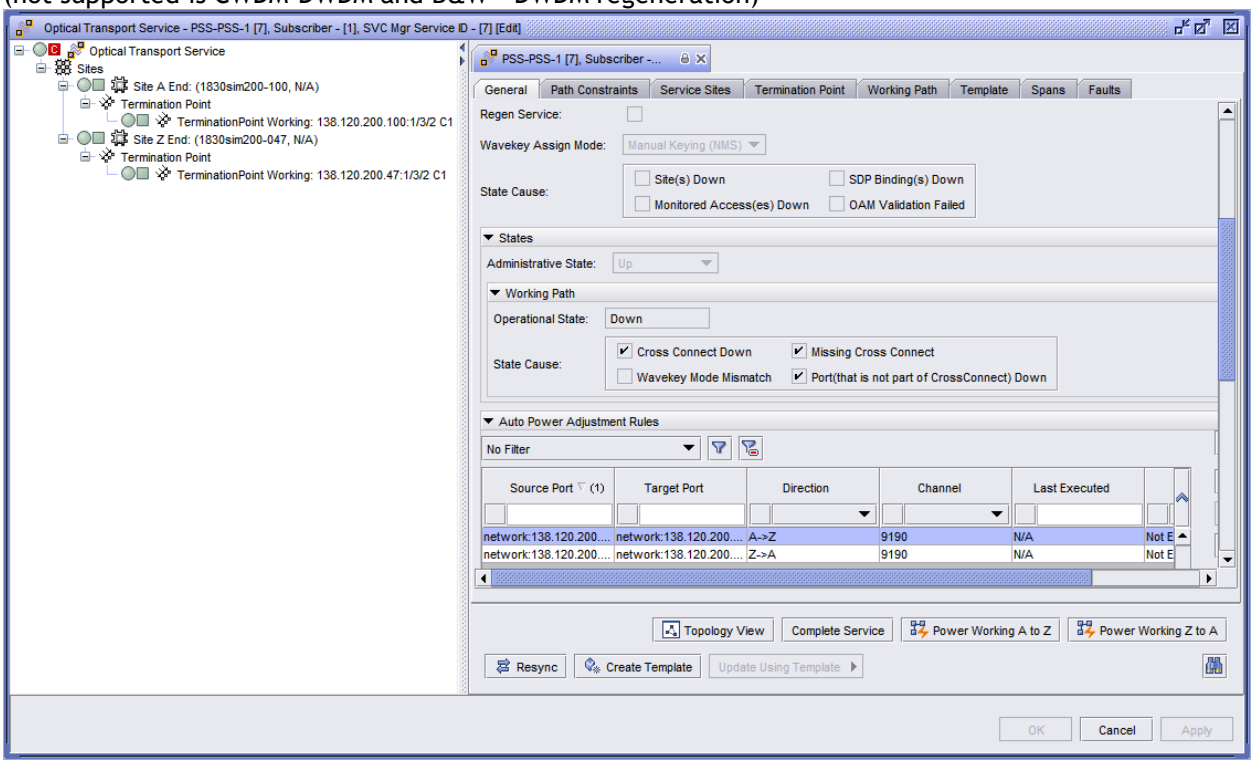
5620 SAM supports the discovery of protected and unprotected optical transport services. The services could have been provisioned on the NE's via another management system or via CLI, WebUI etc. Protection schemes supported for discovery are Y-Cable, ESNCP and OPS.

Association of 2 discovered unprotected services into a single diverse route service is supported in 5620 SAM.

5620 SAM supports the provisioning and discovery of regenerated optical transport services using the same or different wavelengths. 5620 SAM supports the provisioning and discovery of 3 configurations of regenerated services:

- DWDM-DWDM and CWDM-CWDM back to back OT's connected via their client ports
- DWDM-DWDM cross regen on OTs that support CrossRegen mode between their line ports
- DWDM-DWDM unidirectional single port regen

(not supported is CWDM-DWDM and B&W – DWDM regeneration)



Service Configurations

5620 SAM supports the provisioning of 2 major groups of Optical transport service configurations:

- Services that terminate on routers. The following non optical network elements are supported: 7750SR, 7450 ESS, 7705 SAR, 7210 SAS. All types within these families are supported, e.g. SR-7, SR-12 etc.
- Services that terminate on supported 1830's. These service configurations are based on the service types defined on the 1830 Product Information and Planning Guide.

