5620 SAM
Services Operations and Provisioning

Student Guide

TOS36042_V3.0-SG Edition 1

Terms of use and legal notices

TERMS OF USE AND LEGAL NOTICE

Alcatel-Lucent provides this training course to you subject to these Terms of Use and Legal Notice. Your use of this training course and/or this site constitutes your acceptance of and agreement to these Terms of Use and Legal Notice. These Terms of Use and Legal Notice, as well as the contents of this training course, may be updated or amended by Alcatel-Lucent from time to time without prior notice to you. Your use of the Alcatel-Lucent training materials after such update or amendment constitutes your acceptance of and agreement to said updated or amended Terms of Use and Legal Notice.

SAFETY WARNING

Alcatel-Lucent training materials can be for products or refer to products that have both lethal and dangerous voltages present. Always observe all safety precautions and do not work on the equipment alone. The user is strongly advised not to wear conductive jewelry while working on the products. Equipment referred to or used during this course may be electrostatic sensitive. Please observe correct anti-static precautions.

PERMISSION TO USE CONTENT

The information, communications, scripts, photos, text, video, graphics, music, sounds, images and other materials provided in this training course (collectively the "Content"), is intended for the lawful use of employees of Alcatel-Lucent and other authorized participants in this Alcatel-Lucent training course. You are hereby granted a non-exclusive, non-transferable permission to access and use the Content solely for your personal training and non-commercial use. This permission may be terminated by Alcatel-Lucent at any time for any reason or no reason, with or without notice. You must immediately cease use of the Content upon such termination.

COPYRIGHTS AND TRADEMARKS

The unauthorized copying, displaying or other use of any Content from this training course is a violation of the law and Alcatel-Lucent's corporate policies. The Content is protected in France, the U.S. and other countries by a variety of laws, including but not limited to, copyright laws and treaty provisions, trademark laws, patent laws and other proprietary rights laws (collectively, "IP Rights"). In addition to Alcatel-Lucent's IP Rights in the Content, in part and in whole, Alcatel-Lucent, and any of the third parties who have licensed and/or contributed to the Content, owns a copyright in the formatting and presentation of the Content.

Alcatel-Lucent does not grant you any permission to use the Content other than the permission expressly stated in these Terms of Use and Legal Notice. All other use of Content from this training course, including, but not limited to, modification, publication, transmission, participation in the transfer or sale of, copying, reproduction, republishing, creation of derivative works from, distribution, performance, display, incorporation into another training course or presentation, or in any other way exploiting any of the Content, in whole or in part, for uses other than those expressly permitted herein is strictly prohibited and shall not be made without Alcatel-Lucent's prior written consent. All characters appearing in this training course are fictitious. Any resemblance to real persons, living or dead, is purely coincidental.

There may be a number of proprietary logos, marks, trademarks, slogans and product designations found in the Content. Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logos are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent does not grant you a license to use any of the foregoing logos, marks, trademarks, slogans and product designations in any fashion. Granting of the right to access and use the Content for training purposes does not confer upon you any license under any of Alcatel-Lucent's or any third party's IP Rights.

DISCLAIMER

ALCATEL-LUCENT DISCLAIMS ALL WARRANTIES REGARDING THE TRAINING COURSES OR THE CONTENT, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE ALCATEL-LUCENT WILL NOT BE RESPONSIBLE OR LIABLE FOR ANY INJURY, LOSS, CLAIM, DAMAGE, OR ANY SPECIAL, EXEMPLARY, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION LOSS PROFITS OR LOSS SAVINGS), WHETHER BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, THAT ARISES OUT OF OR IS IN ANY WAY CONNECTED WITH (A) ANY USE OR MISUSE OF THE CONTENT OR THE TRAINING COURSES BY YOU, OR (B) ANY FAILURE OR DELAY BY ALCATEL-LUCENT, ITS OFFICERS, DIRECTORS, AGENTS OR EMPLOYEES IN CONNECTION WITH THE CONTENT OR THE TRAINING COURSES (INCLUDING, WITHOUT LIMITATION, THE USE OF OR INABILITY TO USE ANY COMPONENT OF THE CONTENT OR TRAINING BY YOU). SOME JURISDICTIONS LIMIT OR PROHIBIT SUCH EXCLUSION OF WARRANTIES OR LIMITATION OF LIABILITIES AND SO THE FOREGOING EXCLUSION OF WARRANTIES OR LIMITATION OF LIABILITY MAY NOT APPLY TO YOU.

GOVERNING LAW

These Terms of Use and Legal Notice are governed by the laws of France. The operation and use of the training course is governed by the laws of the country that governs your employment contract, if applicable. If any provision of these Terms of Use and Legal Notice, or the application thereto to a person or circumstance, is held invalid or unenforceable by law, statute or a court of competent jurisdiction, for any reason, then such provision shall be modified and/or superseded by a provision that reflects the intent of the original provision as closely as possible. All other provisions of these Terms of Use and Legal Notice shall remain in full force and effect. You may not assign these Terms of Use or any permission granted hereunder without Alcatel-Lucent's prior written consent. Nothing herein shall be deemed an employment agreement or an offer of employment or an alteration in any way of a user's terms of employment with or within Alcatel-Lucent.

Course outline

Welcome to 5620 SAM
Services Operations and Provisioning

1. Overview
    1. Service Overview
    2. Network Architecture
    3. 5620 SAM Service Support
2. Service structure
    1. Components
3. Service Types
    1. VPLS
    2. VLL
    3. IES
    4. VPRN
    5. Composite
    6. Mirror
4. OAM diagnostics
    1. OAM Diagnostics
5. Service and Network Tests
    1. Service Test Manager
    2. Service Throughput Tests
    3. RCA Audit
6. Templates
    1. Service and Tunnel Templates
7. Service classification and Forwarding
    1. QoS Policy

Course objectives

5620 SAM
Services Operations and Provisioning

Upon completion of this course, you should be able to:

- Describe the Alcatel-Lucent service concept,
- Identify the roles and corresponding Alcatel-Lucent equipment in an IP/MPLS network,
- Describe the components of a service,
- Create service tunnels and configure service access ports
- Provision IP/MPLS services (VPLS, VLL, IES, and VPRN)
- Provision composite services, service mirrors, and dynamic services
- Perform OAM diagnostic tests
- Configure tests using the Service Test Manager to verify the services's operational state
- Create service throughput tests to verify SLAs
- Perform root cause analysis to identify configuration problems for services and physical links
- Create services using customer-defined templates
- Apply a QoS policy to a service

Your feedback is appreciated!
Please feel free to Email your comments to:

training.feedback@alcatel-lucent.com

Please include the following training reference in your email:
TOS36042_V3.0-SG Edition 1

Thank you!

Section 1
Overview

Module 1
Service Overview

TOS36042_V3.0-SG-English-Ed1 Module 1.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to identify:

- The Alcatel-Lucent service concept

This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 The Alcatel-Lucent service model

1.1 Network Challenges: The Evolution of Transport and Services

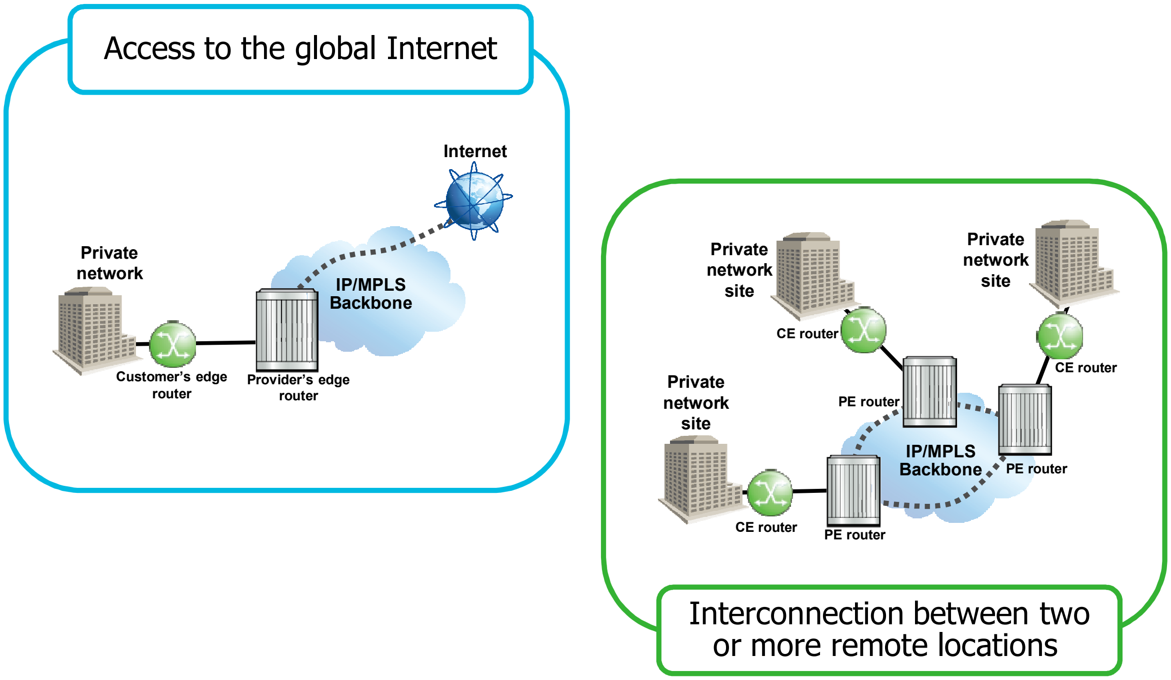
Challenges

- Tremendous pressure to reduce cost base
- Obsolescence and inefficiency in legacy networks
- Need to make strategic investments in a modern infrastructure

Answer

- Support of legacy, ***and*** next generation services, over a converged, IP/MPLS , Ethernet-centric network
- Scalable, resilient, cost-effective, platforms for private line, layer 2 and full IP routed services

1.2 Service definition



Alcatel·Lucent UNIVERSITY

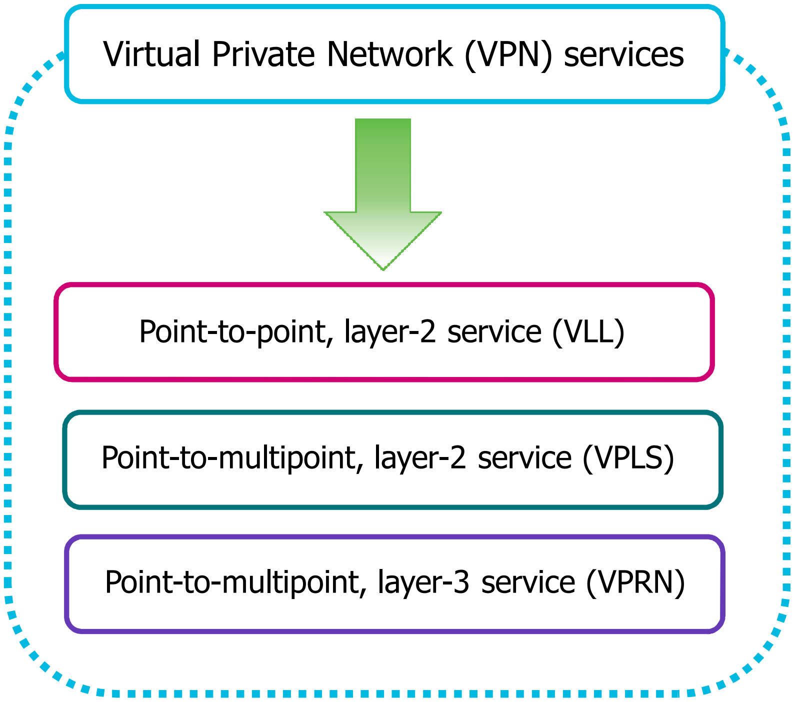
A service in this context consists of extending the connectivity provided by a private network.

Services can be classified into two groups, depending on the type of extended connectivity they provide:

- Access to the global Internet
- Interconnection between two or more remote locations as if they were co-located

The second service group is known as a **Virtual Private Network (VPN)**. Its name comes from the fact that two or more separate islands of a private network have the service provider in the middle, but they still get the impression that the whole network is private. This is to some extent true because full privacy is maintained from end to end by keeping logically separated flows of data at all times.

1.2 Service definition [cont.]



Alcatel·Lucent UNIVERSITY

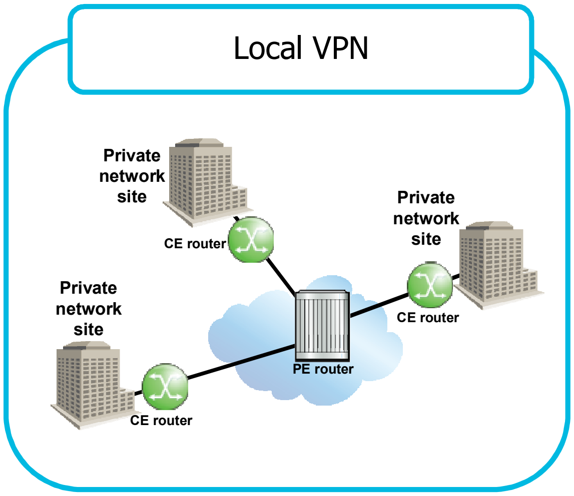
VLL, VPLS and VPRN are all examples of VPN. IES is the way access to the Internet can be provided with all the benefits introduced by the service concept, as explained later.

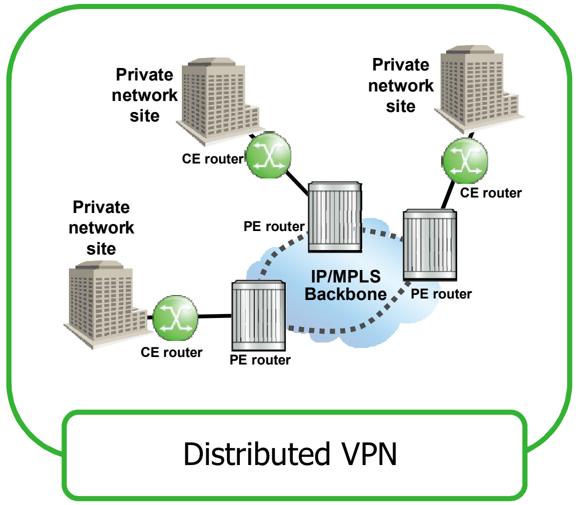
Point-to-point, layer-2 service (VLL): there is a pipe interconnecting two remote locations, frames enter one end and are delivered at the remote end

Point-to-multipoint, layer-2 service (VPLS): several locations may be interconnected, forwarding decisions are based on the frame’s destination MAC address

Point-to-multipoint, layer-3 service (VPRN): several locations may be interconnected, forwarding decisions are based on the packet’s destination IP address

1.2 Service definition [cont.]



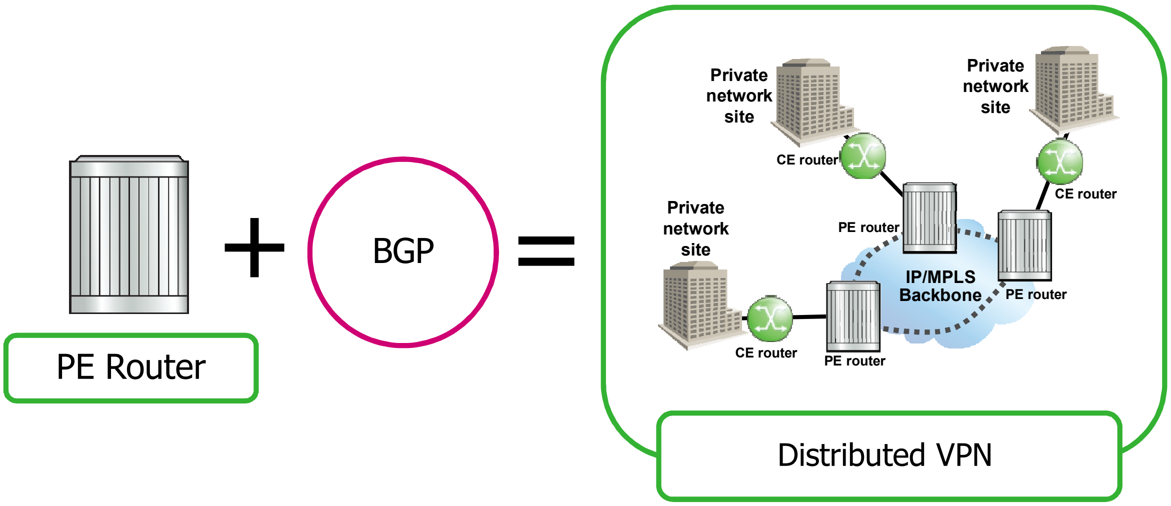


Alcatel·Lucent UNIVERSITY

Lastly, Virtual Private Network (VPN) services can also be classified as:

- **Local VPN**: there is only one service provider's node involved in providing the service
- **Distributed VPN**: there is two or more service provider's nodes involved in providing the service

1.3 Requirements for service provisioning

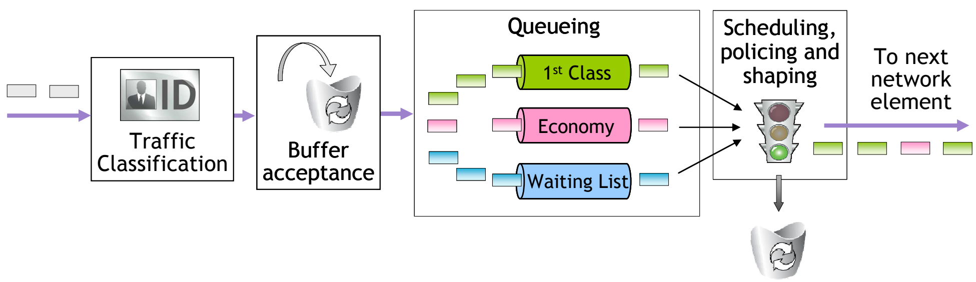


For a PE router to be able to provide a distributed layer-3 VPN (VPRN), it needs additionally to run the **BGP** routing protocol. More specifically, Multi-Protocol BGP (**MP-BGP**) is needed to exchange customer routing information with the other PEs involved in providing the same service.

1.3 Requirements for service provisioning [cont.]

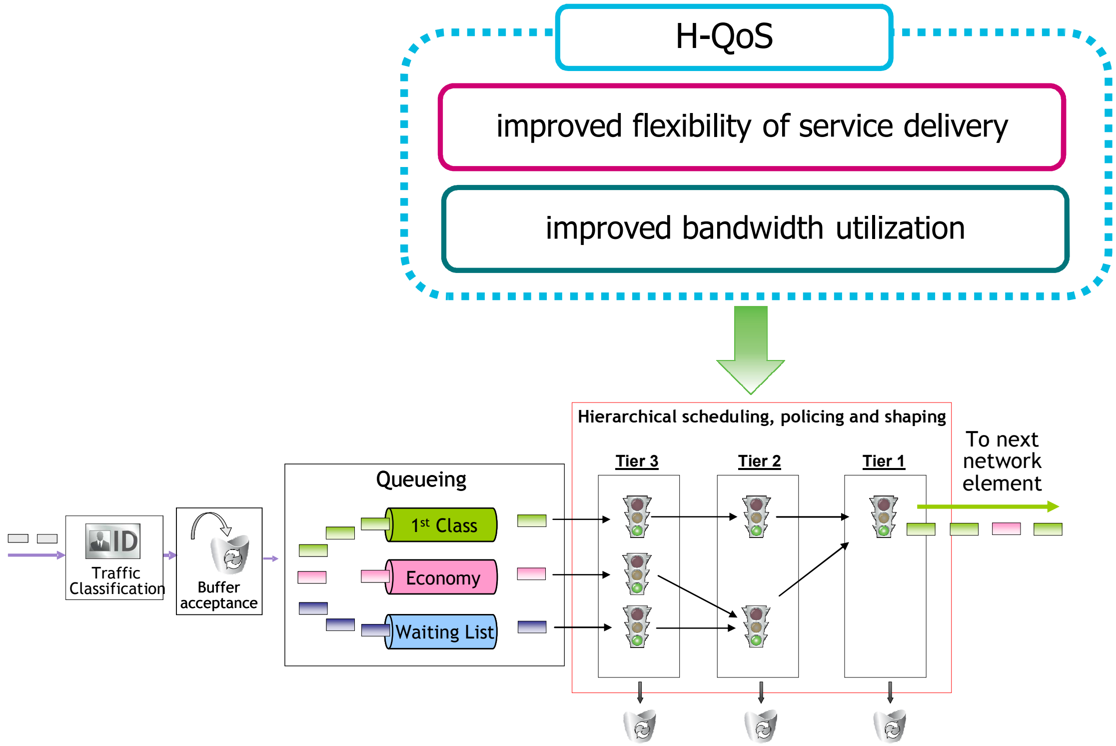
QoS Techniques

- Traffic classification
- Separate queuing for each traffic class
- Differentiated scheduling/forwarding for each traffic class



When the traffic being carried by a service needs time-constrained delivery (e.g. VoIP), Quality of Service (**QoS**) techniques are required.