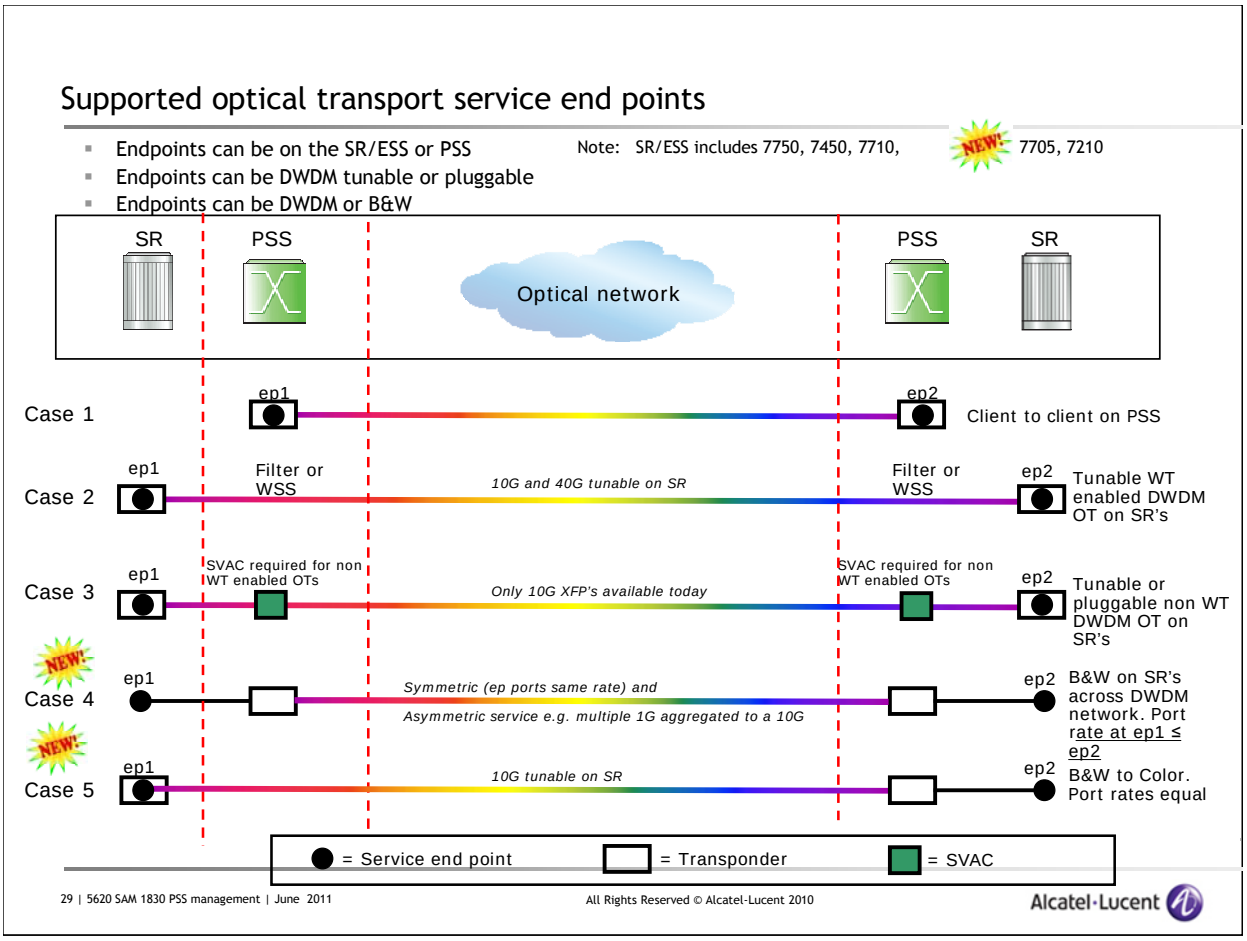
The workflow in both cases is the same.

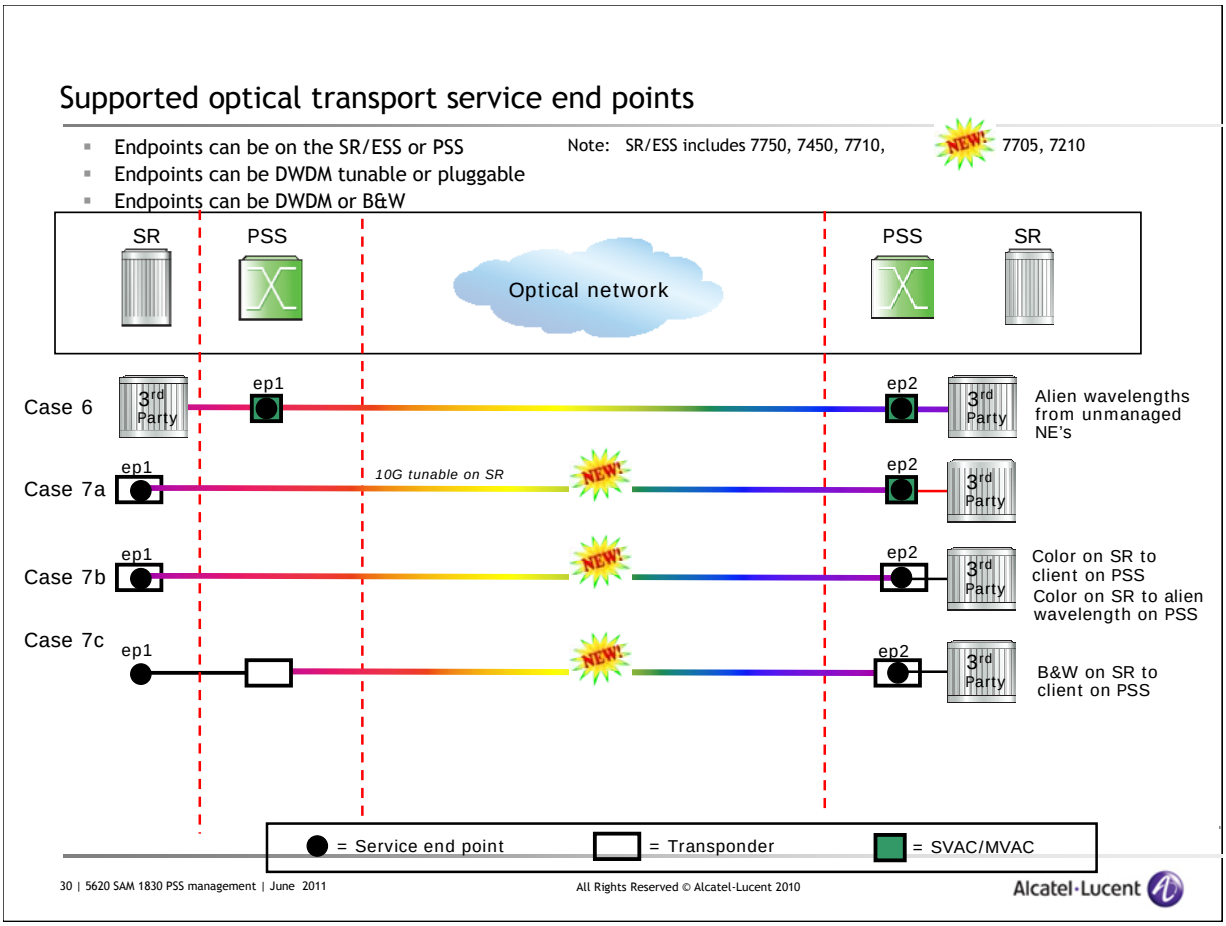
5620 SAM supports the provisioning of hybrid optical transport services where one end is a router and the other termination is on a 1830 PSS.

5620 SAM supports the provisioning of services where the port data rate of the two termination points is different e.g. in the case of aggregation services.

5620 SAM supports the creation of DWDM, CWDM and B&W optical transport services in FOADM, TOADM and ILA configurations.

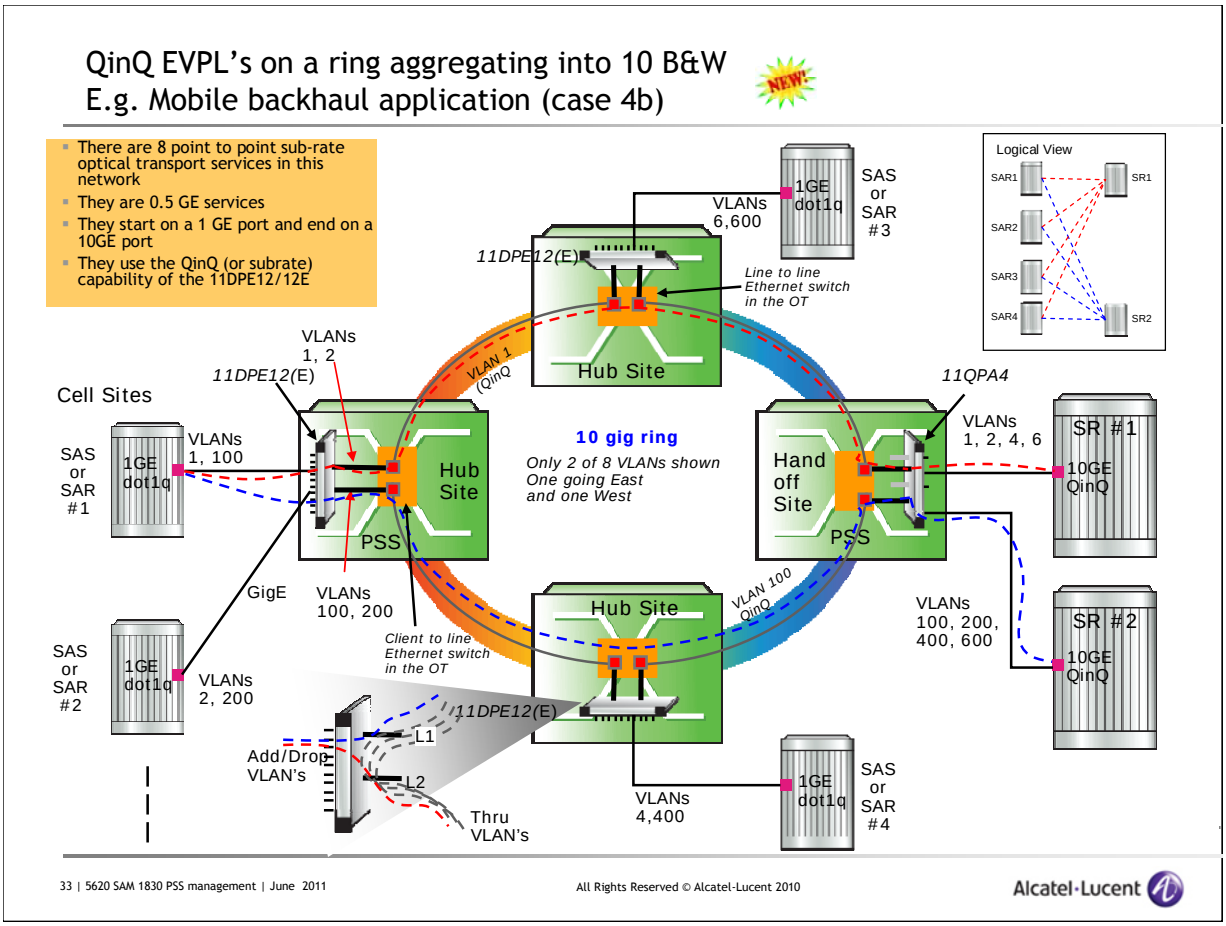
A more complete list of supported configurations is shown below:


Supported optical transport service end points
Endpoints can be on the SR/ESS or PSS
Endpoints can be DWDM tunable or pluggable
Endpoints can be DWDM or B&W
Note: SR/ESS includes 7750, 7450, 7710, NEW! 7705, 7210
SR
PSS
Optical network
PSS
SR
Case 1
ep1
ep2
Client to client on PSS
Case 2
ep1
Filter or WSS
10G and 40G tunable on SR
Filter or WSS
ep2
Tunable WT enabled DWDM OT on SR's
Case 3
ep1
SVAC required for non WT enabled OTs
Only 10G XFP's available today
SVAC required for non WT enabled OTs
ep2
Tunable or pluggable non WT DWDM OT on SR's
NEW!
Case 4
ep1
Symmetric (ep ports same rate) and
Asymmetric service e.g. multiple 1G aggregated to a 10G
ep2
B&W on SR's across DWDM network. Port rate at ep1 ≤ ep2
NEW!
Case 5
ep1
10G tunable on SR
ep2
B&W to Color. Port rates equal
= Service end point
= Transponder
= SVAC
29 | 5620 SAM 1830 PSS management | June 2011
All Rights Reserved © Alcatel-Lucent 2010
Alcatel·Lucent



EVPL Services

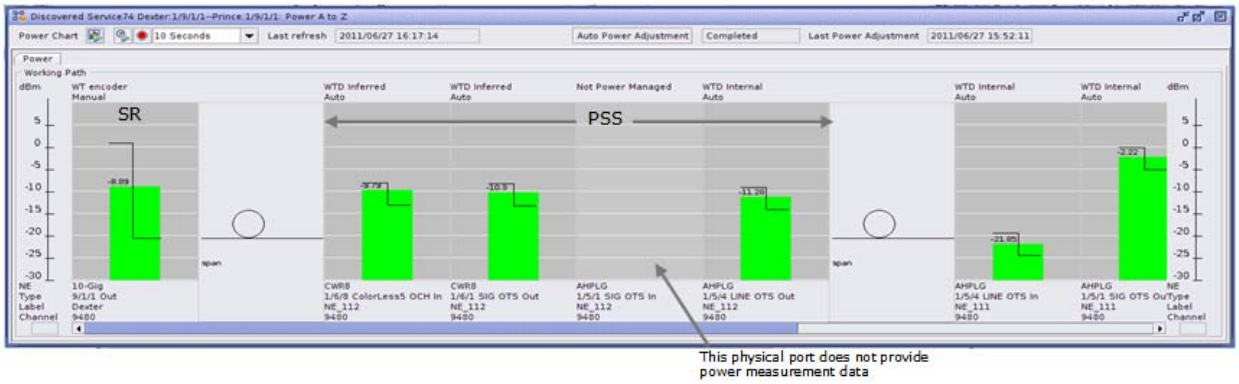
5620 SAM supports the creation of EVPL based optical transport services using the 11DPE12 and 11DPE12E optical transponder.
The figure below shows a typical example of such a service configuration:



Photonic Power Graphing

The 5620 SAM displays power graphs showing optical power levels obtained from the 1830 PSS and 7x50 network elements at every hop on the service including encode points, decode points and non power managed points. The power graphs display the measured power and the target high / low water marks. The latter are displayed as Z bars. Power levels are shown on a per optical transport service basis showing all the measurement points along the path. Multiple graph windows can be opened to show A-Z, Z-A power for working and protection paths. The data on the graph is updated in real time while the graph is displayed (10 second updates)

A different power graph can also display on a single port the power levels of all channels passing through that port.