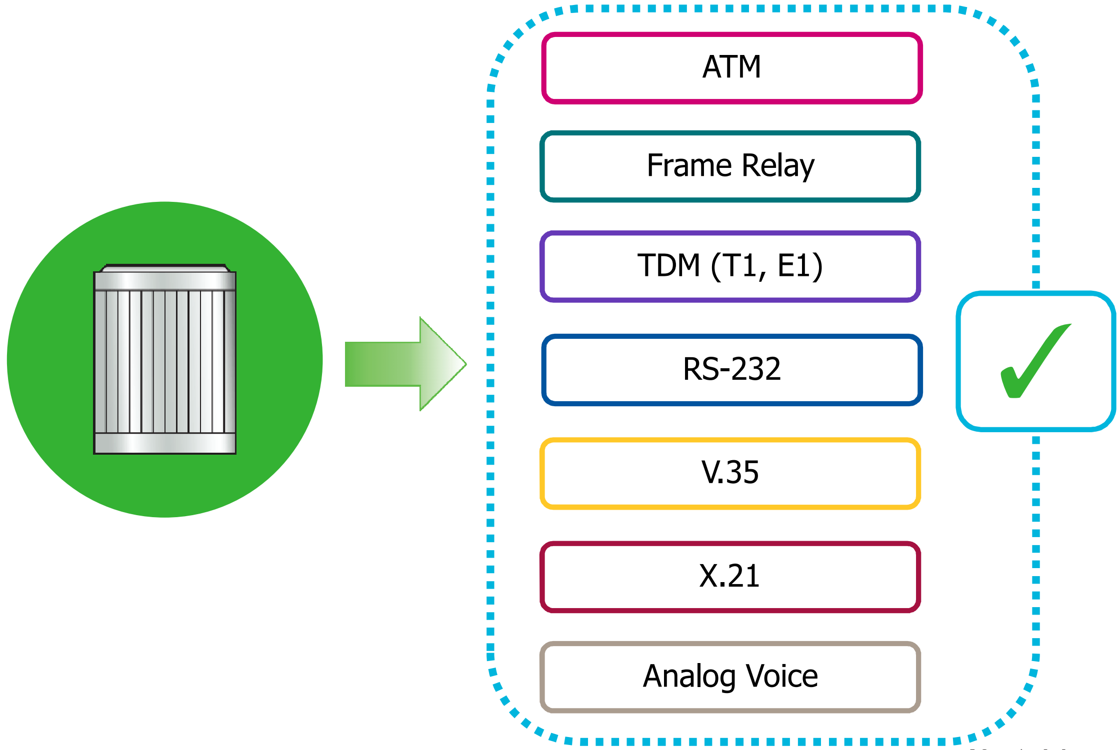
1.3 Requirements for service provisioning [cont.]



Alcatel·Lucent UNIVERSITY

Scheduling/forwarding policies can be arranged in a **hierarchical** structure to improve flexibility and utilization (H-QoS)

1.3 Requirements for service provisioning [cont.]



When a customer is running a **legacy network**, the service provider's node needs to be able to have interfaces compatible with such legacy technologies; for example: ATM, Frame Relay, TDM (T1, E1), RS-232, V.35, X.21, and analog voice.

Knowledge Verification – Remote Interconnection

Which one of the following services is not an interconnection between two or more remote locations ?

a. VLL
b. IES
c. VPRN
d. VPLS

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

This page is left blank intentionally

End of module
Service Overview

Section 1
Overview

Module 2
Network Architecture

TOS36042_V3.0-SG-English-Ed1 Module 1.2 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to identify:

- Different roles in a typical service provider network
- The Alcatel-Lucent IP/MPLS portfolio
- Role of each type of equipment in the network

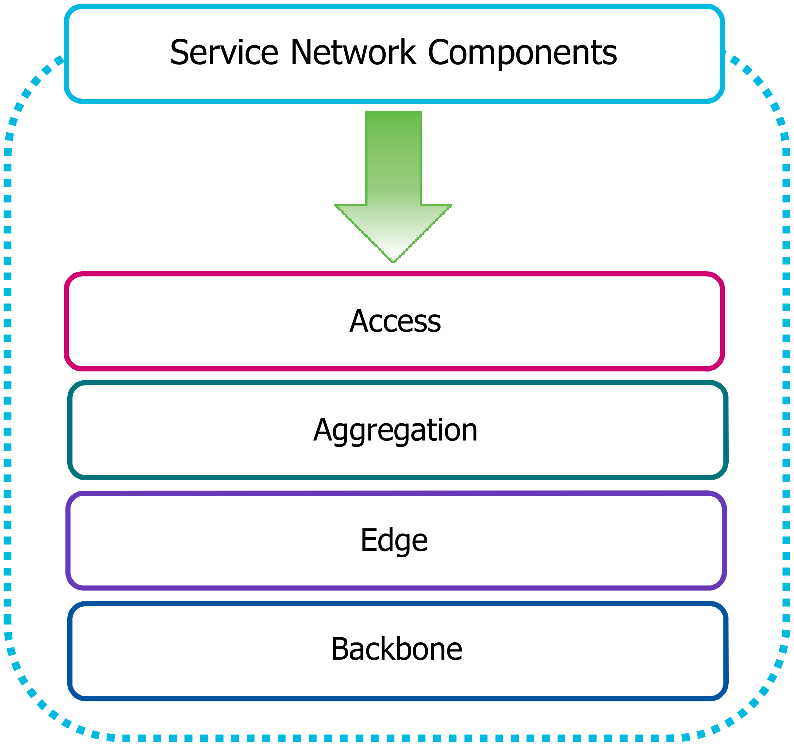
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Network Architecture

1.1 Typical service provider network architecture

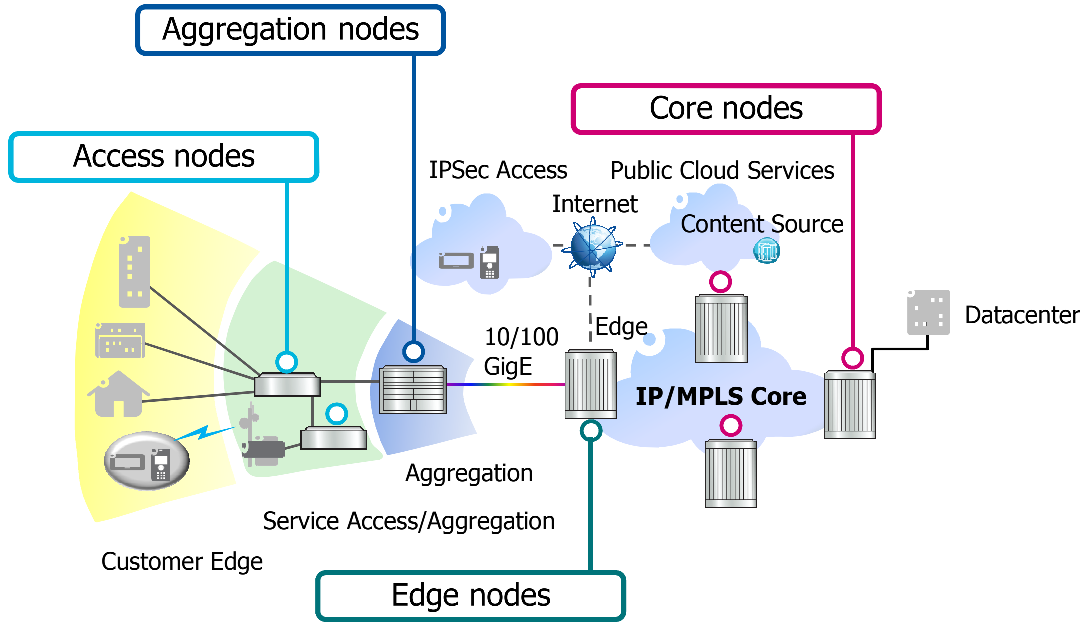


Alcatel·Lucent UNIVERSITY

There are four main components in a network created to provide services:

- **Access:** Includes devices directly connected to the customer equipment that generates/receives the traffic carried by the service provider on behalf of the customer
- **Aggregation:** Includes devices that receive traffic from different access nodes or directly from customers and aggregates the traffic into a smaller number of streams
- **Edge:** Includes feature-rich devices that receive traffic either directly from customers, or from access or aggregation nodes, and provide a variety of services to the end customers
- **Backbone:** Part of the network in charge of receiving traffic at a certain location and carrying it at high speed to remote locations

1.1 Typical service provider network architecture [cont.]



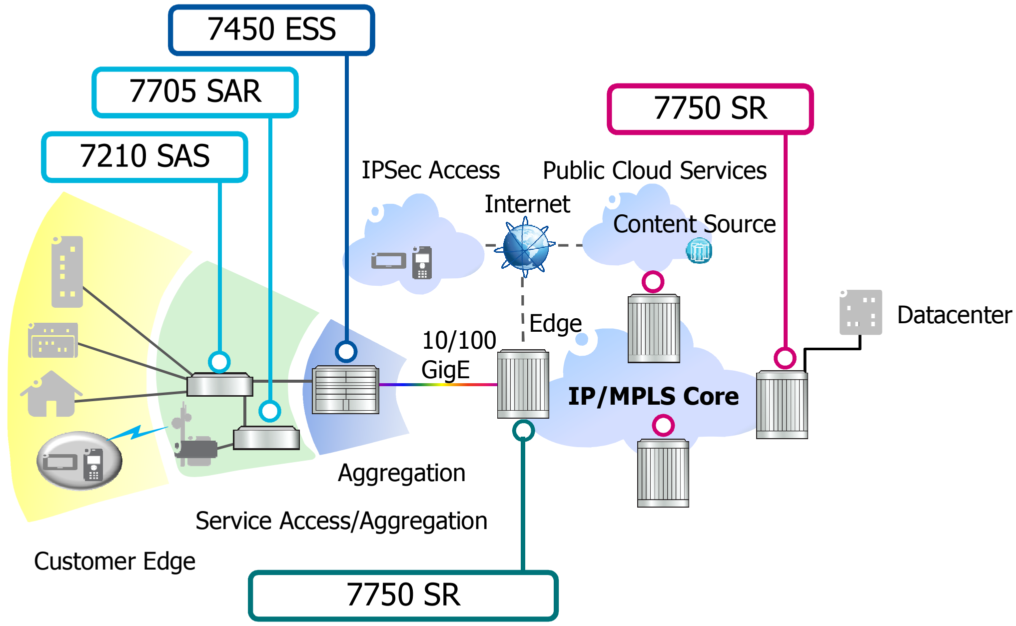
Access nodes, in general, do not need very high capacity or very high processing power since they will be dealing with a reduced number of traffic streams, and therefore a reduced number of configured services (as compared to nodes at the network's edge). What they do need, however, is to be compatible with whatever technology the customer has implemented.

Aggregation nodes are added to improve scalability at the edge and the core of the network by forwarding a reduced number of traffic streams. Because of their function, having to deal with a relatively large number of traffic streams, they need in general to have higher capacity and higher processing power than access nodes.

Edge nodes are responsible for providing to the customer the rich set of services offered by Alcatel-Lucent, including (as described earlier) layer-2 and layer-3, as well as IES and VPN types of services, with QoS guarantees as required, and to remote locations (distributed), if required. Access and aggregation nodes can be thought of as a way of extending the reach of the benefits offered by edge routers to customers that do not have a direct access to them. That is the reason why edge nodes must be feature-rich. Additionally, edge routers must also have a very high capacity and processing power since they will likely have to deal with a large number of configured services; another reason is that they are usually part of, or interact directly, with nodes in the core of the service provider network.

Finally, **core nodes** need to be very high-capacity, high-speed devices since they are the ones carrying traffic from one location to one or more remote sites. They need to be able to carry, inside pre-configured tunnels, large amounts of traffic corresponding to many different traffic streams, they need to implement proactive resiliency techniques to quickly recover from failures, and do so while honoring Service Level Agreements (SLAs) by implementing QoS techniques.

1.2 Service Router and Ethernet Service Switch Product Portfolio



7210 Service Access Switch
A Carrier Ethernet device that can also be deployed as a cost-effective CE aggregation device.

7705 Service Aggregation Router
A router that provides IP/MPLS and PW capabilities in an aggregation platform.

7450 Ethernet Service Switch
An Ethernet switch that enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/MPLS networks.

7750 Service Router
A high-capacity router that provides scalable, high-speed private data services with SLAs. It is typically deployed in a core network

Technical Reference
See TER36060 Service Routing Fundamentals or TER36068 IP Hardware Overview for more information on Alcatel-Lucent IP routing hardware.

Knowledge Verification – 7750 SR definition

The 7750 SR provides the following network functionality.

a. A Carrier Ethernet device that can also be deployed as a cost-effective CE aggregation device.
b. A high-capacity router that provides scalable, high-speed private data services with SLAs. It is typically deployed in a core network.
c. A router that provides IP/MPLS and PW capabilities in an aggregation platform.
d. An Ethernet switch that enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/MPLS networks.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

End of module
Network Architecture

Alcatel·Lucent
UNIVERSITY

Section 1
Overview

Module 3
5620 SAM Service Support

TOS36042_V3.0-SG-English-Ed1 Module 1.3 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to describe:

- Explain the features and benefits of the 5620 SAM service model

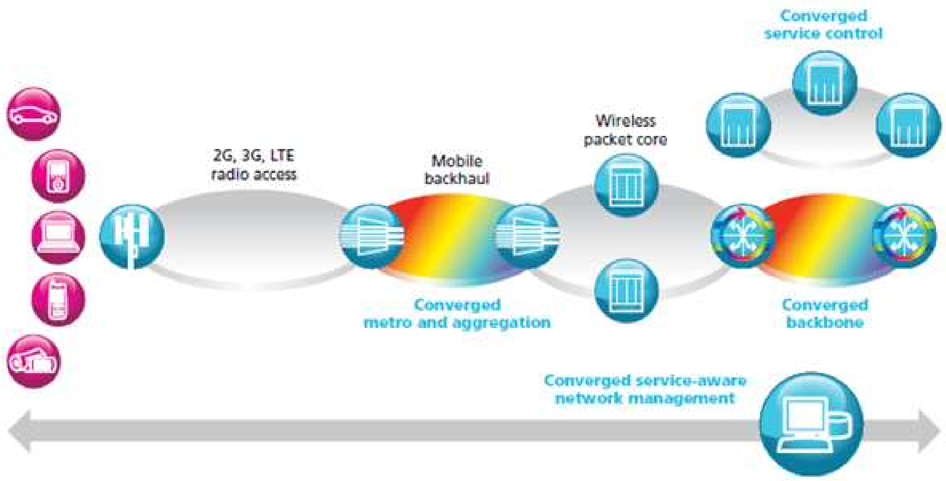
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 5620 SAM service support

1.1 5620 SAM service-aware management

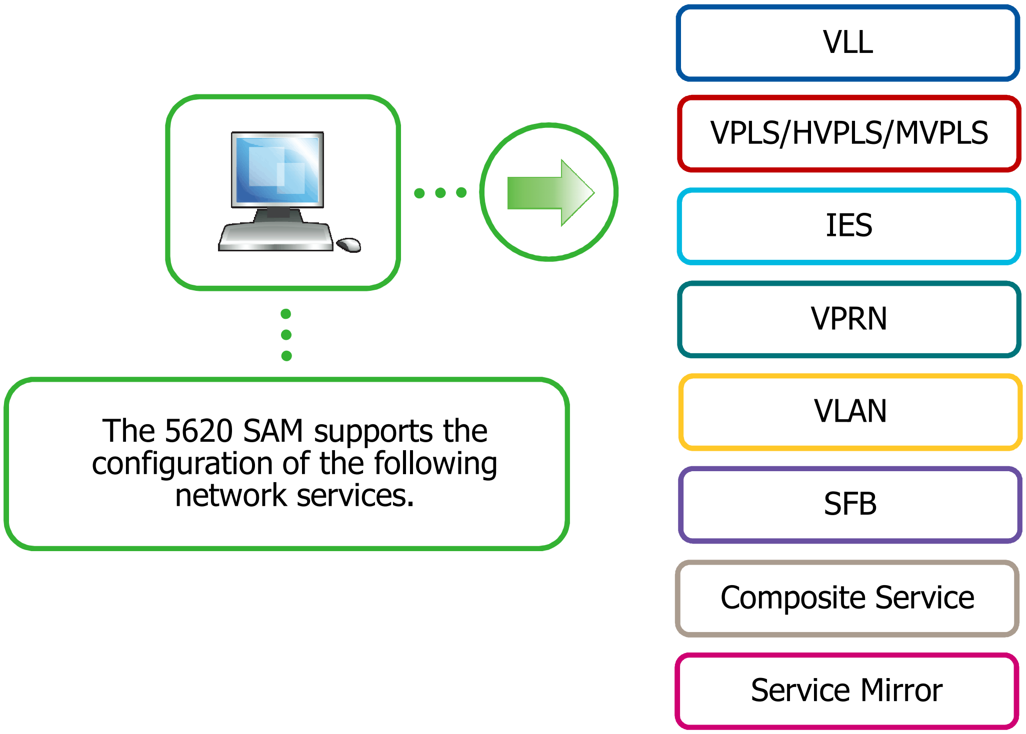


The Alcatel-Lucent 5620 Service Aware Manager (SAM) enables end-to-end network and service management across all domains of the converged, all-IP network. This product helps service providers quickly maximize operational efficiencies through fast provisioning and troubleshooting, proactive assurance and flexibility that eases integration into the network.

The 5620 SAM provides mobile service providers to perform the following functions with their network:

- Implement an end-to-end management for both data and control plane, including RAN, backhaul and packet core
- Correlate faults, pinpointing whether the problem resides in the IP or optical layer and its root cause. This simplifies troubleshooting, and isolates impairments before services are impacted.
- Provision the network with fast and easy configuration and multi-vendor scripting workflows that reduce risk of error and speed network deployment time.
- Proactively prevent service degradation through end-to-end power control, monitoring, tracing and fault localization for individual wavelength channels (enabled by Alcatel-Lucent Wavelength Tracker technology).
- Accelerate setup for integrated IP/optical performance and SLA monitoring with service-aware diagnostics that validate end-to-end data services and IP/optical paths.

1.2 5620 SAM-supported service types



A 5620 SAM operator can create, configure and delete services on sites and routers that are within their span of control. The 5620 SAM supports the following service types:

- Virtual Leased Line, a type of VPN where IP traffic is transported in a point-to-point manner.
- Virtual Private LAN service, a type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. The services may be from different locations, but in a VPLS, they appear to be on the same LAN. When implemented with Layer 2 interfaces, this service is called VPLS. When implemented with Layer 3 interfaces, this service is called an IP-VPN. The 5620 SAM also manages hierarchical and management VPLS types.
- Internet Enhance Service, a routed connectivity service in which a host communicates with an IP router interface to send and receive Internet traffic.
- Virtual Private Routed Network, a network exhibiting at least some of the characteristics of a private network, even though it uses the resources of a public switched network.
- Virtual LAN, a logical grouping of two or more NEs, which are not necessarily on the same physical network segment, but which share the same IP network number.
- Shortest path bridging (SPB), a service that enables multipath routing during network configuration. SPB services are created in conjunction with Backbone VLANs. One Backbone VLAN is designated as the control BVLAN during SPB control instance configuration.
- Composite Service, a set of linked services.
- Service Mirror, where packets from one or more sources are forwarded to their normal destinations and a copy of the entire packet, or a specified portion of the packet, is sent to the mirror destination. The mirrored packet can be viewed using a packet-decoding device, typically called a sniffer.

1.3 Benefits of the 5620 SAM service provisioning model

5620 SAM service provisioning model

- rapid service deployment and reduced configuration complexity
- an end-to-end view of the overall service
- template-based creation of services for rapid and efficient deployment
- template-based creation of policies that specify the classification, policing, shaping, and marking of traffic handled by the managed devices
- significantly lower required training level, risk of user errors, and effort and time for deploying services
- multiple concurrent editing of sites; for example, changing the MTU size on all spokes of a VPLS
- tunnel configuration and transport that are independent of the services
- smooth integration with service management and OSS partnerships
- root cause analysis of an operationally down service
- increased end-customer satisfaction by empowering the network operator to rapidly associate customers with services in response to customer care inquiries

Alcatel·Lucent UNIVERSITY

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to view customers, sites, SAPs, SDPs, and services.

The GUI demonstration includes the displays available through the navigation tree, topology map, and tabbed forms.