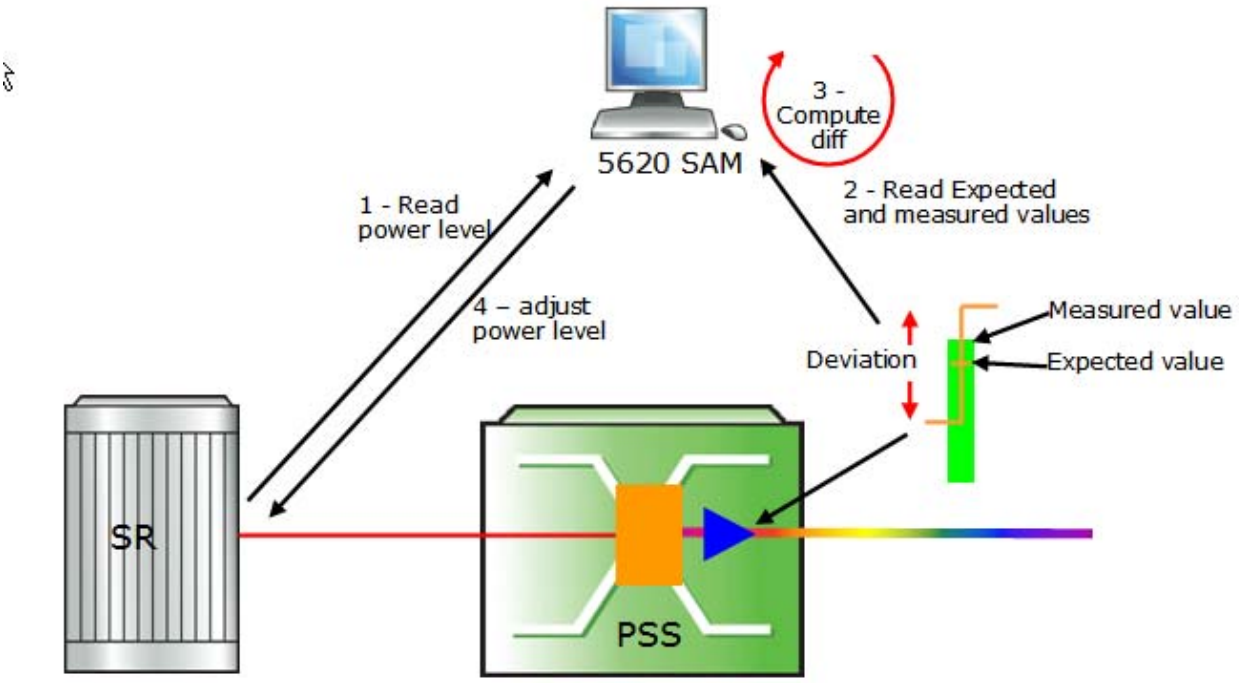
Service Power Launch Management for SR-Based Termination Points

Once commissioned, power levels between 1830 PSS's are maintained by an automatic power level adjustment algorithm running on the nodes based on EPT parameters passed to the nodes during commissioning. When connected to a non 1830 node such as the 7x50, the 1830 does not automatically adjust power on a service launch as there is no in-band communication.

Without 5620 SAM the operator must manually adjust power on the routers until the received powers on the PSS are within spec. With 5620 SAM this power adjustment is done automatically when requested by the operator. An automated algorithm is available in 5620 SAM to ramp up (or down) the SR power level to bring the target power level on the PSS into range.

Once a service is established if a TCA is received that the power has gone out of bounds during operation the operator can trigger a new power adjustment cycle

This feature reduces operator workload and chance of error when creating optical transport services from SR's



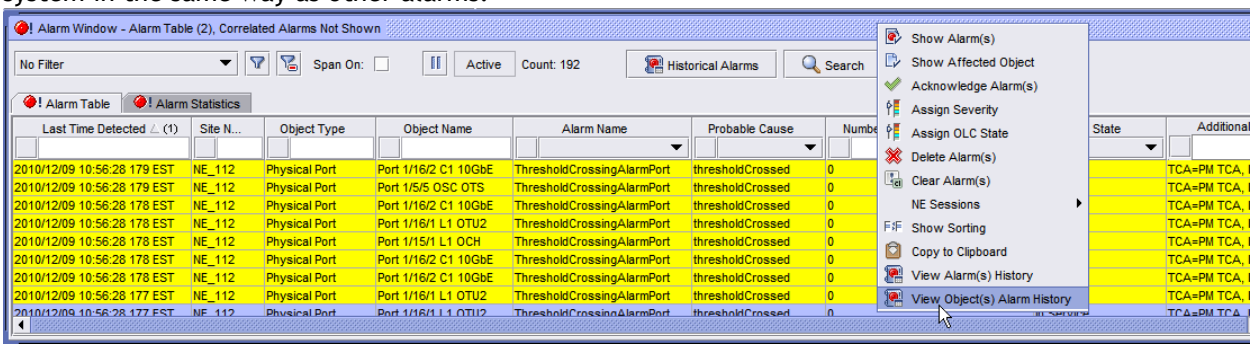
Service Templates

5620 SAM supports the use of service templates to simplify the creation of Optical Transport Services.

Assurance

Alarm Management

Alarms from the PSS family of network elements are managed in the 5620 SAM alarm management system in the same way as other alarms.

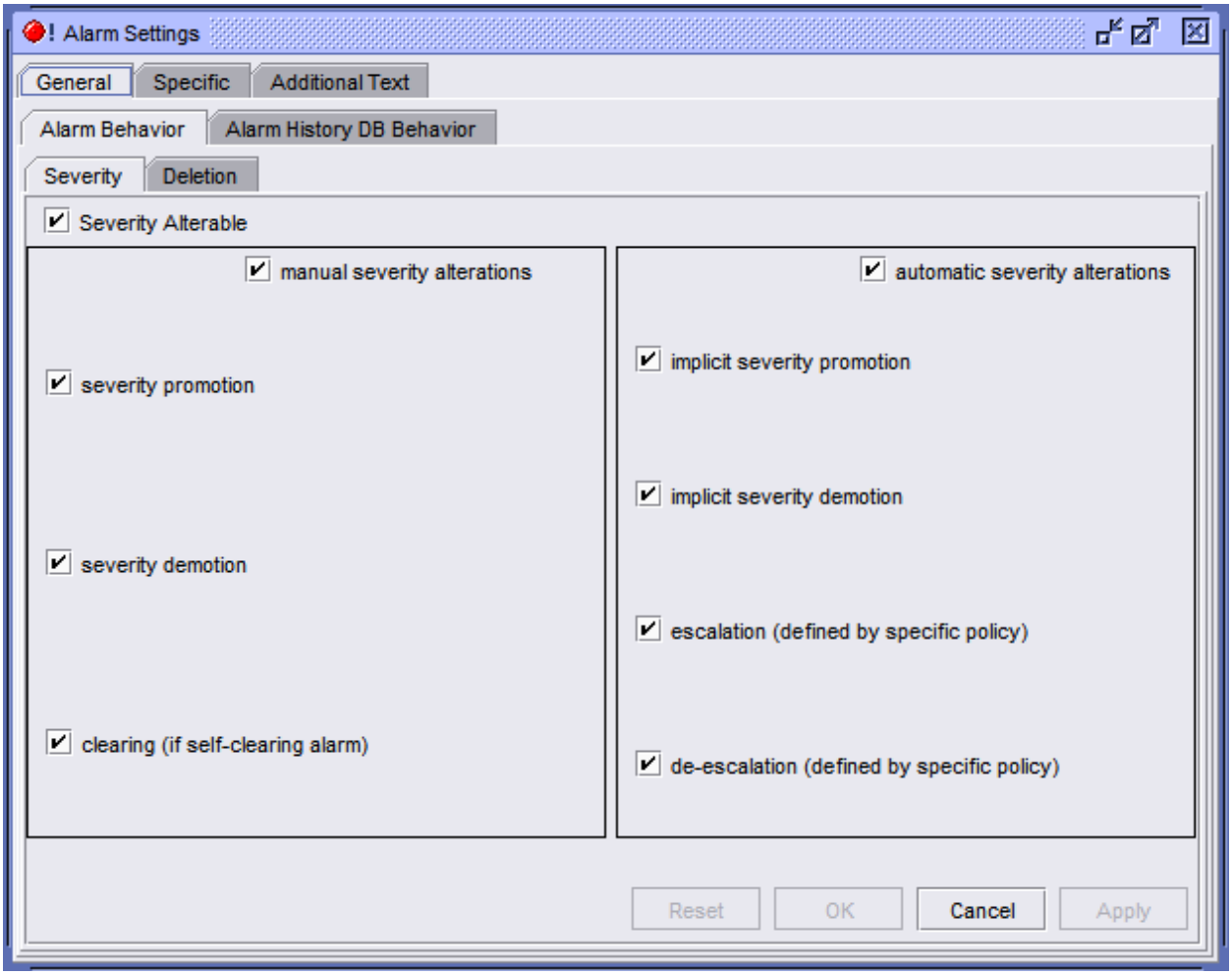


Alarms that are deleted or cleared appear in the alarm history.