Lab Exercises
Common Service Management Actions

Time allowed: 10 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

End of module
5620 SAM Service Support

Alcatel·Lucent
UNIVERSITY

Section 2
Service structure

Module 1
Components

TOS36042_V3.0-SG-English-Ed1 Module 2.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to describe:

- Service components
  - Service Access Points (SAP)
  - Service Distribution Paths (SDP)
  - Service tunnels and labels
- MTU considerations

This page is left blank intentionally

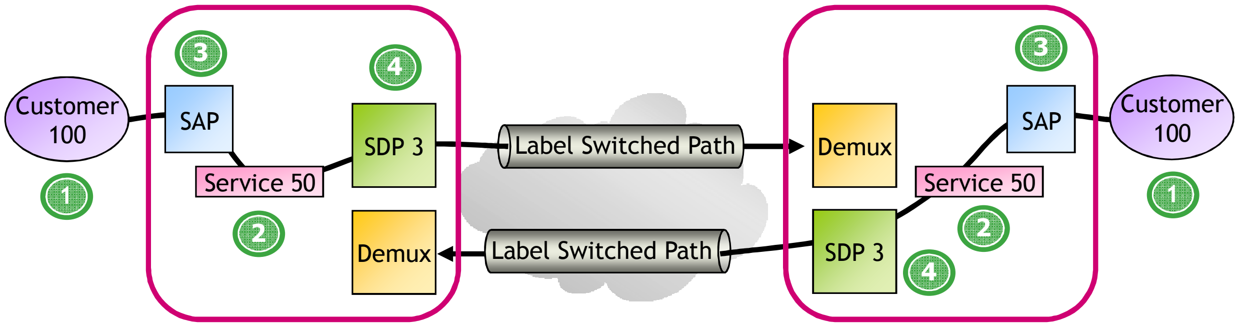
Table of Contents

This page is left blank intentionally

1 Service Model

1.1 Service Configuration Requirements

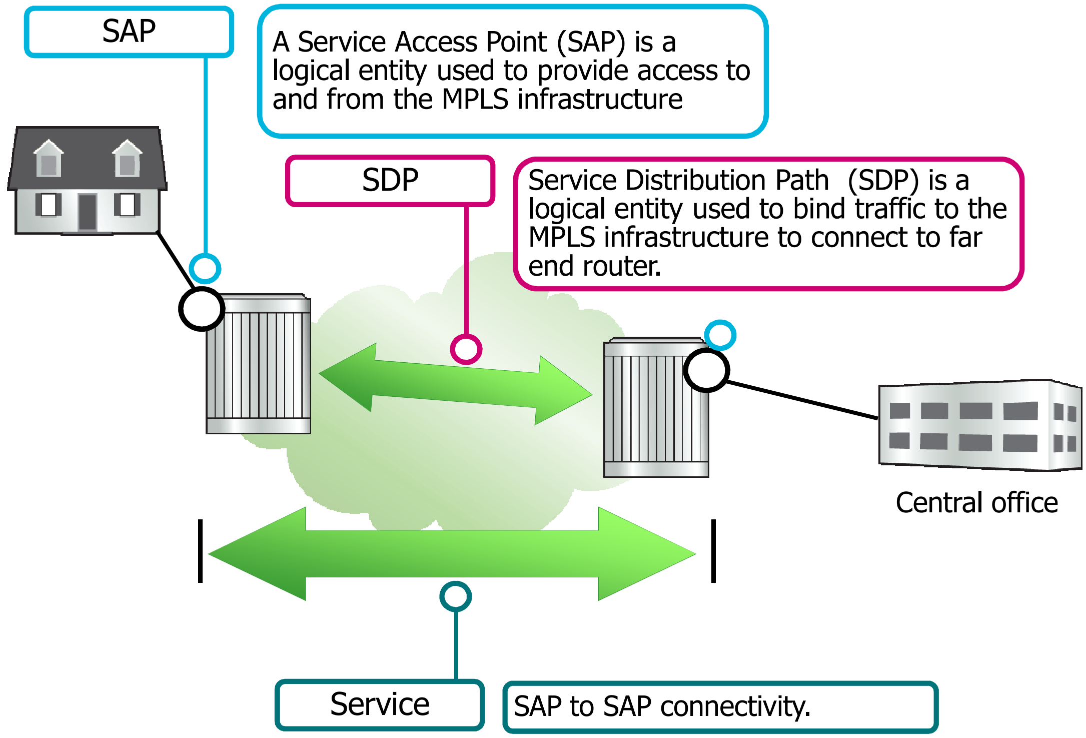
Configure the following components to provision a service



You must define the following components o provision a service:

- Customer
- Service Type
- Service Access Point (SAP)
- Service Distribution Point (SDP)

1.2 Service Terminology

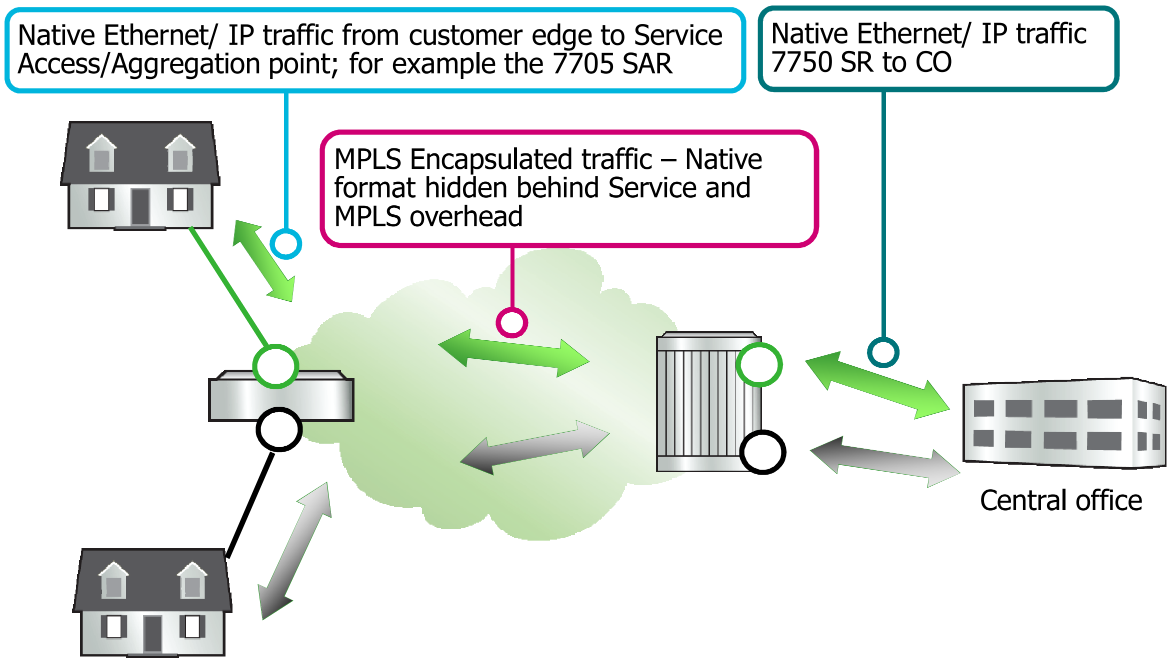


Within the Alcatel-Lucent Service architecture, the point at which traffic will be taken into, or passed out of, the MPLS infratsructure is referred to as the Service Access Point or SAP. This is a logical contruct and will be discussed in more detail later in this module.

To move traffic between access nodes, as illustrated above, a Service Distribution Path (SDP) is required. This a logical construct that is used to bind subscriber data to the MPLS infrastructure and will be discussed in more detail later in this module.

The SAP-to-SAP connectivity forms the Service for which its individual components create the Service Topology. The requirement to deal with service characteristics to support various service topologies requires different service types.

1.3 Data within the Network - Overview



Customer data changes formats as it flows through the network from source to destination. In an LTE MBH network, data between the residence and the 7750 is in the *native* IP format; 1500 byte user data payload and the Data Link Control Layer overhead that can be either 14- , 18- or 22- bytes depending whether VLAN-tagging is configured or not. This wil be discussed in more detail later in this module.

Once the cross connection has been made into the EATN, the customer IP packet is *hidden* behind the MPLS infrastructure overhead. Within this portion of the network, the nodes will deal only with the MPLS overhead therefore, the customer's IP packet is effectively *transparent*.

At the central office (CO), the MPLS overhead is removed from the packet and the customer IP packet, originating at the eNodeB, is passed to the MSC in its *native* IP format; 1500 byte user data payload and the Data Link Control Layer overhead that can be either 14- , 18- or 22- bytes depending whether VLAN-tagging is configured or not.

In defining tasks and/ or functions within a networking environment, the concepts of customer and provider equipment and responsibiliies define which group or organization the various components belong. From a service perspective:

Customer – is that portion in the end-to-end service topology where the subscriber data is in its *native* IP format. In the illustration above, the Customer Edge would be from the 7705 SAR interface out to the subscribers mobile phone and between the 7750 SR in the MSN and the MSC.

Provider – is that portion of the network where the subscriber data is adapted to the MPLS infrastructure; effectively, the EATN. Within the EATN, the 7705 SAR and 7750 SR would be considered the Provider Edge devices.

1.4 Service Components

Service Type and ID

- defines characteristics of how customer data will be treated within the network
- L2 and L3 services, including: VLL & VPLS (L2 VPN) and VPRN & IES (L3)
- requires ID unique to node (best practice = unique in network)
- “owned” by one customer only

Customer and ID

- logical entity used as service “owner”
- requires unique ID (best practice = unique ID through network)
- can “own” more than one service

Service Sites

- Provider Edge devices
- usually more than one for each service (distributed service)

In the SR-OS context, services define the characteristics by which customer data will be provided access to appropriate resources over the IP/MPLS infrastructure. Regardless of the specifics of the various service types, all services have the following components:

1. **All services must be configured within a Service Type and have a unique ID.**
   - The service type defines the characteristics of how customer data will be treated within the network. Services are classified as Layer 2 VPN Services or Layer 3 Services.
   - Layer 2 VPN services include: Virtual Leased Line, point-to-point *pipe* services; and Virtual Private LAN Service, a multipoint service within a common broadcast domain.
   - Layer 3 services include: Virtual Private Routed Network, a multipoint service that provides routed VPNs over a common infrastructure; and an Internet Enhanced Service which provides access to the Internal Routing Protocol route tables to pass traffic through the network.
2. **All services must belong to Customer and that customer must have a unique ID.**
   - A customer is a logical entity that serves as a service „owner“. Each customer must have a unique ID to the node upon which it is configured. Each service may belong to one customer only. However, a customer may own more than one service. For consistency‘s sake, and to avoid future complications, it is recommended that service providers ensure that customer ID remains unique within the network and across nodes invloved in supporting the individual service.
3. **Services will exist within a Service Site.**
   - Service sites are the Provider Edge routers or the PE-CE interface (customer-facing). In CLI, this would be the device upon which the service is being configured.
   - Services sites are a 5620 SAM construct.

1.4 Service Components [cont.]

SAP and ID

- sometimes referred to as "sub-interface"
- logical construct used to bring customer data into/out of MPLS network
- supported on physical Ethernet port, POS channel, TDM channel, LAG
- set for "Access" mode
- Encapsulation type and unique ID
- ID = VLAN tag
- minimum two (2) required per service

SDP and ID

- network facing logical construct
- supported on physical Ethernet port, POS channel, TDM channel, LAG
  - set for "Network" mode
- unique ID relative to ingress PE device
- bound to a Label Switch Path (LSP) creating Service Tunnel
  - Service Tunnel - moves traffic between PE devices over MPLS network

2 · 1 · 12
Service structure · Components
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

4. **All services must have a Service Access Point (SAP) for each customer interface.**
   - A SAP is a logical construct that is used to interface with the customer. It consists of:
     - a physical ethernet port, Packet over SONET channel, TDM Channel or Link Aggregate Group (LAG) set for *Access* mode;
     - port encapsulation type and a unique VLAN ID. The encapsulation type defines th extent to which cutsomer data will be examined for VLAN information; will all traffic be treated as one or more streams? This commonly refers to VLAN tags; microstreamd of data within any physical port.

5. **Where a service supports a SAP on two or more nodes, a Service Distribution Path must be used to move traffic to the egress PE.**
   - An SDP is a logical construct that is used to move customer traffic into the IP/MPLS infrastructure on its way to the egress PE. It consists of:
     - a physical ethernet port, Packet over SONET channel, TDM Channel or Link Aggregate Group (LAG) set for *Network* mode;
     - is significant only to the ingress PE and must be unique to that node;
     - is bound to a Label Swicth Path (LSP) which, in turn, creates a Service Tunnel. A Service Tunnel is the actual mechanism through which customer traffic is transferred to the egress PE.

Knowledge Verification – SDP

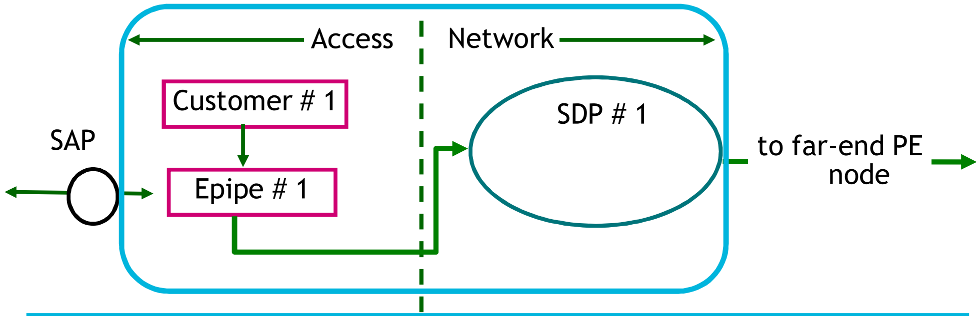
What is the definition of a Service Distribution Point (SDP)?

a. Logical entity used to provide access to and from the MPLS infrastructure.
b. Logical entity used to bind traffic to the MPLS infrastructure to connect to far end router.
c. SAP to SAP connectivity.
d. logical entity used as service “owner”.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.5 Logical View – Ingress PE



PE node has two (2) roles:
- Access – interface to customer data (PE- CE interface)
- Network – adapt customer data to IP/MPLS network infrastructure

Service type (Epipe) with unique ID tied to a customer
- default customer = ID # 1

Associate SAP for customer data interface

Bind data to SDP which is associated to LSP terminating at far-end PE
- known as *SDP Binding*

The diagram above illustrates the block level association of each of the components for a service within the ingress PE.

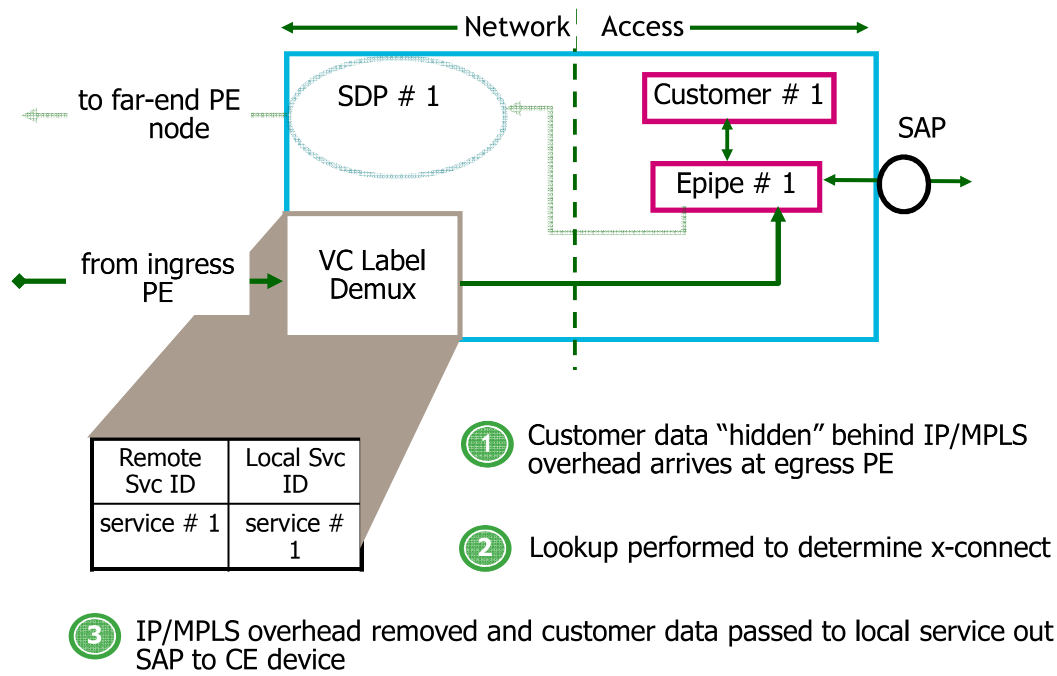
Effectively, the ingress PE node has two (2) functions:

1. Access - support the PE - CE interface; and
2. Network - support the interface for passing customer traffic into the IP/MPLS infrastructure.

The basic components of a service are illustrated, as follows:

- **Customer and ID** = customer # 1
- **Service Type and ID** = epipe service # 1
- **Service site** = ingress PE node
- **Service Access Point** = port-id: encapsulation ID (VLAN ID). An example would be sap 1/1/1:0. The *0* indicates null encapsulation where all data is treated as a single stream. Where a VLAN tag is expected, the SAP ID would replace *null* with the VLAN ID (i.e. sap 1/1/1:250 would be the ID for VLAN 250 on port 1/1/1).
- **Service Distribution Path** = SDP # 1. The SDP configuration would include the association to the appropriate LSP which would be identified by its name. (i.e. lsp to egress PE)

1.6 Logical View – Egress PE



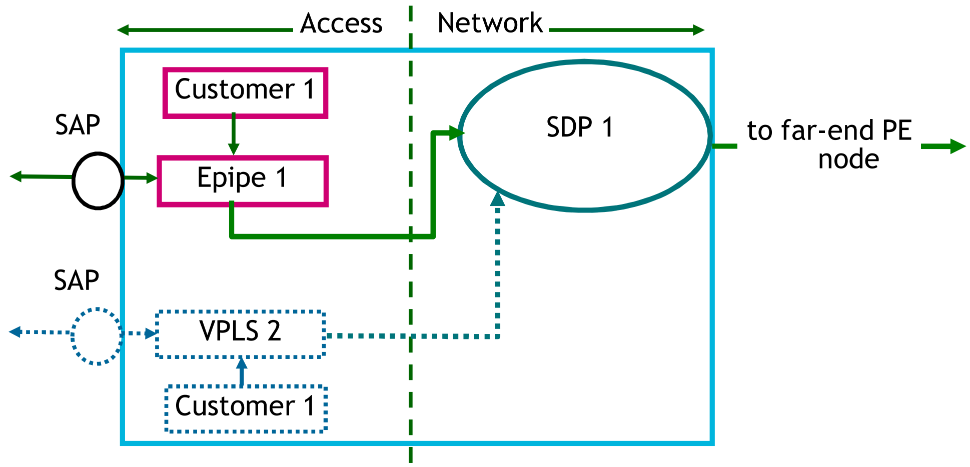
Alcatel·Lucent UNIVERSITY

To be able to remove customer traffic from within the IP/MPLS and send it along to the CE device connected to the egress PE:

1. The packet arrives, along the service tunnel from the ingress PE. The MPLS label is removed after which the system passes the packet to the VC Label Demux;
2. The VC Label Demux performs a cross connect lookup to determine to which of the local serivces it is connected. In the illustration above, the lookup table indicates that service #1 from the ingress PE is cross connected to service #1 on the local router;
3. The VC Label information is removed from the incoming packet, the remainder of which is passed to local service #1;
4. Local service #1 is *owned* by customer #1 and is connected to a Service Access Point (SAP). Data from the originating host is passed along to the destination host. Communication between them is successfully established.

Through the course of creating the service, ensuring bi-directional connectivity will require that an SDP be created and the service bound in the same manner discussed on the previous page.

1.7 Multiple Services in Same SDP



Service providers will often find that multiple services will span the same ingress and egress PE nodes. Requiring that each serivce be associated to a spearate SDP would quickly exhaust the available IDs and immensely complicate the management of such a topology.

An SDP can support multiple service connections. Services inherit the characteristics and status changes of the SDP to which they are connected.

Multiple serivces arriving at the egress PE VC Label Demux point causes a concern; how does the VC Label Demux differntiate between the different services and ensure proper correlation to its locally connected service?

Knowledge Verification – Customer data interface

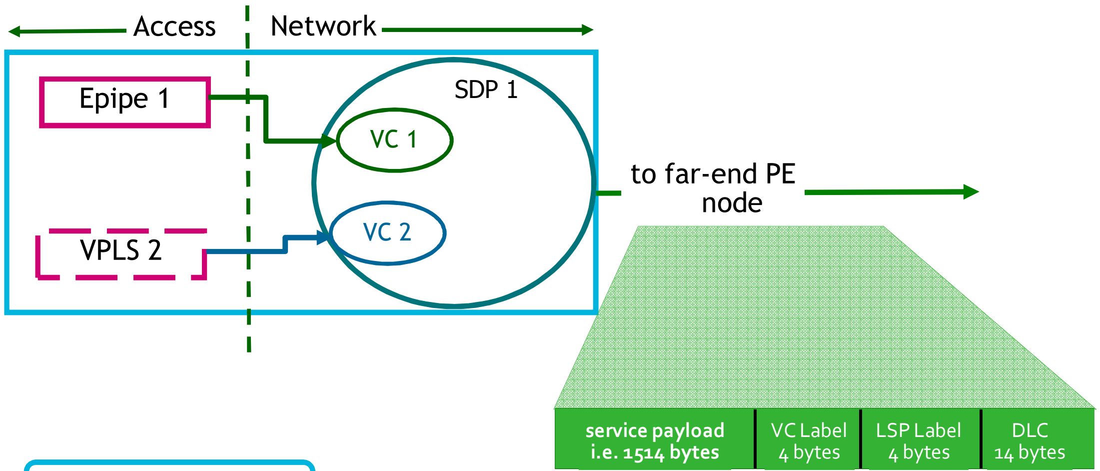
Which of the following service components is an interface to customer data?

a. Access Interface.
b. Service Distribution Point.
c. Network Interface.
d. Provider Edge (PE node).