The same alarm policies are available.

5620 SAM does not directly read the alarm tables on the network element but responds to changes and creates alarms as required.

All alarms are available through the northbound open interface.



Optical Transport Service Power Troubleshooting

The wave-tracker features supported in 5620 SAM provide a powerful graphical means to clearly see the analog power from end to end on a service. 5620 SAM will graphically display the measured power as well as the expected power at each of the wave tracker measurement points including such points on IPD routers and of course on the PSS network elements.

5620 SAM also displays the measured and target power levels for all channels on a specific WT enabled port. This provides a powerful graphical way to see if there are problems with individual channels or the port as a whole.

5620 SAM Upgrade

5620 SAM Release 9.0 R5 does not support upgrade of 1830 PSS features from earlier versions of 5620 SAM. A user that has 1830 PSS NE's managed in 5620 SAM releases prior to 9.0 R3 (8.0 R7 or 9.0 R1) should un-manage the PSS nodes and Optical transport services and re-discover them.

V. LTE

For more detailed information about 5620 SAM support for LTE, please see the *5620 SAM LTE ePC User Guide*, *5620 SAM LTE RAN User Guide* and *5620 SAM LTE LE4.0 Release Description* document.

The 5620 SAM offers great ease and accuracy in managing the SR family of nodes (including SAR, SAS, and ESS nodes). With Alcatel-Lucent entering the 4G mobility market (through LTE) 5620 SAM supports this new facet of the 7750.

In its new form, the 7750 acts as a SGW or a PGW depending on the application given to the Groups managing the ISMMG Cards that have been inserted. The 5620 SAM will detect the mobility dedicated 7750s and will discover them as being a variant of the 7750 SR (this is based on the SysObjectID that is different on an SR MG node when compared to an SR node).

5620 SAM support includes the introduction for a new type of Service called the Mobile Service on which an operator can run diagnostics using existing 5620 SAM tools, the management of User Bearers and the EPS path discovery and the ability of relate to the underlying connectivity (routed network, physical links, ports) to offer a better view of the managed network and to quickly analyze the impact of certain events in the network (i.e. : port or card down, link broken, routing protocol errors, etc). Lastly, 5620 SAM will also offer the 5620 SAM operator a tool that will allow creation and AGW (SGW and PGW) in 10 mouse clicks; the AGW Creator Facilitator will guide the operators through every step of the way

Key Elements

The following are represented in the 3GPP Architecture example shown below.

SGW: It routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-NodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 (not shown in the illustration above) interface and relaying the traffic between 2G/3G systems and PGW). For idle state UEs, the SGW terminates the DL data path and triggers paging when DL data arrives for the UE. It manages and stores UE contexts, e.g. parameters of the IP bearer service, network internal routing information. It also performs replication of the user traffic in case of lawful interception.

PGW: This gateway provides connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple PDNs. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful Interception and packet screening. Another key role of the PGW is to act as the anchor for mobility between 3GPP and non3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

PCRF: The Policy and Charging Rule Function component enables operators to have rules based, real time dynamic control over bandwidth, charging and usage.

HSS: The Home Subscriber Server is an integrated network for telecommunications carriers that use the IP protocol as its foundation for packetized voice, video and data.

MME: The Mobility Management Entity is the key control node for the LTE access network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved in

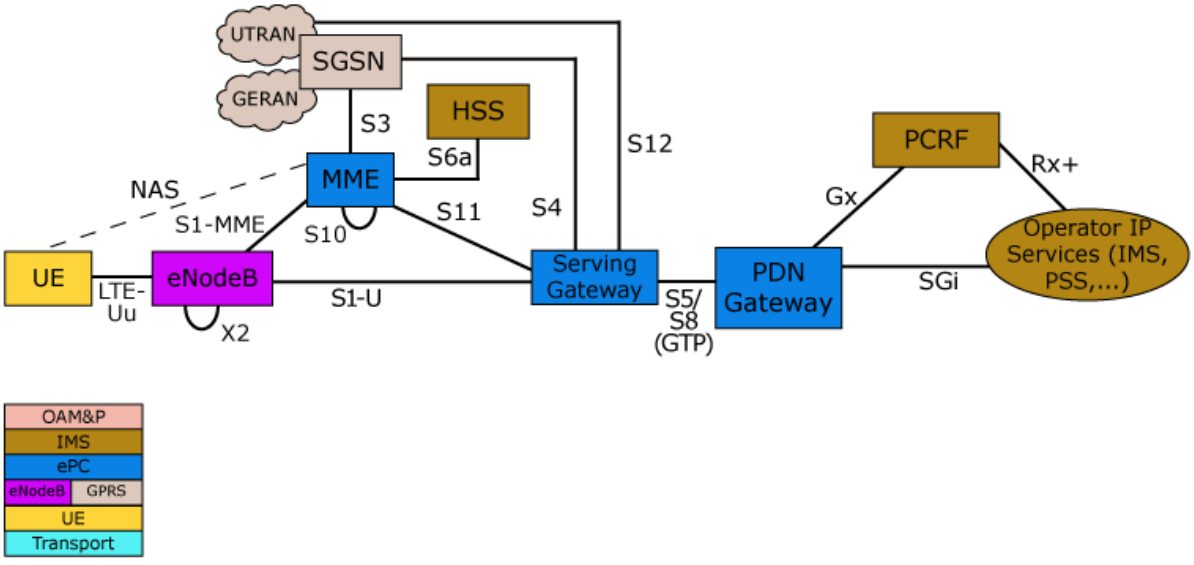
the bearer activation/deactivation process and is also responsible for choosing the SGW for a UE at the initial attach and at time of intraLTE Hand-over involving Core Network node relocation. It is responsible for authenticating the user (by interacting with the HSS).