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.8 VC Label



VC Label

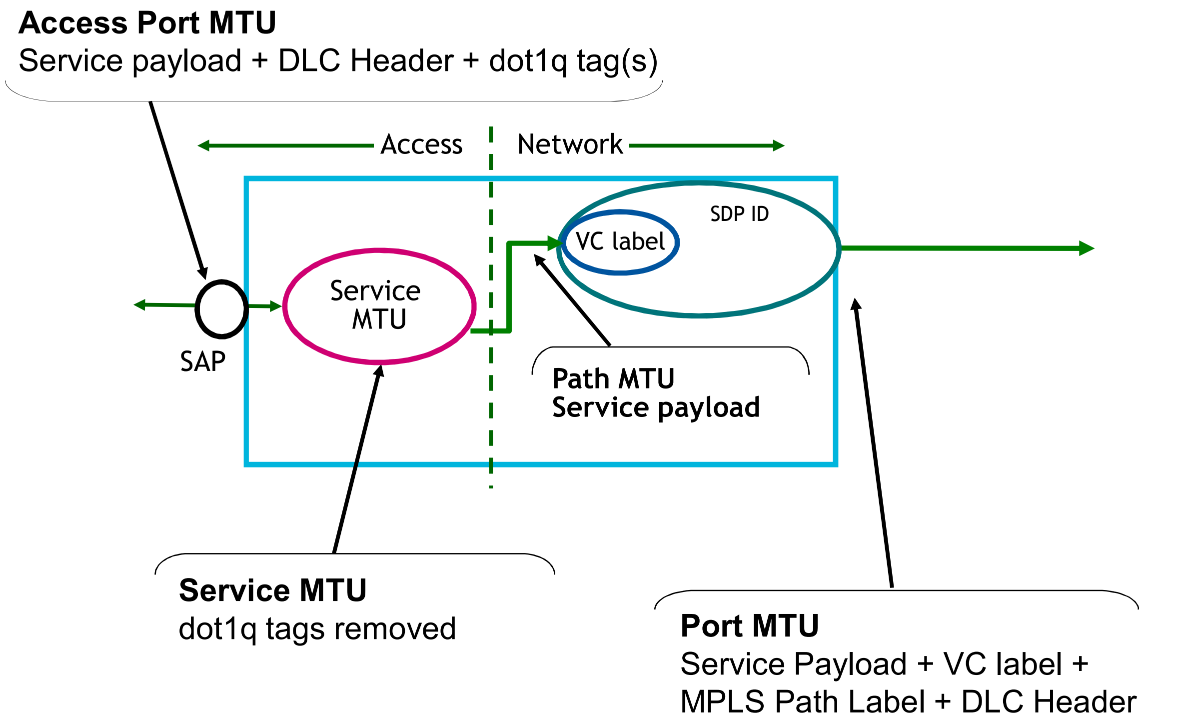
- 4-byte header used to uniquely identify service within an SDP
- Must be unique within the SDP; in SR-OS the label is unique to node and cannot be reused
- Specified when binding the service to the SDP; best practice is VC ID = Svc ID

The differentiator is known as the VC Label, or Virtual Circuit Label. The VC label is a 4-byte identifier that is used to identify individual services with the IP/MPLS network. The MPLS Forum specifies that the VC label must be unique within the SDP. However, the SR-OS uses a common label pool such that once a label is used, it is no longer available for another service. This is illustrated above where epipe 1 is connected into SDP 1 with VC Label 1. The VPLS service (ID 2) is also connected to SDP 1 but cannot use VC Label 1 since it is already used.

It is considered a *best practice* for service providers map the VC ID to the Service ID. This practise ensures that a unique ID will be assigned for each service and provide consistency in the numbering pattern which can greatly simplify identifying associated components, particularly during fault isolation exercises.

2 Maximum Transmission Unit

2.1 MTU Types



Alcatel·Lucent UNIVERSITY

MTU Size Considerations

Maximum Transmission Unit (MTU) size defines the maximum size, in bytes, for a single unit of data that can be sent over a given link. If a packet cannot fit into the MTU of a given link, it is fragmented, and the fragments reassembled on the other end of the connection. Since fragmentation is an expensive operation and cannot be done at line rates it is not supported on the 7750 SR. If there is an MTU mismatch, a service will not work.

There is an MTU associated with all of the data links on the 7750 SR, including both physical virtual circuits. A virtual circuit can be built using either MPLS or GRE encapsulation.

Physical MTU:
This MTU is configured on the physical ports of the 7x50 router and applies to both access and network ports. This MTU governs how large packets can be on a given physical wire. If the physical MTU on an egress interface or PoS channel indicates the next hop on an SDP path cannot support the current path-mtu, the operational path-mtu on that SDP will be modified to a value that can be transmitted without fragmentation.

Service MTU:
This MTU is associated with a service and determines how large packets can be that are sent from the customer across the service. The service-mtu defines the service payload capabilities of the service. It is used by the system to validate SAP creation and SDP binding within the service. Based on the encap-type and the physical mtu, a SAP created on an access interface will be limited to a maximum service payload size. If that service payload is less than the required service-mtu, the SAP will not enter the operative state.

SDP Path MTU:
This MTU determines how large packets can be that are sent over the service path.
Path MTU configures the Maximum Transmission Unit (MTU) in bytes that the Service Distribution Path (SDP) can transmit to the far-end without packet dropping or IP fragmentation overriding the SDP-type default path-mtu. Dynamic maintenance protocols on the SDP like RSVP may override this setting.

2.2 Physical MTU Size - MPLS

Network interface MTU must be greater than maximum service MTU plus largest encapsulation type.

Minimum MTU size for 1514-byte Service over MPLS

Packet over SONET	Ethernet	Overhead
1514 bytes	1514 bytes	Service Payload
4 bytes	4 bytes	MPLS tag used as Service Identifier
4 bytes	4 bytes	MPLS Tag used as Egress LSP
4 bytes	n/a	MPLS External Header
2 bytes	n/a	PPP MCLSP Header
n/a	14 bytes	DLC Header
1528 bytes	1536 bytes	Total

2.3 Physical MTU Size - GRE

Network interface MTU must be greater than maximum service MTU plus largest encapsulation type.

Minimum MTU size for 1514-byte Service over GRE

Packet over SONET	Ethernet	Overhead
1514 bytes	1514 bytes	Service Payload
4 bytes	4 bytes	MPLS tag used as Service Identifier
4 bytes	4 bytes	Generic Router Encapsulation
20 bytes	20 bytes	IP Header
2 bytes	n/a	PPP IPCP Header
n/a	14 bytes	DLC Header
1544 bytes	1556 bytes	Total

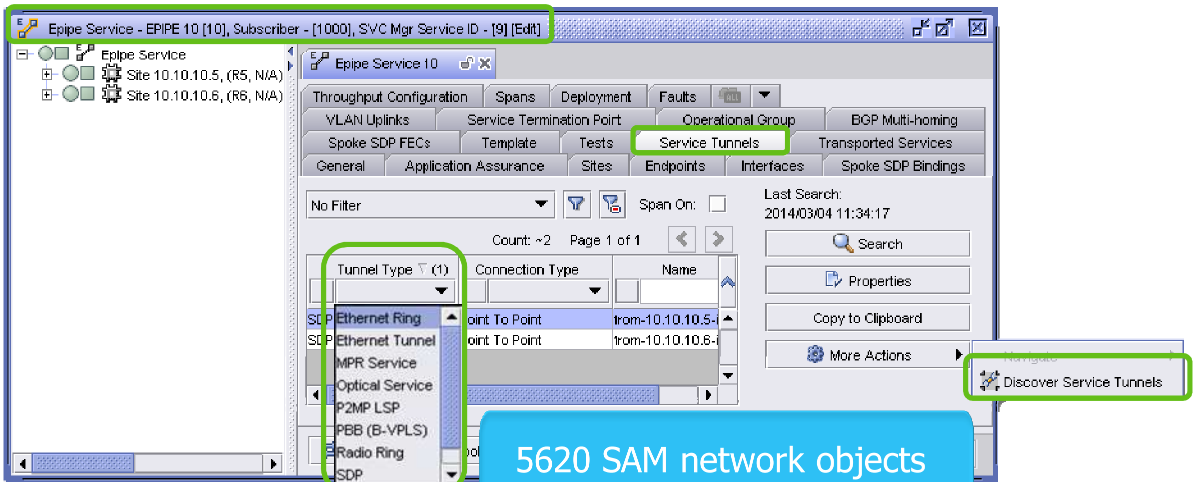
Physical MTU Default Values

Port Type	Mode	Encap Type	Default (Bytes)
Ethernet	access	null	1514
Ethernet	access	dot1q	1518
Fast Ethernet	network	-	1514
Other Ethernet	network	-	9212
PoS Channel	access	bcp-null	1522
PoS Channel	access	bcp-dot1q	1526
PoS Channel	access	ipcp	1502
PoS Channel	network	-	9208

3 Service Tunnels

3.1 Service Tunnel Overview

Service tunnels are a logical construct within the 5620 SAM, used to uni-directionally direct traffic from one device to another device.



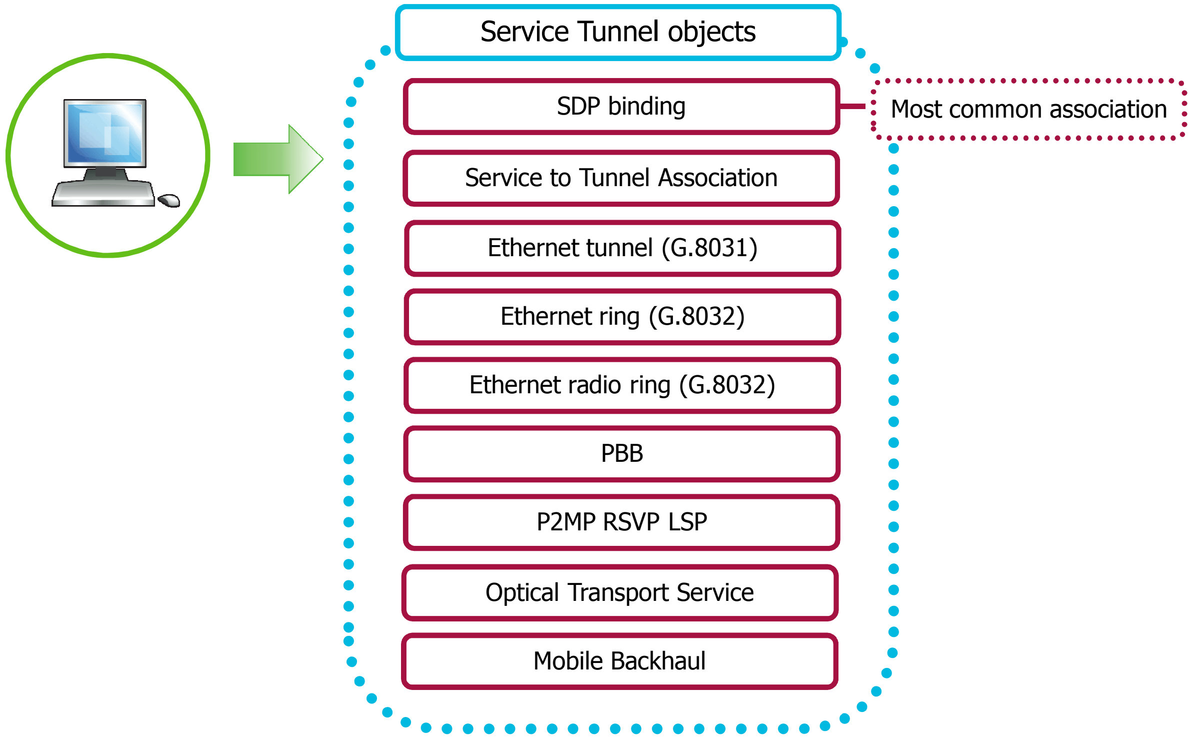
5620 SAM network objects be used as service tunnels.

Alcatel·Lucent UNIVERSITY

The most common type of tunnel used in 5620 SAM is a Service Distribution Point binding. Service tunnels originate on an SDP on a source NE and terminate at a destination NE. The destination NE directs packets from the service tunnel to the correct service egress interfaces (SAPs) on that device. Services that originate and terminate on the same NE do not require service tunnels, because the same NE is both the source and the destination. However, because the concept of a tunnel is a logical construct within 5620 SAM, a number of different configurable objects can actually be used as service tunnels.

The Service Tunnels tab exists on the applicable service configuration forms. This tab lists the objects considered as service tunnels (such as SDPs, Ethernet rings, Ethernet tunnels, other services) that are currently used by the service you are querying. The associated Discover Service Tunnels button removes any previously discovered service tunnels on the service and initiates a manual rediscovery of the tunnels, based on direct usage and current service configurations.

3.2 Service Tunnel Object Types

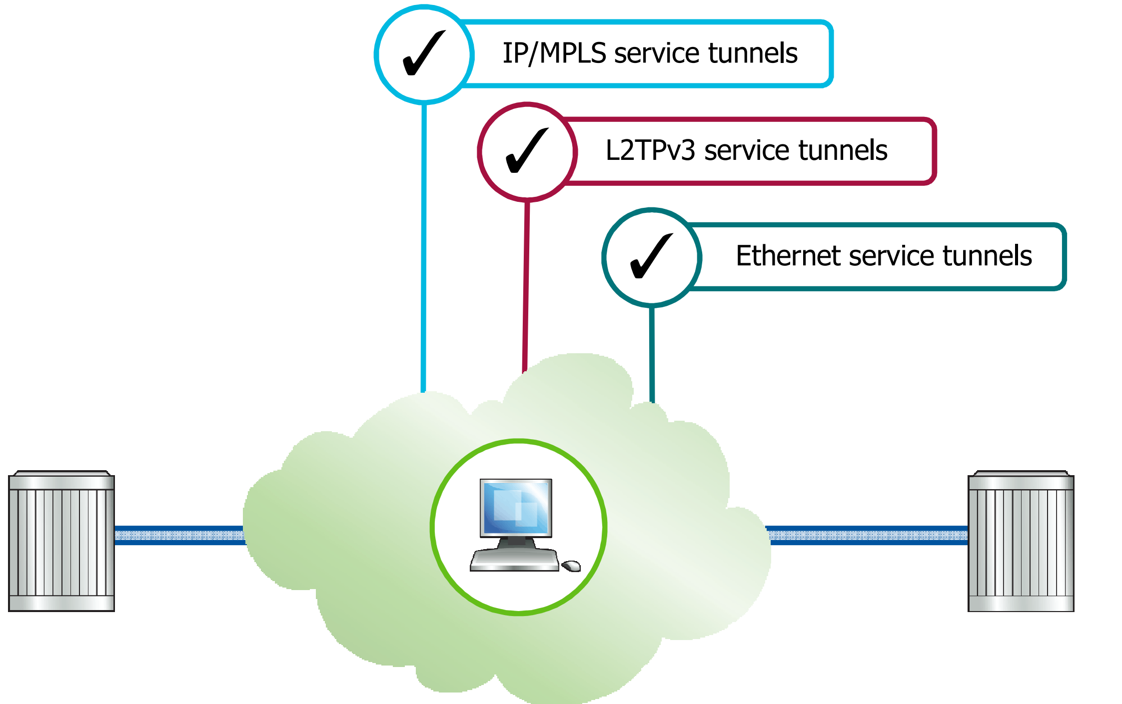


The most common type of tunnel used in 5620 SAM is a Service Distribution Point binding. Service tunnels originate on an SDP on a source NE and terminate at a destination NE. The destination NE directs packets from the service tunnel to the correct service egress interfaces (SAPs) on that device. Services that originate and terminate on the same NE do not require service tunnels, because the same NE is both the source and the destination.

However, because the concept of a tunnel is a logical construct within 5620 SAM, a number of different configurable objects can actually be used as service tunnels, including:

- **SDP binding:** Because SDP bindings can be associated to a service of any type, the service tunnel discovery includes services that are associated to SDP bindings of a given service.
- **Service to Tunnel Association:** Discovery adds tunnels that are associated to a given service.
- **Ethernet tunnel (G.8031):** Discovery adds the global Ethernet Tunnel that the Tunnel Endpoint (SAP's terminating port) is a member of.
- **Ethernet ring (G.8032):** Discovery adds the Ethernet Ring that the Ethernet Element is a member of.
- **Ethernet radio ring (G.8032):** Discovery adds the Ethernet radio ring that the Ethernet Element is a member of.
- **PBB:** Discovery adds the VPLS or MVPLS services which contain the PBB tunnel (B-Sites) of the given Epipe or VPLS.
- **P2MP RSVP LSP:** Discovery adds the P2MP LSPs retrieved from the MVPN LSP Template associated to PIM sites.
- **Optical Transport Service:** Discovery adds optical services that are traversing network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service.
- **Mobile backhaul (applicable to 9500 MPR and 7705 SAR on MPLS-based services running over VLAN):** Discovery adds MPR VLL services that are associated to an SDP tunnel or are traversing through network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service.

3.3 Tunnel Types



2 · 1 · 26
Service structure · Components
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

IP/MPLS service tunnels

Distributed service traffic is transported between PE NEs by circuits aggregated in unidirectional service tunnels. The encapsulation of the data between the two managed edge NEs appears as a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

L2TPv3 service tunnels

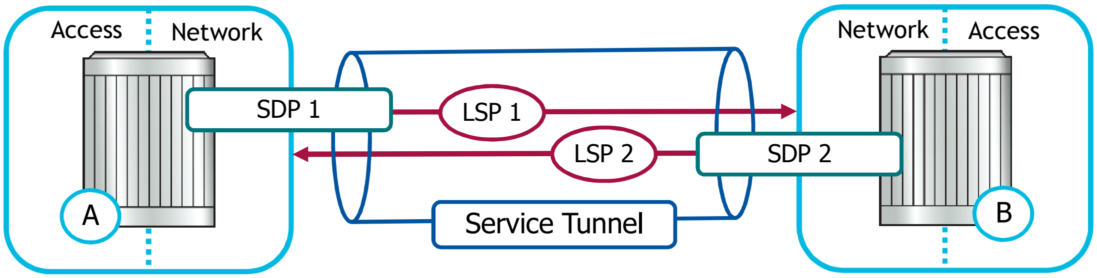
Transport L2 Ethernet frames across a native IPv6 environment. This feature provides Ethernet pseudo wire-like services without the use of MPLS encapsulation and labels. The logical service separation and mux/demux is achieved by using discrete source and destination IPv6 addresses on the routers, rather than tunnel session or service labels.

Ethernet (G.803.1) service tunnels

You can select an Ethernet tunnel when configuring an L2 access interface on a B-VPLS. The 5620 SAM uses two different approaches to configure Ethernet tunnels in the network:

- 5620 SAM provisions an end-to-end Ethernet G.8031 tunnel which reduces configuration errors and aids the diagnosis of any problem in the tunnel. 5620 SAM automatically configures the Ethernet tunnel endpoint and path endpoint on each of the participating NEs.
- The 5620 SAM provides the ability to provision Ethernet tunnel endpoints and path endpoints separately on each NE. If Ethernet tunnel endpoints are created this way (or discovered from the NE) you can associate them to a network-wide Ethernet tunnel and path, but this must be done manually.

3.4 IP/MPLS Service Tunnel Overview



The operational theory of a service tunnel is that the encapsulation of the data between the two managed edge NEs appears as a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

A Service Tunnel is the logical construct that is used to *transport* traffic from the ingress PE to its destination as defined by the associated LSP.

Though the SR-OS supports creating static service tunnels, service providers will typically allow the system to do so. Dynamic creation of service tunnels uses targeted-LDP, which is a sub-set of the LDP protocol that will be dscussed later. Additionally, the service model also requires that a return service the tunnel must also exist before it can be used to transport customer traffic.

3.5 IP/MPLS Tunnel Encapsulation

Generic Routing Encapsulation (GRE)

- Encapsulates traffic in an IP/GRE header; appears like an IP packet
- Low control plane overhead
- Uses normal IP routing to find a path

Multi Protocol Label Switching (MPLS)

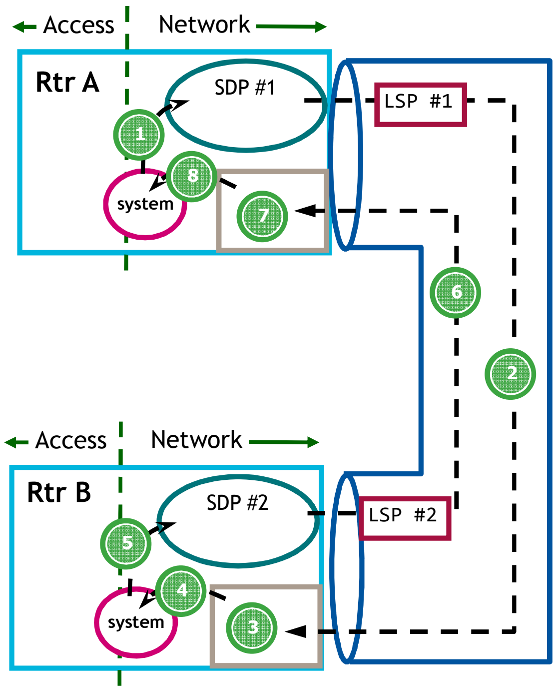
- Uses LDP or RSVP for label signaling
- LDP auto-bind available to simplify configuration
- LDP relies on an IGP to find its path
- RSVP
  - Requires manual configuration
  - Can be loose or strict
  - May reserve bandwidth
  - Can use Fast ReRoute to speed convergence

Alcatel·Lucent UNIVERSITY

SDP Encapsulation

- Generic Routing Encapsulation
  - Low control plane overhead
  - Uses an IGP (ie. OSPF, IS-IS) to find a path from edge to edge
  - Convergence depends on the IGP
- MPLS
  - Uses Label Switched Paths (LSP). Primary and secondary paths provide LSP protection.
  - Paths can be manually configured or signalled using LDP or RSVP-TE

3.6 Tunnel signaling process



1. Send "hello" to Rtr B 'system' interface thru SDP
2. Route to next hop via LSP label table (RSVP or LDP)
3. CAM lookup on MDA - destination = Rtr B 'system'
4. Pass to 'system': 'hello' message: fm Rtr A
5. Send response via SDP with destination of Rtr A
6. Route to next hop via LSP label table (RSVP or LDP)
7. CAM lookup on MDA - destination = Rtr A 'system'
8. Pass to 'system': 'response' message: fm Rtr B
9. Round trip exists Signal tunnels Operational UP

The diagram above illustrates the process for service tunnel signaling. In summary, the source router sends a connect message to the destination router system interface through the associated SDP. At the destination, the request is passed to the system interface which sends a response back to the source router through an SDP.

The source router recognizes this as a response to the original request arriving from an LSP, onfirming that a return service tunnel is available. Both ends signal that a bidirectional set of tunnel is available and ready to support VPN traffic through the core.

Knowledge Verification – MPLS tunnel encapsulation

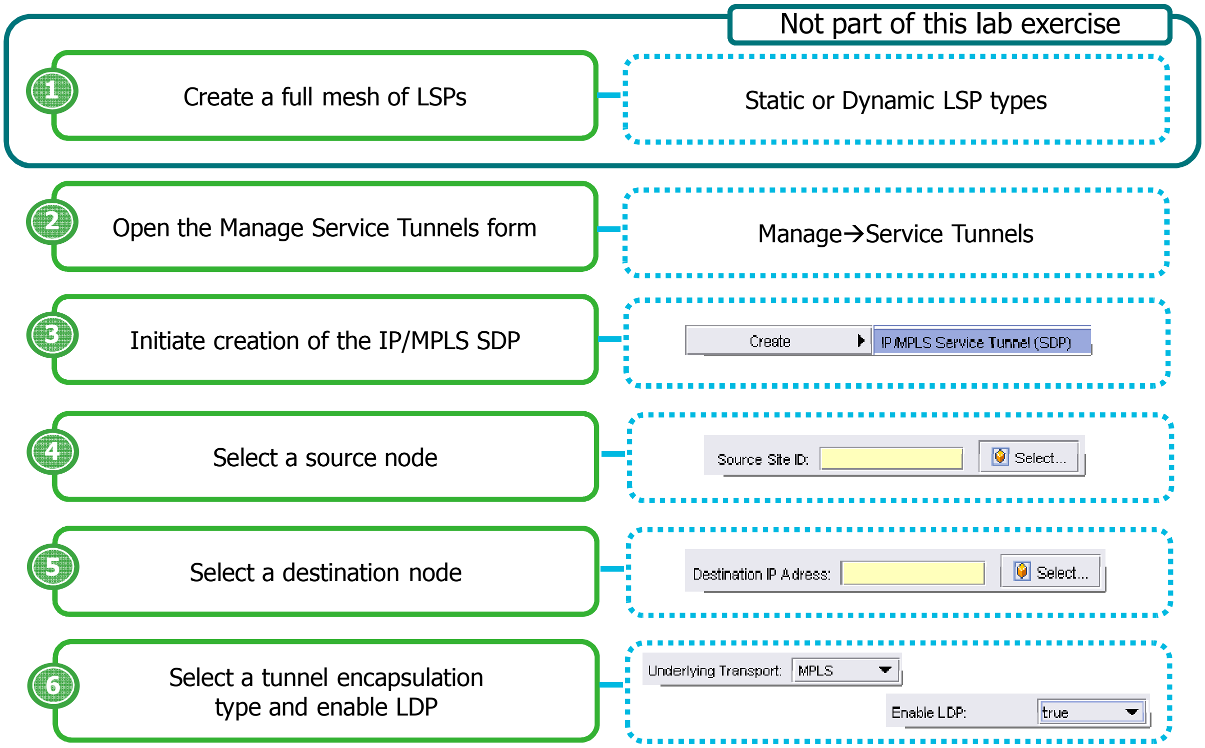
Which of the following items is not a characteristic of MPLS tunnel encapsulation?

a. Uses LDP or RSVP for label signaling.
b. LDP auto-bind available to simplify configuration.
c. Uses normal IP routing to find a path.
d. LDP relies on an IGP to find its path.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

3.7 Service tunnel configuration workflow



Alcatel·Lucent
UNIVERSITY

The above workflow outlines the high-level steps necessary to create an IP/MPLS service tunnel.

Service tunnels are **unidirectional**, so they are required in both directions between the source NE and the destination NE. Repeat the steps associated with the IP/MPLS Service Tunnel (SDP) configuration wizard to configure the return tunnel.

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to create a service tunnel

Lab Exercises
Create an IP/MPLS Service Tunnel

Time allowed: 10 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

This page is left blank intentionally

End of module
Components

Alcatel·Lucent
UNIVERSITY

Section 3
Service Types

Module 1
VPLS

TOS36042_V3.0-SG-English-Ed1 Module 3.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to:

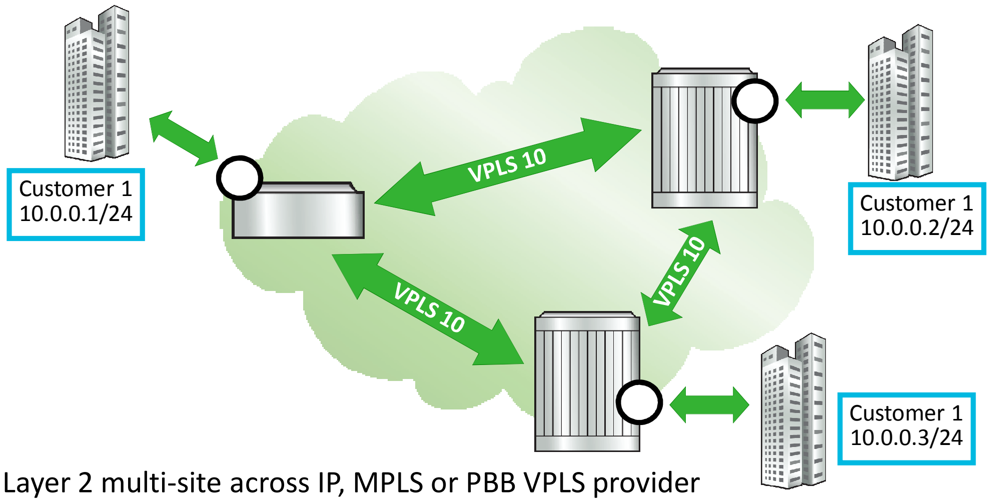
- Describe Characteristics and benefits of a VPLS service
- Explain the 7750 SR VPLS implementation
- Explain the operation of a VPLS service
- List the steps in configuring a VPLS service
- Identify VPLS service management tasks

This page is left blank intentionally

This page is left blank intentionally

1 Virtual Private LAN Service (VPLS)

1.1 VPLS Overview



- Layer 2 multi-site across IP, MPLS or PBB VPLS provider network
- Customer sites appear to be in single broadcast domain (same LAN)
- Uses Ethernet access interface, simplifying LAN/ WAN boundary
  - *Layer 2 MAC learning at Access interface*
  - *independent of IP routing in IP/ MPLS core*

Virtual Private LAN Service (VPLS) as described in Internet Draft *draft-ietf-ppvpn-vpls-ldp-01.txt*, is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning.

VPLS offers a balance between point-to-point Frame Relay service and outsourced routed services (VPRN). VPLS enables each customer to maintain control of their own routing strategies. All customer routers in the VPLS service are part of the same subnet (LAN) which simplifies the IP addressing plan, especially when compared to a mesh constructed from many separate point-topoint connections. The VPLS service management is simplified since the service is not aware of and does not participate in the IP addressing and routing.

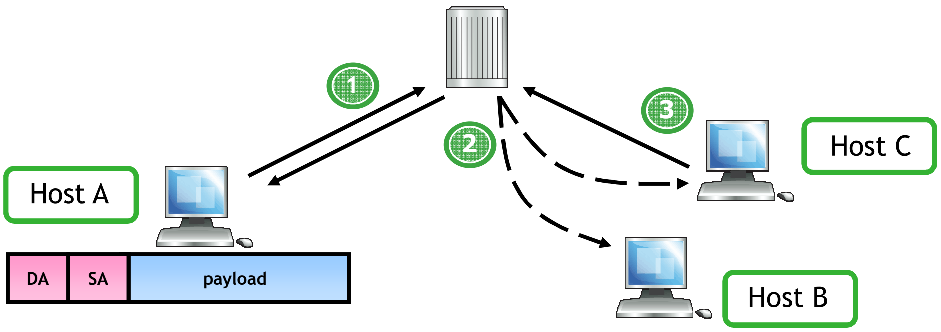
A VPLS service provides connectivity between two or more SAPs on one (which is considered a local service) or more (which is considered a distributed service) service routers. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the VPLS service.

Other VPLS advantages include:

- VPLS is a transparent, protocol-independent service.
- There is no Layer 2 protocol conversion between LAN and WAN technologies.
- There is no need to design, manage, configure, and maintain separate WAN access equipment, thus, eliminating the need to train personnel on WAN technologies such as Frame Relay.

2 Preliminary concepts

2.1 Populating a Forwarding Database (FDB)



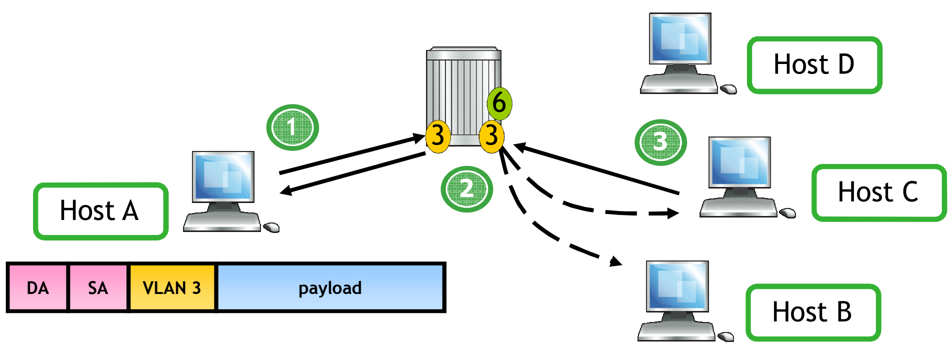
Ethertype for some common Protocols	
1/1/1	00-00-5e-00-01-8e
1/1/3	00-00-5e-00-01-8e

Host A sends a frame to Host C

1. The switch receives a frame on port 1/1/1
   - Host A's MAC address is learned from the frame's Source Address field and is associated with port 1/1/1
2. If the Destination Address is not already in the FDB, the switch floods the frame out all ports except for the source port 1/1/1
3. Host C responds to Host A, and all other devices drop the flooded frame
   - From Host C's response frame, the switch associates Host C's MAC address with port 1/1/3

2.2 Forwarding Databases Using Tagging

Virtual LANs (VLANs) are used to split a single switch into multiple virtual switches, each with the ability to service the hosts associated within that VLAN



Alcatel·Lucent UNIVERSITY

As an example Hosts A B C are part of VLAN 3, Host D is part of VLAN 6:

1. The switch receives a frame on port 1/1/1:3 (:3 signifies VLAN 3). Host A’s MAC address is learned and is associated with in VLAN 3’s FDB.
2. If the Destination Address is not already in the FDB, the switch floods the frame out **all ports associated with VLAN 3.**
3. Host C responds to Host A, and all other devices drop the flooded frame. From Host C’s response frame, the switch populates Host C’s MAC address in VLAN 3’s FDB.

2.3 Ethertype

The Ethertype field describes the payload of the Ethernet frame

Internet Protocol, Version Provider Bridging 4 (IPv4)	0x0800
Address Resolution Protocol (ARP)	0x0806
VLAN – Tagging (Dot1Q)	0x8100
VLAN – Tagging (QinQ)	0x9100
IPv6	0x86DD
MPLS unicast	0x8847
Provider Bridging	0x88a8

For example, Etype 8847 identifies this packet as Unicast MPLS

DA	SA	0x8447	MPLS Label	VC Label	Payload	FCS

Etype

EtherType numbering generally starts from 0x0800. In the example used, Etype 8847 indicates a unicast MPLS ethernet frame. As we have seen, an MPLS header includes a MPLS Label and Virtual Circuit id. When the 7750 SR looks at the etype field and sees 8847, immediately the following applies:

Service Payload / MTU: 1514 bytes

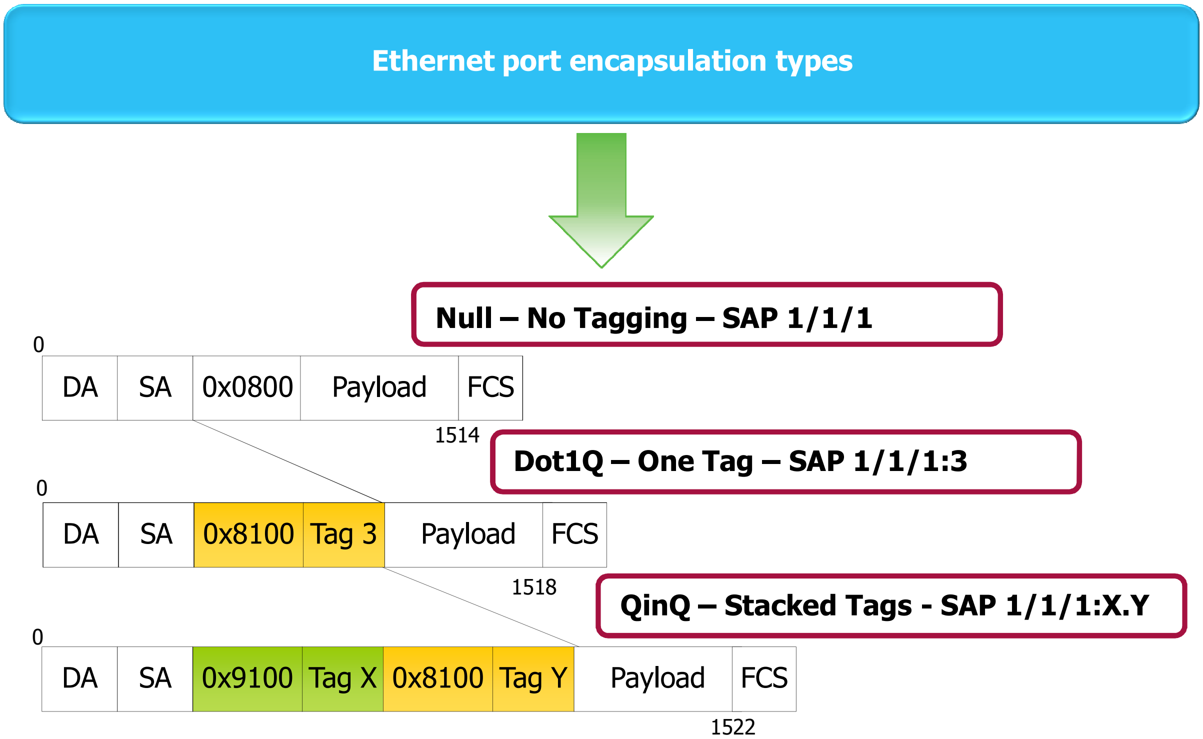
MPLS tag used as service label: 4 bytes

MPLS tag used for transport label: 4 bytes

DLC Header: 14 bytes

1536 bytes

2.4 Ethertype - VLAN



Ethernet port encapsulation type can be configured as one of the following:

- Null Header (Raw Mode), all bits after the ‘type’ field are treated as data
- Dot1q Header (Single tag header), adds an additional 4 byte “TAG”
- QinQ Header (Two tags header), adds two TAGs after Source Address field

The Physical MTU on an ethernet access interface needs to be set to at least:

- 1514 with mode-access and encap-type null
  - 1500 + 14 DLC header
- 1518 with mode-access and encap-type dot1q
  - 1500 + 14 DLC header + 4 dot1q tag
- 1522 with Q-in-Q tagging
  - 1500 + 14 DLC header +4 dot1q tag +4 additional Q tag

SAP Ingress:

- Any frame that does not match a defined SAP within a service will be dropped
- Tags that are explicitly matched become stripped on ingress
- A wildcard can be used as a SAP defined tag (SAP:* or SAP:X.*), this has a 4-byte impact upon the service MTU as the tag is retained rather that stripped
- There is no limit is put on the number of inner tags or the value of each tag provided the MTU size has been adjusted to accommodate the extra tagging as these tags are considered part of the payload

SAP Egress:

- SAP:X push dot1q-etype and tag X on egress frames
- SAP:X.Y push QinQ-etype and tag X / Dot1q-etype and tag Y on egress
- Default and wildcard SAPs do not regenerate tags on egress

Knowledge Verification – VPLS definition

What is the best definition of Virtual Private LAN Service.

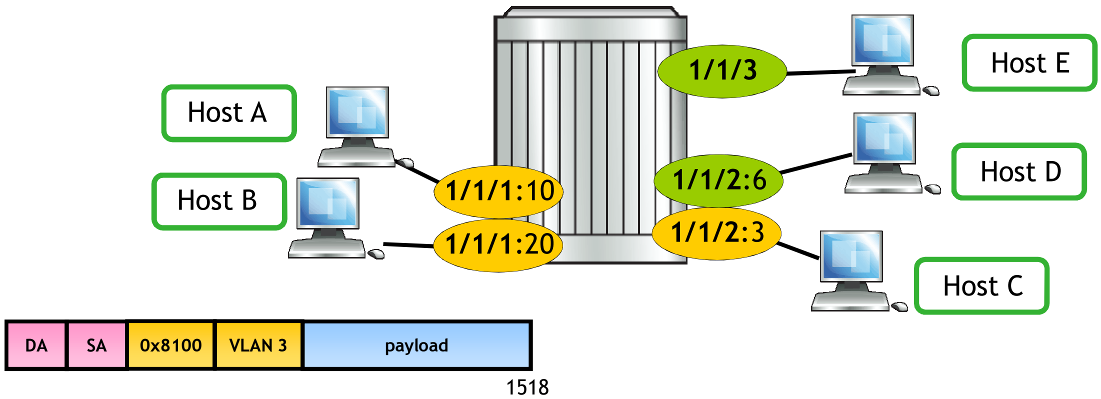
a. A type of VPN where IP is transported in a point-to-point manner. CPE devices are connected through nodes, and the nodes are connected to an IP tunnel.
b. A host communicates with an IP router interface to send and receive Internet traffic.
c. A network exhibiting at least some of the characteristics of a private network, even though it uses the resources of a public switched network.
d. A type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. The services may be from different locations, but appear to be on the same LAN.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

3 Configuration of a VPLS service

3.1 Building a Local Virtual Private LAN Service (VPLS)



1. Change the ports facing customers to mode access.
2. Enable tagging on the ports, if needed.
3. Create Service Access Points (SAPs) within the VPLS service using the desired port/tag.

Alcatel·Lucent UNIVERSITY

Creating a Local VPLS Service, meaning a service that exists solely on a single node:

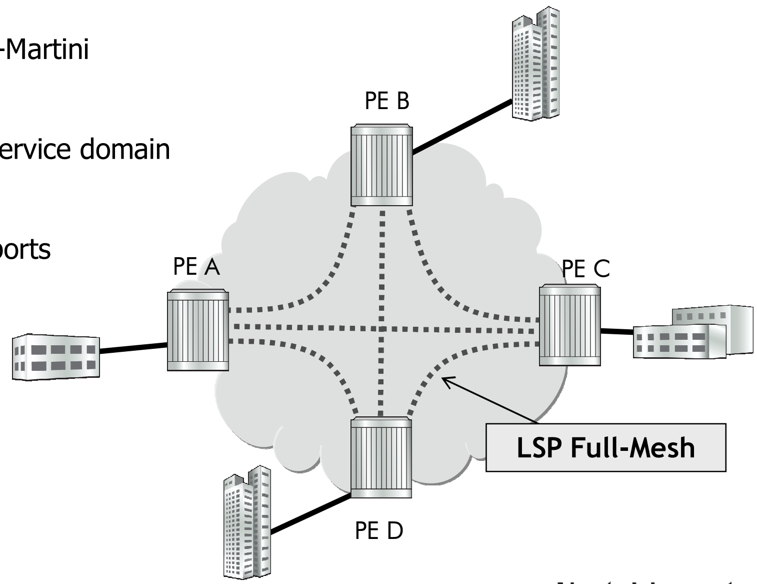
- Change the ports facing customers to mode access
  - Ethernet mode access
- Enable tagging on the ports, if needed
  - Ethernet encap-type dot1q
- Create Service Access Points (SAPs) within the VPLS service using the desired port/tag
  - VPLS 300
    - sap 1/1/1:10
    - sap 1/1/1:20
    - sap 1/1/2:3
  - VPLS 600
    - sap 1/1/2:6
    - sap 1/1/3

All frames that ingress to a service are compared to the FDB to determine which SAP or SDP the frame is to be forwarded out. If the egressing port is a SAP, the frame will be regenerated with the appropriate tags (dot1Q and QinQ) based on the SAP definition. For example, a dot1q SAP that is provisioned as 1/1/1:3 will have the dot1q tag 3 inserted into all frames that egress that port based on the FDB.

When a wildcard is used, for example 1/1/1:* although the SAP is defined as dot1Q, no additional tags are added on egress.

3.2 How is a VPLS provided over MPLS?

1. **Bridging capable PE routers**
   - connected with a full mesh of MPLS LSP tunnels
2. **Per-Service VC labels**
   - negotiated using draft-Martini
3. **Unknown/broadcast**
   - traffic replicated in a service domain
4. **MAC learning**
   - over tunnel & access ports
   - separate FIB per VPLS



3 · 1 · 17
Service Types · VPLS
5620 SAM · Services Operations and Provisioning

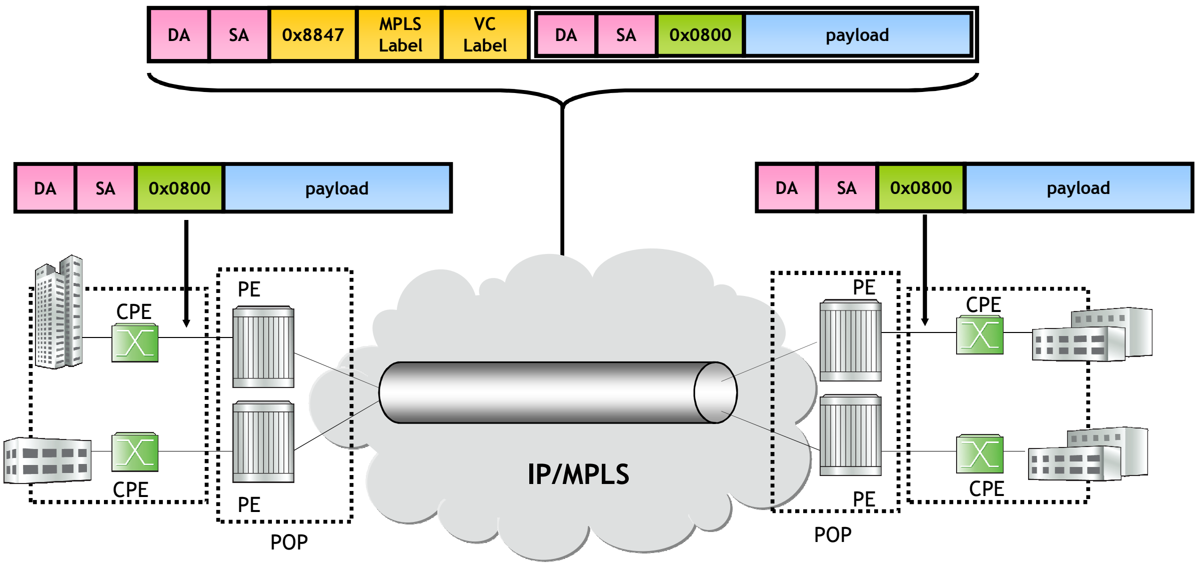
Alcatel·Lucent UNIVERSITY

For each VPN at each site, a Customer Edge (CE) device connects to the Provider Edge (PE) router via a point-to-point access connection.