SGSN: The Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions.

eNB: The "Evolved NodeB (eNodeB)" is new enhanced base stations as per 3GPP standards. This enhanced BTS provides the LTE air interface and performs radio resource management for the evolved access system.

The figure below shows a series of Control (EPS) Bearers that must be present to allow communication between different components of the LTE network.

S1u: Between SGW and eNB (GTP based)
S5: SGW and PGW using GTPC, GTPU, or PMIPv6 (can be referred as S8)
S11: SGW and MME using GTPC
S12: SGW and UTRAN
Gxc: SGW and PCRF
Gx: PGW and PCRF
S2a: PGW



Example of 3GPP Architecture

VI. DEPRECATIONS

Deprecations This Release

Platform Deprecations

5620 SAM Release 9.0 no longer supports Windows on the 5620 SAM server and database.

5620 SAM Release 9.0 no longer supports Sun MicroSystems T-series servers hosting either a 5620 SAM server or database.

Two CPU Core Workstations

As of 5620 SAM Release 9.0, workstations / servers containing two CPU cores or less are not supported. This includes servers such as for example: SPARC v240/v245, Ultra 20 M2, or v440/v445 with only two CPU sockets occupied.

Disk Space

Due to the increased space requirements of Oracle 11, 5620 SAM Database (both distributed and collocated) installations on a single 73GB disk are no longer supported. A minimum of either two 73GB disks or one 146GB disk is required.

Minimum Memory (RAM)

5620 SAM Server, 5620 SAM Database and 5620 SAM Collocated configurations are no longer supported on platforms with 4GB of RAM.

5620 SAM Server and 5620 SAM Collocated configurations are no longer supported on platforms with 8GB of RAM. Support for installations with less than 12GB of RAM is limited to non production environments with some functionality disabled (3GPSS). Installations on workstations with less than 8GB of RAM are blocked.

1830 OSSI model for Service and Equipment

The OSSI model for Services and Equipment from 8.0 R7 is deprecated. Changes in the service and port modeling have taken place since the last release. (These were marked as deprecated in the 8.0 R7 release).

NAT Deprecations

Network Address Translation (NAT) between 5620 SAM main servers, auxiliary servers and databases is deprecated in 5620 SAM Release 9.0 R5 Beta and later. NAT remains supported between:

- main server and single-user client or client delegate server
- main or auxiliary servers and managed network

Deprecations in Future Releases

Dynamic Shelf Drawings

5620 SAM Release 6.x was the first release that implemented static shelf drawings for newly supported NEs. The trend toward static drawings will continue, and in a future release of the 5620 SAM, the Equipment Manager will be removed and all functionality provided by it will be moved to individual equipment properties forms.

SAM-O Deprecations

The following jars are deprecated and will be removed in a future release. Only samOss.jar should be used to connect to the 5620 SAM server:

samOssJBoss.jar
samOssAnyServer.jar

See the SchemaChanges90.html file in the 5620 SAM XML Reference for information about deprecated XML API content.

Service Template Deprecations

5620 SAM Release 10.0 R1 will no longer support the conversion function for templates created in pre-6.0 releases of 5620 SAM.

Platform Deprecations

5620 SAM Release 10.0R1+ will no longer support 5620 SAM GUI client application on Windows 2000 platform.

VII. REFERENCES

The following documents have been referenced:

5620 SAM LTE LE4.0 Release Description, 3HE 06861 AAAA TQZZA
5620 SAM LTE LE3.0 Release Description, 3HE 06687 AAAA TQZZA
5620 SAM Network Element Compatibility Guide, 3HE 06686 AAAA TQZZA