Ethernet serves as the framing technology between the CE device and the PE router in the provider's network. Frames can include IEEE 802.1Q Ethernet VLAN tags, which allow customers to segment their networks and assign quality of service priorities to LAN traffic. VPLS also supports "QinQ" encapsulation, where a second VLAN tag is added as a service delimiter. From the customer's perspective, the entire VPN looks like a single Ethernet LAN, with the PE acting as a bridge that switches frames on the basis of their Layer-2 destination MAC addresses.

On the provider's side, however, PEs are interconnected with Generic Routing Encapsulation (GRE) and/or Multiprotocol Label Switching (MPLS) tunnels. If PEs are connected using GRE tunnels traffic is encapsulated and routed through the core network using standard IP frame formats and addressing. If PEs are connected using MPLS tunnels traffic is encapsulated in an MPLS frame and transmitted using MPLS labels. MPLS routes can be signaled using RSVP-TE or LDP.

3.3 Packet Format



The customer frame becomes the payload of the MPLS frame

Alcatel·Lucent UNIVERSITY

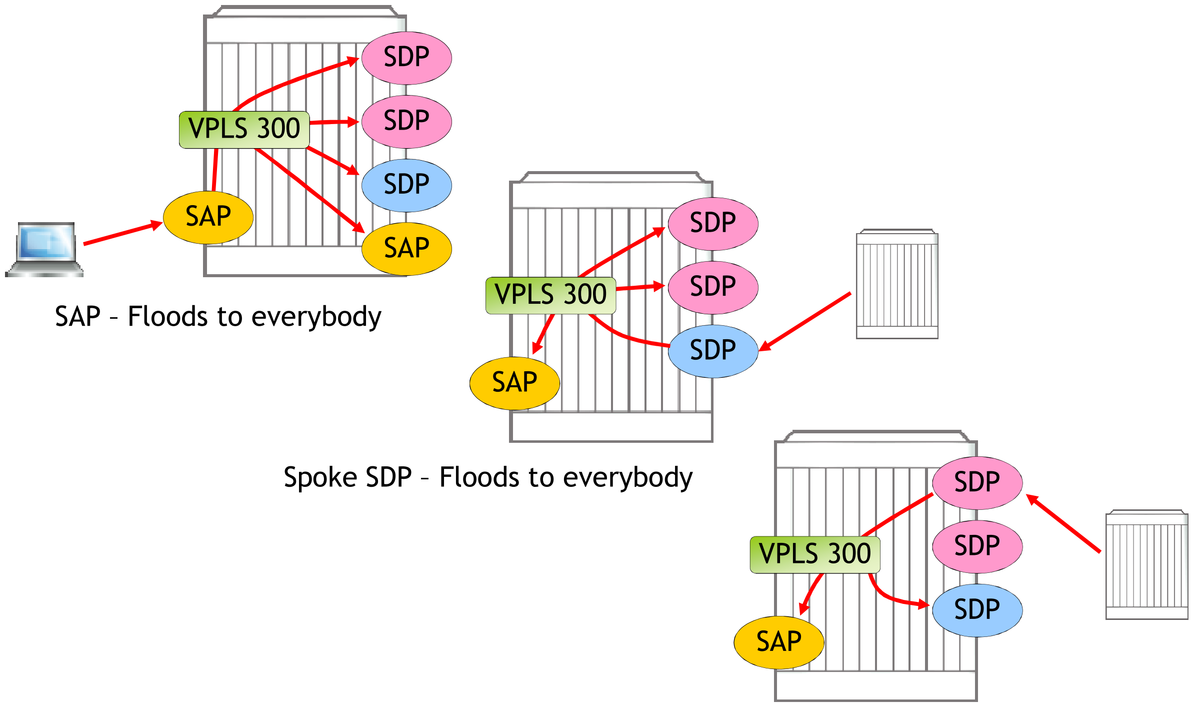
The L1 encapsulation is the additional L1 information, most likely SONET or SDH, needed to move data across a carrier's infrastructure.

The transport label is the MPLS label that identifies the MPLS tunnel transporting the encapsulated L2 frames or cells through the MPLS network.

The VC label is an MPLS label that identifies a particular service, that is being transported through the MPLS tunnel.

The control word contains information about the connection. It may be optional or mandatory depending on the network configuration.

3.4 Flooding Traffic within a VPLS



Alcatel·Lucent UNIVERSITY

Flooded traffic received on:

- SAP – Flooded traffic received on a SAP is replicated to other SAPs, Spoke SDPs, and Mesh SDPs
- Spoke-SDP – Flooded traffic received on a Spoke SDP is replicated to other SAPs, Spoke SDPs, and Mesh SDPs
- Mesh-SDP – Flooded traffic received on a Mesh SDP is replicated to other SAPs and Spoke SDPs, but **is not** transmitted on other Mesh SDPs

All frames that ingress to a service are compared to the FDB to determine which SAP or SDP the frame is to be forwarded out. Flooding only occurs if there is no existing entry in the FDB. Egress tags are generated based on the SAP definition of the egress port in the FDB.

Knowledge Verification – Flooding traffic with a VPLS

What network component does not flood VPLS traffic to all?

a. SAP.
b. Mesh SDP.
c. Spoke SDP.

Alcatel·Lucent
UNIVERSITY

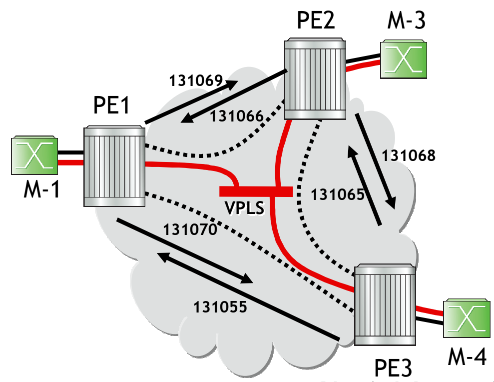
Choose the correct answer for the knowledge verification question above.

3.5 VPLS - VC Label

VC-label Signaling between PEs per VPLS service instance

- Each PE automatically initiates a targeted LDP (TLDP) session to the far-end System IP address as soon as an SDP is bound to a layer-2 service
- TLDP is used to negotiate the VC (or service) label that will be used when sending data packets for the service
- TLDP uses the VC ID to identify the service tunnel, so it must match between PE nodes (best practice is to set VC ID the same as the service ID)
- The VC label allocated by each PE may be different

PE1->PE2: For VC-ID **102** Use VC-label **131069**
PE2->PE1: For VC-ID **102** Use VC-label **131066**
PE1->PE3: For VC-ID **103** Use VC-label **131070**
PE3->PE1: For VC-ID **103** Use VC-label **131055**
PE2->PE3: For VC-ID **203** Use VC-label **131068**
PE3->PE2: For VC-ID **203** Use VC-label **131065**



Alcatel·Lucent UNIVERSITY

Customer packets are transported either inside an IP packet (GRE) or inside an MPLS packet.

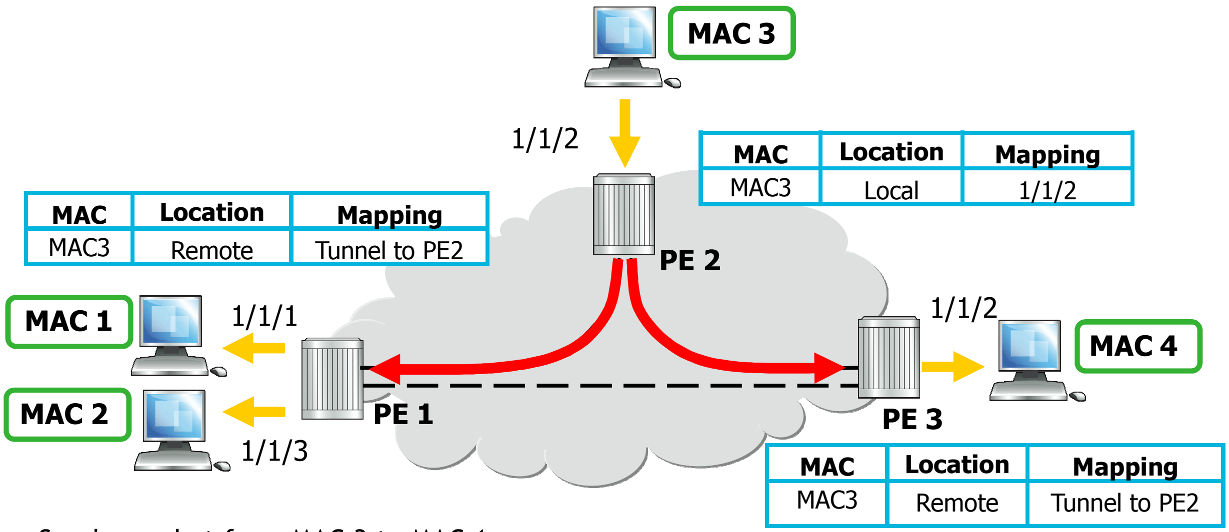
The packet carries an inner (VC) label that identifies the service the packet belongs to. This label is sometimes referred to as the Martini label which is an MPLS label that identifies the particular service that is being transported through the MPLS tunnel.

When a packet arrives at the destination, the outer IP address or MPLS label is stripped off. At this point the inner label is examined to determine which service the packet belongs to.

After determining which service the packet belongs to, the customer's Ethernet packet is examined and its MAC address is looked up in a table on the PE to determine which SAP the packet should go to.

VC labels can be assigned manually or automatically using targeted LDP (TLDP). The TLDP protocol is used to dynamically negotiate VC labels between PE's. This method is not error prone and scales much better than manually assigning labels.

3.6 VPLS Packet Walkthrough - VPLS Learning



Send a packet from MAC 3 to MAC 1

- PE2 learns that MAC 3 is reached on Port 1/1/2
- PE2 floods to PE1 with VC-label pe2-1 and PE3 with VC-label pe2-3
- PE1 learns that MAC 3 is behind PE2
- PE3 learns that MAC 3 is behind PE2
- PE3 sends on Port 1/1/2
- PE1 sends on Port 1/1/1 & 1/1/3

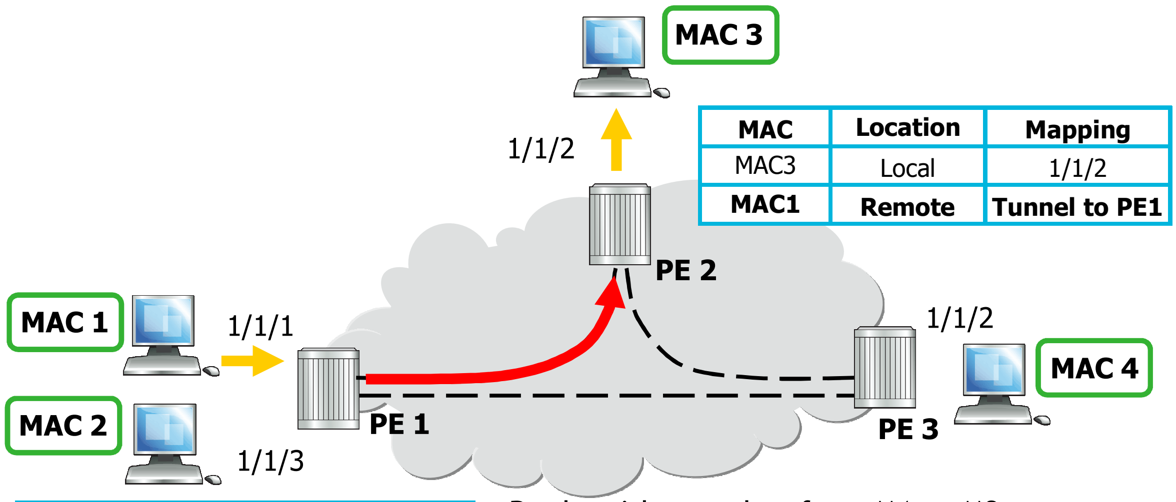
PE routers learn the source MAC addresses of the traffic arriving on their access and network ports.

Each PE router maintains a Forwarding Data Base (FDB) for each VPLS service instance and learned MAC addresses are populated in the FDB table of the service.

All traffic is switched based on MAC addresses and forwarded between all participating PE routers using the LSP tunnels.

Unknown packets (i.e. destination MAC address has not been learned) are forwarded on all the LSPs to the participating PE routers for that service until the target station responds and the MAC address is learned by the PE routers associated with that service.

3.7 VPLS Packet Forwarding



MAC	Location	Mapping
MAC3	Local	1/1/2
MAC1	**Remote**	**Tunnel to PE1**

MAC	Location	Mapping
MAC3	Remote	Tunnel to PE2
MAC1	**Local**	**1/1/1**

Reply with a packet from M1 to M3

- PE1 learns M1 is on Port 1/1/1
- PE1 knows that M3 is reachable via PE2
- PE1 sends to PE2 using VC-label pe1-2
- PE2 learns MAC 1 is reachable via PE1
- PE2 knows that M3 is reachable on Port 1/1/2

Local and Remote Aging Timers

In a manner similar to a layer 2 switch, learned MAC addresses can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). Each VPLS instance has independent aging timers for local (ingressed on a SAP) learned MAC and remote (ingress on a SDP) learned MAC entries in the forwarding database. Usually the remote-age timer is set to a longer interval to reduce the amount of flooding of destination-unknown MAC addresses through the carrier domain. The MAC aging timers can be disabled, preventing any MAC entries from being removed from the FIB because of aging.

Disable MAC Learning

When disable-learning is enabled, new local or remote MAC addresses will not be entered into the VPLS FIB. This feature is best combined with the following feature, Discard Unknown MAC addresses, otherwise your network runs the risk of being overwhelmed by excessive flooding of MAC addresses.

Discard Unknown MAC Addresses

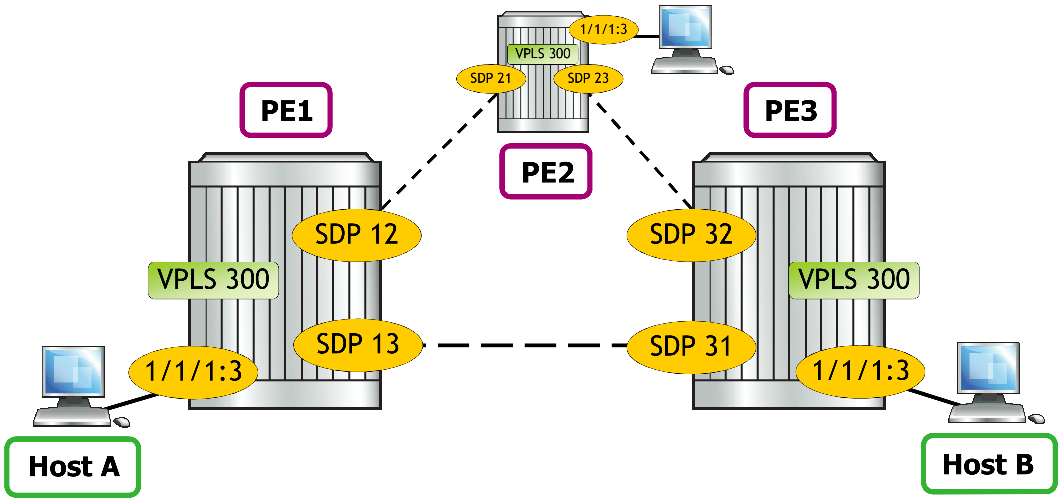
Unknown MAC discard is a feature which discards all packets ingressing a service where the destination MAC address is not found in the FIB. Normally all such packet would be flooded to all end points in the service. Unknown MAC discard can be used with the Disable MAC Learning and Disable MAC Aging options to create a fixed set of MAC addresses that are allowed to enter and pass through the service.

FIB Size Limit

The 7750 SR allows setting the maximum number of MAC entries allowed in the FIB per VPLS instance. This prevents a VPLS instance from consuming a disproportionate amount of resources. When the number of FIB entries allocated to the VPLS instance are exhausted, MAC learning is disabled until space becomes available in the FIB.

The size of the VPLS FIB can be configured with a low watermark and a high watermark, expressed as a percentage of the total FIB size limit.

3.8 Building a Distributed VPLS Service



1. Add Service Access Points (SAPs) 1/1/3 to the VPLS 300 service on each node
2. Add Service Distribution Points (SDPs) to the VPLS 300 service on each node

SDP per VPLS Limit

The 7750 SR supports 100 SDPs per VPLS as of release 6.1 (50 SDPs per VPLS pre R6.1)

Service-id: ***VPLS***

Customer (subscriber) Association

Service Access Point ***Select node and port***

Select Accounting Policy (optional)
Select Ingress/Egress QOS Policies (optional)
Select scheduler policy (optional)
Select Filter policies (optional)

Service Distribution Path ***Binds a service to an SDP***

Can be a Spoke or Mesh SDP

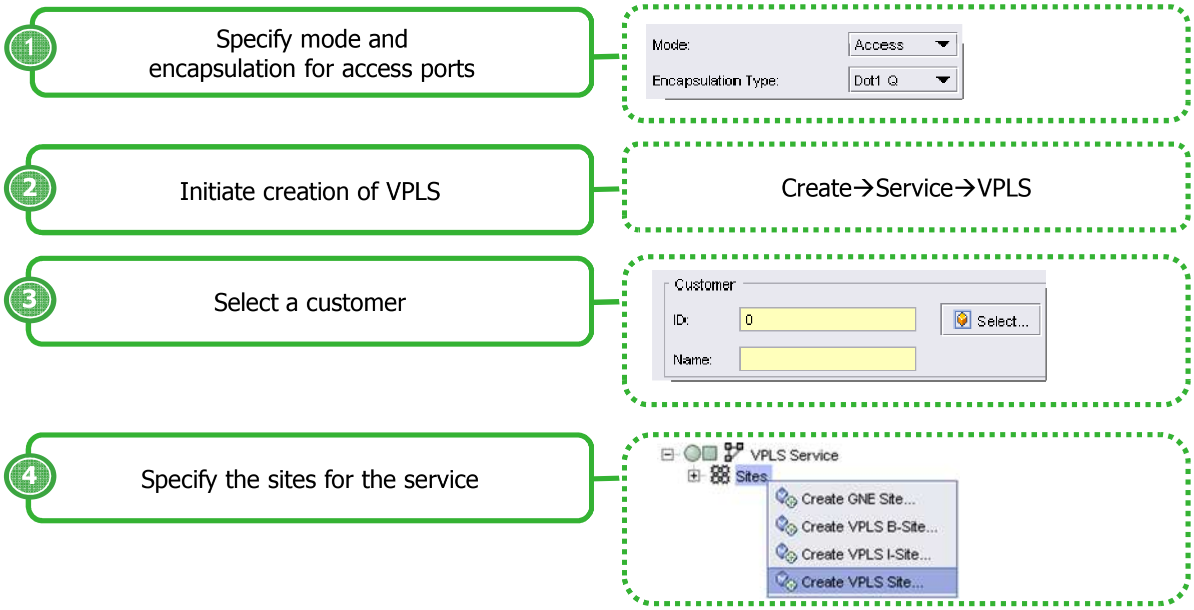
Knowledge Verification – VPLS configuration

You must have configure a customer before configuring a VPLS.

a. True.
b. False.

Choose the correct answer for the knowledge verification question above.

3.9 VPLS configuration workflow



Alcatel·Lucent UNIVERSITY

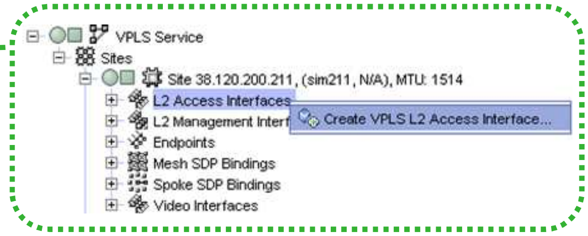
The workflow illustrated above describes the steps for a network administrator or operator to configure a Virtual Private LAN Service.

As a prerequisite for creating a VPLS service, this workflow assumes the following:

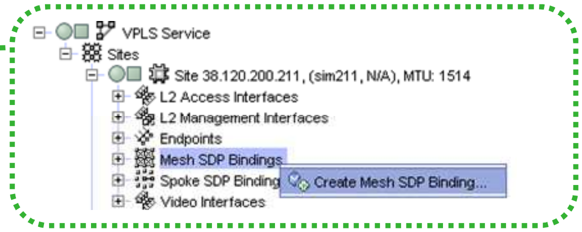
- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured

3.9 VPLS configuration workflow

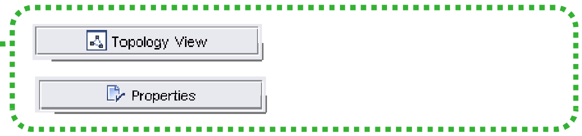
5 Configure the L2 Access Interfaces, including selection of terminating port



6 Configure Mesh SDP bindings, including manual or auto selection of SDP

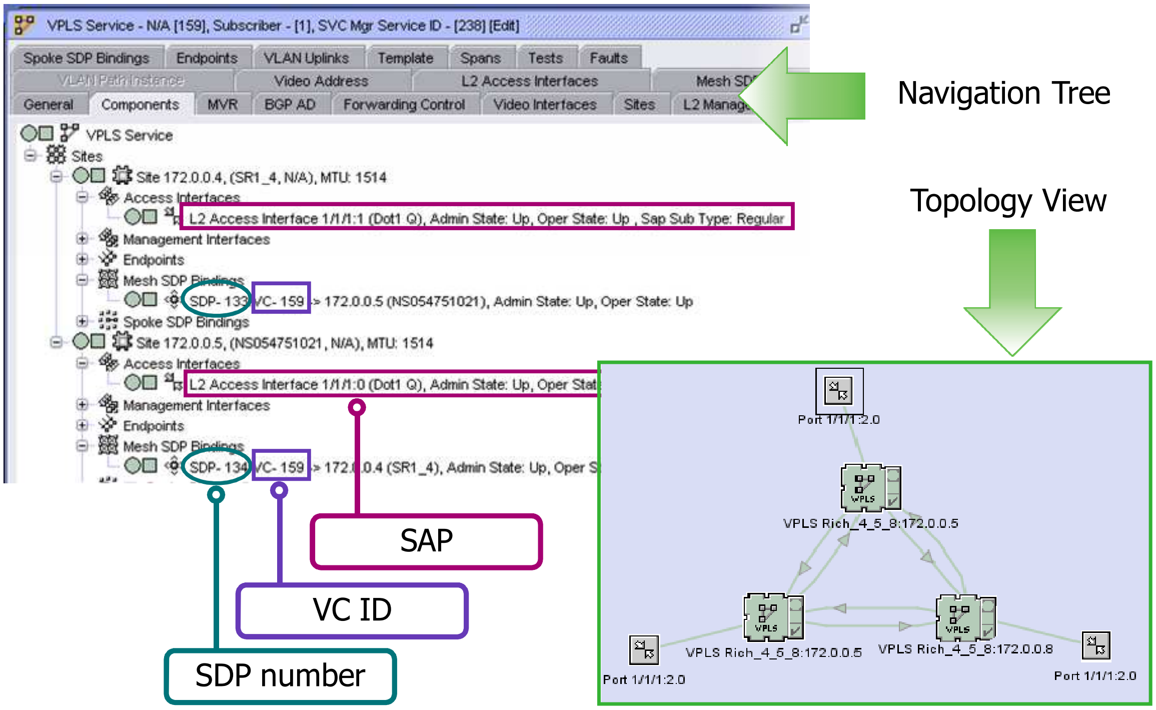


7 Manage Service



Alcatel·Lucent UNIVERSITY

3.10 VPLS SAP and SDP display in the 5620 SAM



Alcatel·Lucent UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VPLS

Lab Exercises
Create a Virtual Private LAN Service (VPLS)

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

End of module
VPLS

Alcatel·Lucent
UNIVERSITY

Section 3
Service Types

Module 2
VLL

TOS36042_V3.0-SG-English-Ed1 Module 3.2 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to:

- Describe the characteristics of the different VLL types
  - Epipe, or Ethernet VLL service
  - Ipipe, or IP interworking VLL service
  - Apipe, or ATM VLL service
  - Cpipe, or circuit emulation VLL service
  - Fpipe, or frame relay VLL service
  - Hpipe, or HDLC service

This page is left blank intentionally

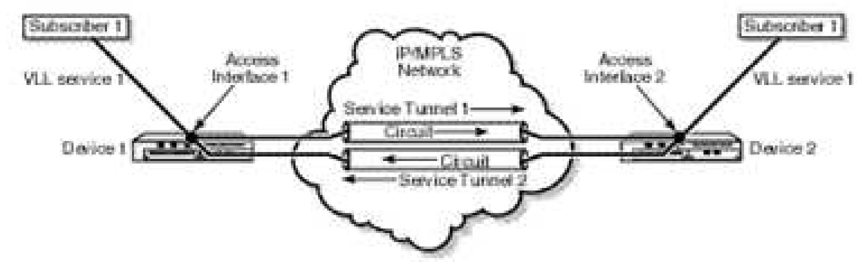
Table of Contents

This page is left blank intentionally

1 VLL overview

1.1 Virtual Leased Line overview

The 5620 SAM supports the provisioning of VLL services on edge devices. A VLL service is an L2 point-to-point service that connects access interfaces. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this, the device performs no MAC learning in a VLL service.



Alcatel·Lucent UNIVERSITY

Packets that arrive at an edge device are associated with a VLL service based on the access interface on which they arrive. An access interface is uniquely identified using these parameters:

- physical port or POS port and channel
- encapsulation type
- encapsulation identifier (if required, depending on encapsulation type)

A VLL service uses T-LDP signaling, and uses MPLS or GRE as the service tunnel transport.

1.2 Local Vs. distributed VLL

Local VLL

- connects access interfaces on one device is called a local VLL service
- no need for signaling between devices = no SDPs

Distributed VLL

- connects access interfaces on two devices
- subscriber or customer data enters a distributed VLL service through access interfaces on different edge devices
- encapsulates the data and transports it across a service provider IP/MPLS network through GRE or MPLS service tunnels

1.4 VLL types

The 5620 SAM supports the creation of the following VLL service types

- **Epipe**, or Ethernet VLL service
- **Ipipe**, or IP interworking VLL service
- **Apipe**, or ATM VLL service
- **Cpipe**, or circuit emulation VLL service
- **Fpipe**, or frame relay VLL service
- **Hpipe**, or HDLC VLL service

Knowledge Verification – Local VLL

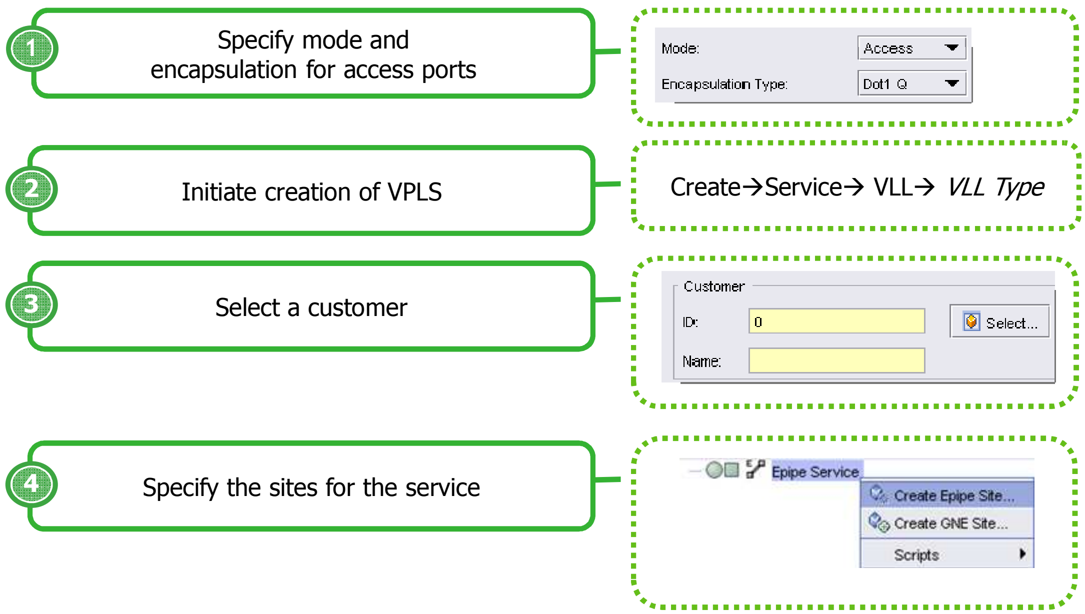
In a local VLL there is no requirement for signaling between devices because there are no SDPs.

a. True.
b. False.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.3 VLL configuration workflow



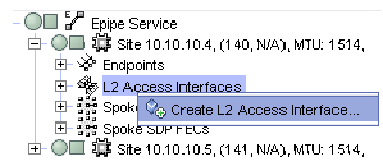
The workflow illustrated above describes the steps for a network administrator or operator to configure a Virtual Leased Line service.

As a prerequisite for creating a VLL service, this workflow assumes the following:

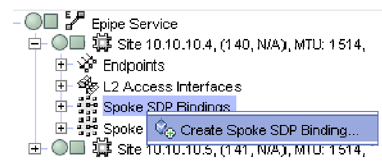
- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured

1.3 VLL configuration workflow [cont.]

5 Configure the L2 Access Interfaces, including selection of terminating port



6 Configure Spoke SDP bindings, including manual or auto selection of SDP



7 Manage Service

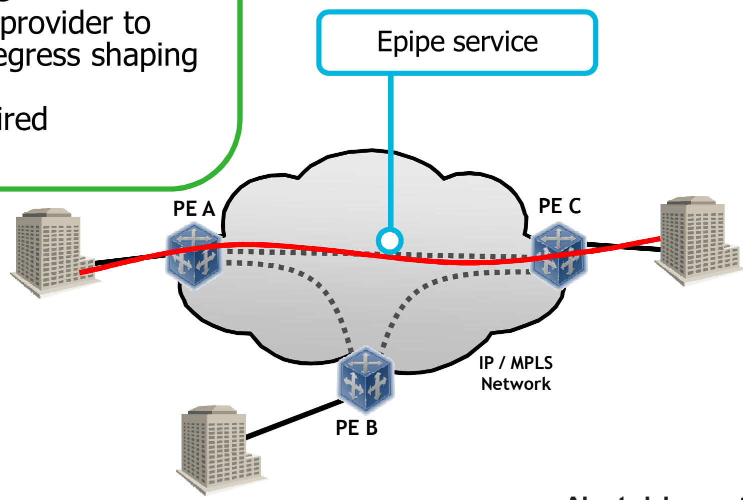
Alcatel·Lucent UNIVERSITY

2 Ethernet VLL service

2.1 Epipe service overview

Epipe

- provides a point to point connection between two nodes
- operates as a leased line between the two locations, from the customer's perspective
- ability for the Service provider to apply billing, ingress/egress shaping and policing
- no MAC learning required



Alcatel·Lucent UNIVERSITY

Characteristics of an Epipe

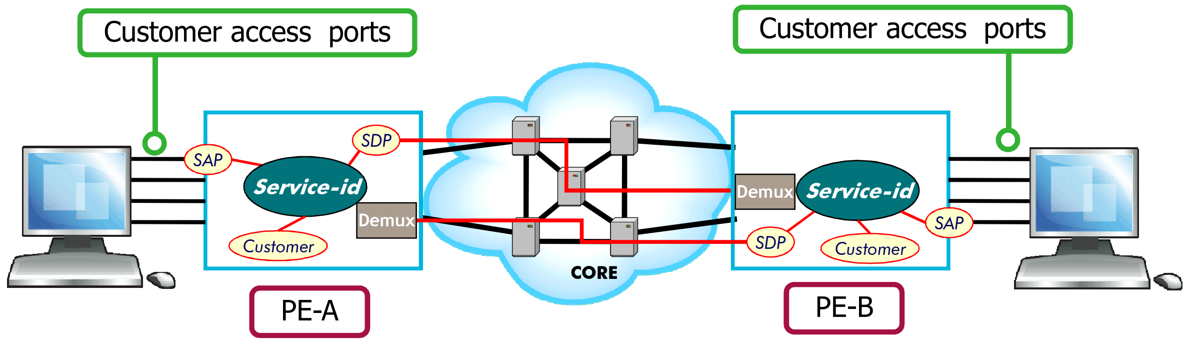
- Point-to-point Ethernet service
- Provides same functionality as a private line/leased line service
- Transparent to higher-layer traffic
- Customer data is encapsulated and transported across an IP/MPLS network
- Does not perform any MAC learning
- Troubleshooting aids such as SDP Ping and Service Ping aid in reducing the complexity of setting up and maintaining the service

2.2 Prerequisites to create an Epipe service

Epipe pre-configuration tasks

- Build the IP core network (cards, ports, interfaces)
- Configure an IGP (routing protocol)
- Configure MPLS LSPs via LDP or RSVP-TE (not needed if GRE tunnels are used)
- Build a mesh of SDPs interconnecting PEs (distributed Epipes, only)
- Create customer accounts
- Create template QoS, scheduler, and accounting policies

2.3 Creating an Epipe Service



Alcatel·Lucent UNIVERSITY

Service-specific tasks Include:

1. Create the service
   - Service type: ePipe
   - Service ID
   - Customer ID

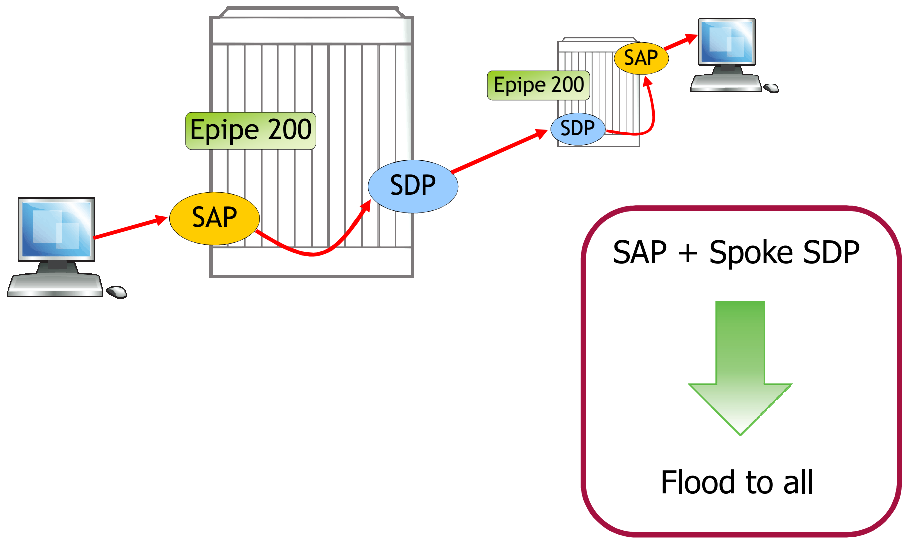
2. Add Service Access Points
   - Select port and encapsulation IDs
   - Select Filter policies (optional)
   - Select Ingress/Egress QOS Policies (optional)
   - Select scheduler policy (optional)
   - Select Accounting Policy (optional)

3. Add Service Distribution Points
   - SDP ID, Virtual Circuit (VC) ID; only needed for a distributed ePipe

When an SDP is bound to an ePipe, it is always done so using the spoke option.

When an SDP is bound to a service, a Virtual Circuit (VC) ID needs to be specified. This is the ID that will be used by TLDP as the FEC (Forwarding Equivalence Class) when it negotiates the service or VC label. The VC ID value configured on one router does not have to be equal to the service ID (although it is good practice), but it does need to match the VC ID value selected on the router located at the far end of the SDP. SDP IDs, however, are allowed to be different.

2.4 SAPs and Spoke-SDPs

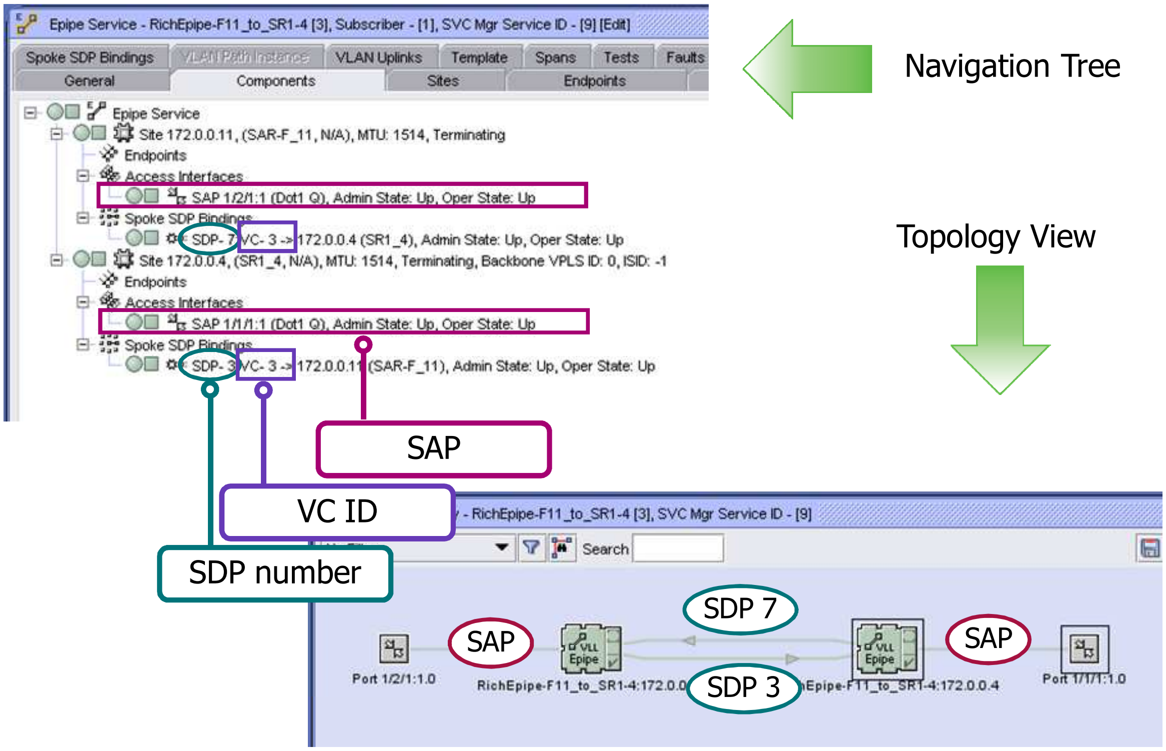


Alcatel·Lucent UNIVERSITY

When flooded traffic is received on a Spoke SDP, the traffic is replicated onto SAPs, other Spoke SDPs, and Mesh SDPs. Similarly, when flooded traffic is received on a SAP it is replicated onto other SAPs, Spoke SDPs, and Mesh SDPs.

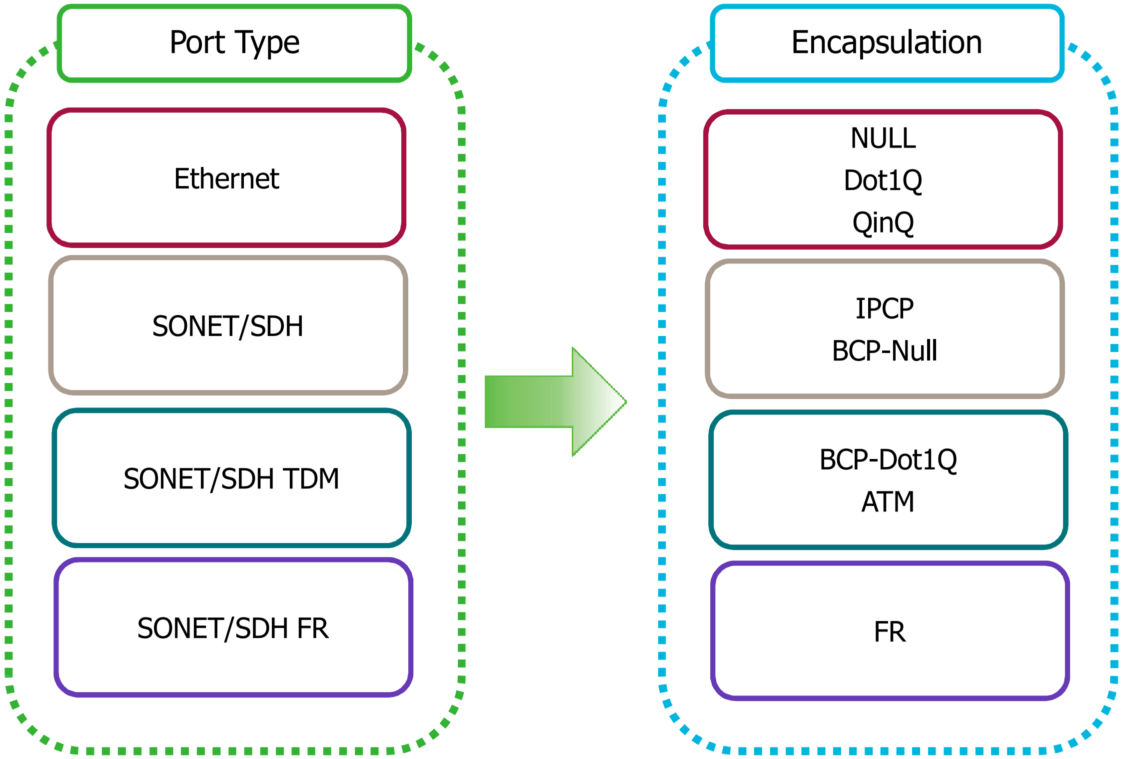
Specifically for an Epipe, since it is a point-to-point service, all traffic received on the Spoke SDP will be forwarded onto the SAP and vice versa.

2.5 Epipe SAP and SDP display in the 5620 SAM



Alcatel·Lucent UNIVERSITY

2.6 SAP Encapsulations for Epipe Services



Alcatel·Lucent
UNIVERSITY

Null – Supports a single service on the port. For example, a single customer edge device attached to the port

Dot1q – Supports multiple services on the port. For example, a customer edge device running Virtual LANs

QinQ – Supports tags within tags

IPCP – Internet Protocol Control Protocol is typically used for interconnection using point-to-point protocol (PPP)

Bridging Control Protocol (BCP-null) is typically used for bridging a single service between two devices using PPP over SONET/SDH with an encap ID of 0

Bridging Control Protocol (BCP-dot1q) supports multiple services on the SONET/SDH port/channel

Knowledge Verification – Epipe SAP encapsulation

What are the SAP encapsulation types supported for Ethernet ports in a VLL Epipe.

a. BCP-Dot1Q and ATM.
b. FR
c. NULL, Dot1Q, and QinQ.
d. IPCP and BCP-Null.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VLL Epipe

Lab Exercises
Create a VLL Epipe

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

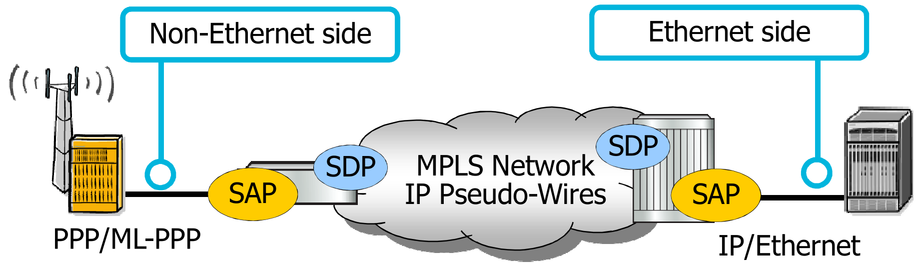
In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

3 IP interworking VLL service

3.1 Ipipe service overview

Ipipe

- Point-to-point Layer 2 service
- Provides IP connectivity between a CE attached to an Ethernet interface and a CE attached to a non-Ethernet interface (e.g. PPP, ATM, FR)
- Requires for both ends to carry IPv4 packets



An Ipipe can provides IP connectivity between a host attached to a point-to-point access circuit (PPP) with routed IPv4 encapsulation and a host attached to an Ethernet interface.

A typical use of this application is in a Layer 2 VPN when upgrading a hub site to Ethernet while keeping the access side with their existing PPP encapsulation.

Supports:

- Ethernet SAP with Null or dot1p encapsulation
- PPP/ML-PPP SAP with IPCP encapsulation
- IP IWF PW: Interworking between IPCP & Ethernet
- Static configuration of CE IP addresses

3.2 Epipe vs. Ipipe

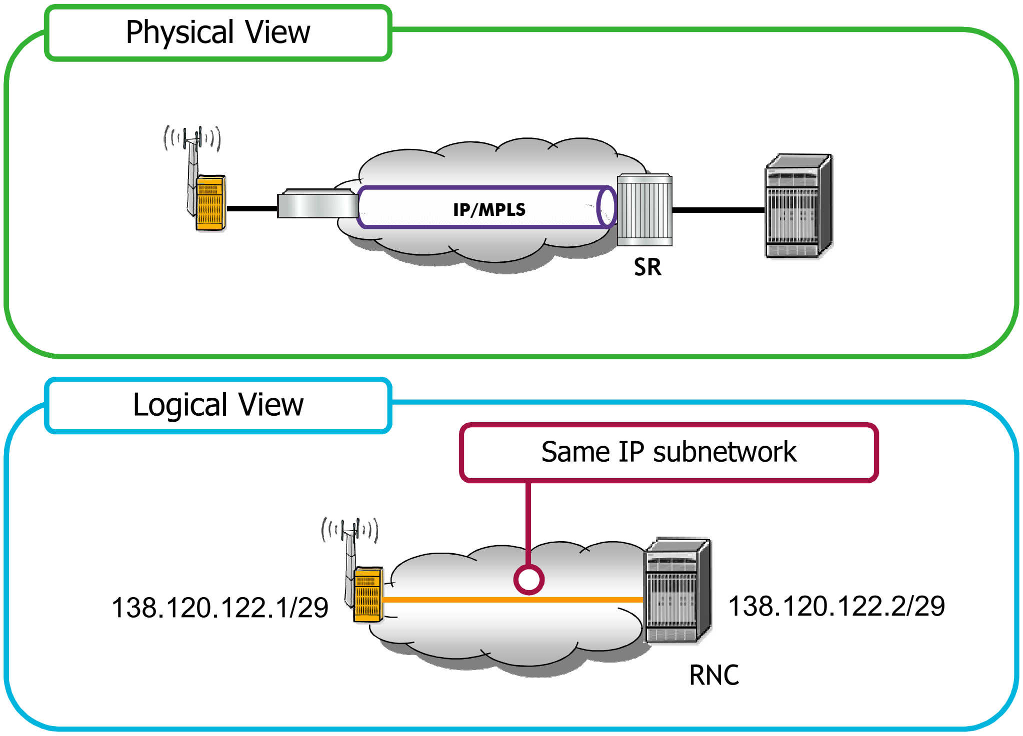
Epipe	Ipipe
Provides Ethernet VPWS	Provides IP interworking VPWS
Supports bridged encapsulation	Supports routed encapsulation
More network overhead because Ethernet header is transported	Less network overhead because Ethernet header is taken out
Both hosts appear to be the same Ethernet LAN	Both hosts appear to be on the same IP subnet or network
No MAC learning	MAC learning
Easier to configure	Local & Remote CE IP address configuration is required

It is worth mentioning that on 7750 SR, Ethernet VPWS Interworking can be used to provide connectivity between Ethernet and ATM/FR sites where **bridged** encapsulation is being used over the ATM/FR links.

Bridged mode encapsulation enables network interworking at layer 2 by allowing the Ethernet frame to be transported across the IP/MPLS intermediary network.

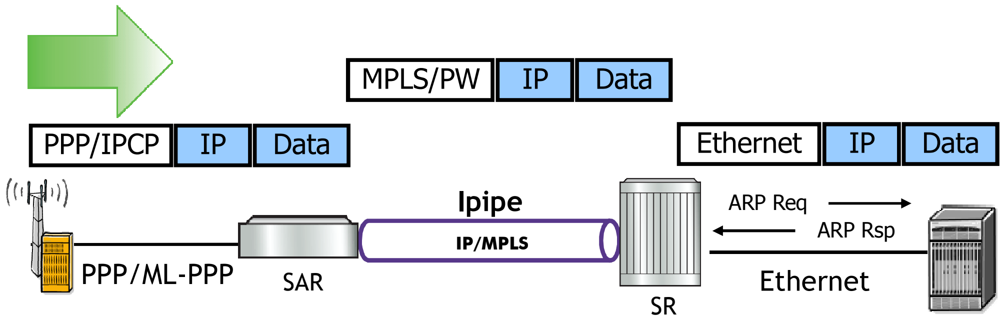
Routed mode encapsulation is used for service interworking between two layer 2 technologies.

3.3 Distributed Ipipe



Alcatel·Lucent UNIVERSITY

3.4 IP packet forwarding: example



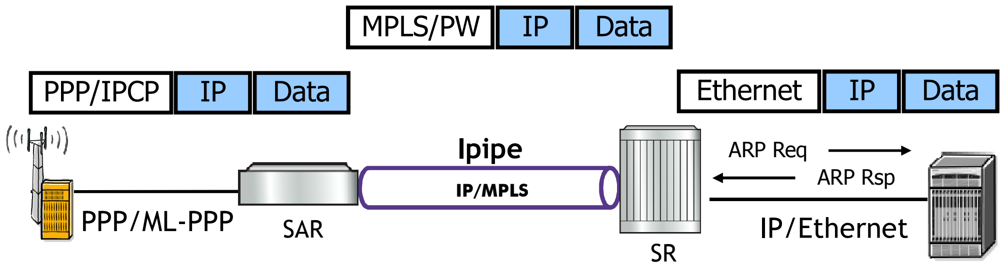
1. The SAR receives an IP packet on the PPP SAP
2. The SAR removes the layer-2 header and encapsulates the IP packet directly into a PW without a control word
3. The SR receives packet and removes the PW encapsulation
4. The SR validates the IP destination address of the received packet and adds Ethernet header before delivering to the local CE.
5. The SR sends an ARP request to determine the MAC address of the local CE.

In this example, there is wireless base station (NodeB) that needs to send data traffic to its Radio Network Controller (RNC). Both will be referred to generically as CE (Customer Edge device). Next to the NodeB there is a Service Access Router (SAR), and next to the RNC there is a more powerful Service Router (SR).

To forward unicast frames destined to the RNC, the SR needs to know the RNC MAC address. When the iPipe SAP is first configured and administratively enabled, the SR sends an ARP request message for the RNC MAC address over the Ethernet SAP.

The SR does not flush the ARP cache unless the SAP goes admin or operationally down. To refresh the ARP cache, the SR sends unsolicited ARP requests.

3.4 IP packet forwarding: example [cont.]

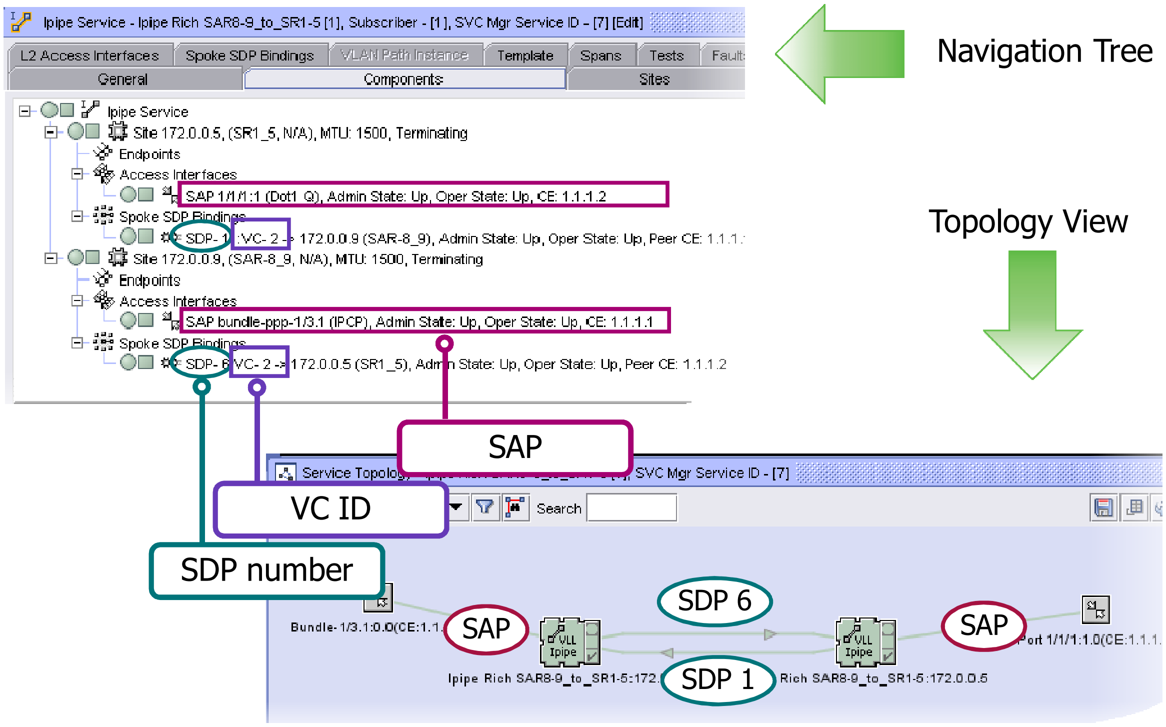


1. In the opposite direction, if MAC address is unknown to the CE it will ARP and the SR responds on behalf of CE on the far end. The SR lends its chassis MAC address pretending to be the far-end CE.
2. The SR receives an IP packet on the Ethernet SAP.
3. The SR removes the layer-2 header and encapsulates the IP packet directly into a PW without a control word.
4. The SAR receives packet and removes the PW encapsulation.
5. The SAR validates the IP destination address of the received packet and adds PPP header before delivering to the local CE.

In the opposite direction, if the MAC address is unknown to the CE (RNC), it will send an ARP Request message. Since the CE on the far end is not running Ethernet, the SR will intercept the ARP request and respond to it on behalf of CE at the far end.

The response transmitted by the SR indicates that the MAC address to be associated to the IP address is its chassis MAC address. In a way, the SR pretends to be the far-end CE so that communication can happen.

3.5 Ipipe SAP and SDP display in the 5620 SAM



Alcatel·Lucent UNIVERSITY

Knowledge Verification – Ipipe characteristics

Which of the following behaviors is not a characteristic of an Ipipe.

a. Provides IP interworking VPWS.
b. Supports routed encapsulation.
c. Both hosts appear to be on the same IP subnet or network
d. No MAC learning.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VLL Ipipe

Lab Exercises
Create a VLL Ipipe

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

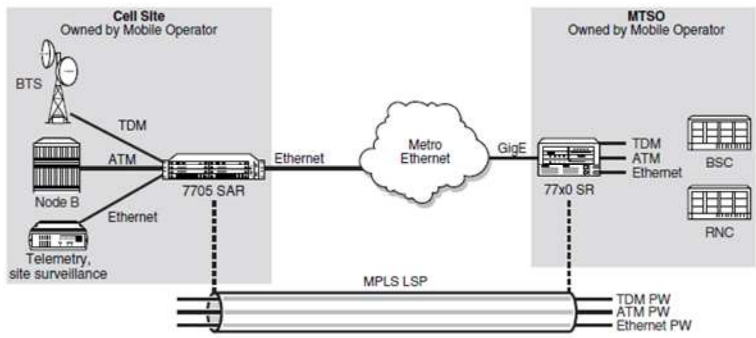
In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

4 ATM VLL service

4.1 Apipe service overview

Apipe

- provides a bi-directional layer 2 connection of ATM service between two users/sites through an IP/MPLS network
- supported on a T1/E1 ASAP port, E3/DS3 port, OC3/STM1 port, or clear-channel or channelized OC3 port when the port is configured for ATM or IMA
- ATM cells received on the ATM SAP are encapsulated into PW packets to be transported over IP/MPLS outer tunnels
- targeted LDP signaling is commonly used to setup the PW



Alcatel·Lucent UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VLL Apipe

Lab Exercises
Create a VLL Apipe service

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

5 Circuit emulation VLL service

5.1 Cpipe service overview

Cpipe

- point-to-point CEM service between users who connect directly to 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7705 SAR, 7710 SR, or 7750 SR devices, or to 7450 ESS devices in an IP/MPLS network
- endpoints of a Cpipe use CEM encapsulation
- Time Slots parameter of the DS0 channel must be configured with at least one time slot
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed

The Cpipe L2 access interface can be bound to a unstructured DS1 or E1 channel, a channelized DS0 channel group, or a DS0 group with CAS signaling.

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VLL Cpipe

Lab Exercises
Create a VLL Cpipe service

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

6 Frame relay VLL service

6.1 Fpipe service overview

Fpipe

- provides a point-to-point frame relay service between users who connect to PE 7750 SR, 7710 SR, or 7450 ESS NEs in an IP/MPLS network
- both endpoints of service use frame relay encapsulation
- connects users through frame relay PVCs
- receives standard Q.922 core frames on the frame relay SAP and encapsulates them in a pseudowire packet according to the 1-to-1 frame relay encapsulation mode
- supports the many-to-one, or port encapsulation mode. supports local cross-connecting when the endpoints are on the same managed device.

7 HDLC VLL service

7.1 Hpipe service overview

Hpipe

- transports HDLC PDUs over an MPLS network
- enables service providers to offer emulated HDLC services over existing MPLS networks
- provides port-to-port transport of HDLC-encapsulated traffic
- HDLC PDU is transported in its entirety, including the HDLC address and control fields, but the HDLC flags and the FCS are excluded
- optional control word is used, the flag bits in the control word are not used and must be set to 0 for transmitting and must be ignored upon receipt.
- mda-mode command must be set to cem-fr-hdlc-ppp at the card level before you can configure the HDLC SAPs
- only ports that are configured with HDLC encapsulation can be mapped to an Hpipe SAP
- HDLC encapsulating ports do not terminate the HDLC — the ports pass the HDLC frames through the Hpipe
- HDLC encapsulated ports can pass through any HDLC-framed traffic, such as Cisco-HDLC, FR, PPP, etc.

Knowledge Verification – Hpipe characteristics

What is the definition of an VLL Hpipe service?

a. Provides a bi-directional layer 2 connection of ATM service between two users/sites through an IP/MPLS network.
b. Point-to-point CEM service between users who connect directly to 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7705 SAR, 7710 SR, or 7750 SR devices, or to 7450 ESS devices in an IP/MPLS network.
c. Provides a point-to-point frame relay service between users who connect to PE 7750 SR, 7710 SR, or 7450 ESS NEs in an IP/MPLS network.
d. Provides port-to-port transport of HDLC-encapsulated traffic.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-02	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

End of module
VLL

Section 3
Service Types

Module 3
IES

TOS36042_V3.0-SG-English-Ed1 Module 3.3 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to:

- Describe the features of an Internet Enhanced Service
- List the steps in configuring an IES

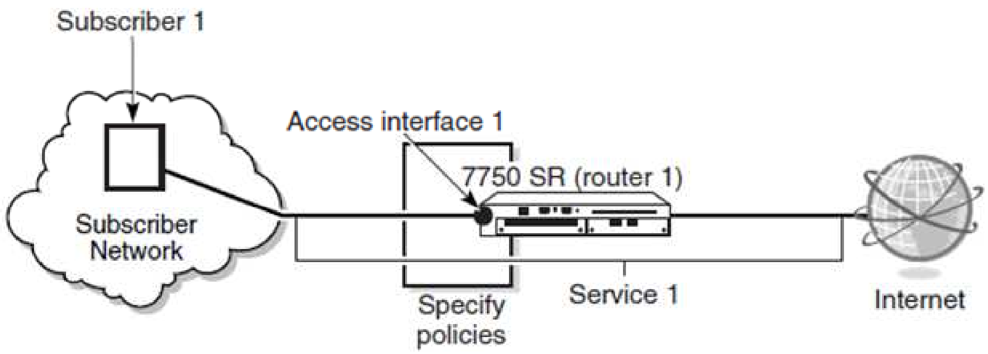
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Internet Enhanced Service (IES)

1.1 IES Overview



- Layer 3 multi-site access using traditional L3 IP routing (Global Route Tables)
- Exchange of IP prefix routing information between customer PE access interfaces established through IRP (Internal Routing Protocol) global routing tables
- IES Access interface prefixes must be unique within the network's global IP addressing scheme
- Since the traffic in an IES service communicates using an IP interface for the core routing instance, there is no need for the concept of tunneling traffic to a remote router. AN IES does not require the configuration of any SDPs

Internet Enhanced Service (IES) is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces each with a SAP which acts as the access point to the subscriber's network . IES allows customer-facing IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and potentially the entire Internet.

While an IES is part of the routing domain, the usable IP address space may be limited. This feature allows a portion of the service provider address space to be reserved for service IP provisioning, and be administered by a separate but subordinate address authority.

IP interfaces defined within the context of an IES service must have a SAP associated as the access point to the subscriber network. Multiple IES services are created to segregate subscriber-owned IP interfaces.

1.2 Support for SAP encapsulation, IP interfaces, and routing protocols

Supported SAP encapsulations

- Ethernet: null, dot1q, and q-in-q
- SONET/SDH: IPCP, BCP-null, and BCP-dot1q

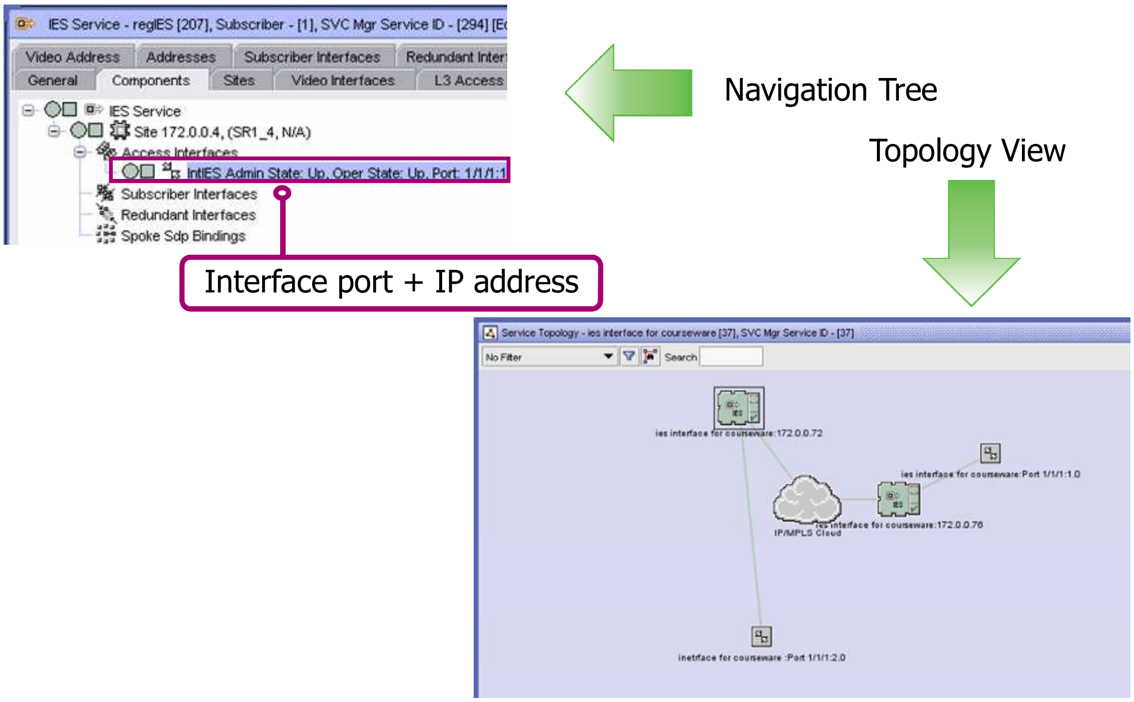
Supported IP interfaces

- Most options found on core IP interfaces
- VRRP – for IES with more than one IP interface
- Secondary IP addresses
- ICMP options

Supported routing protocols

- RIP
- OSPF
- IS-IS

1.3 IES SAP display in the 5620 SAM



Alcatel·Lucent UNIVERSITY

Knowledge Verification – Routing protocols for IES

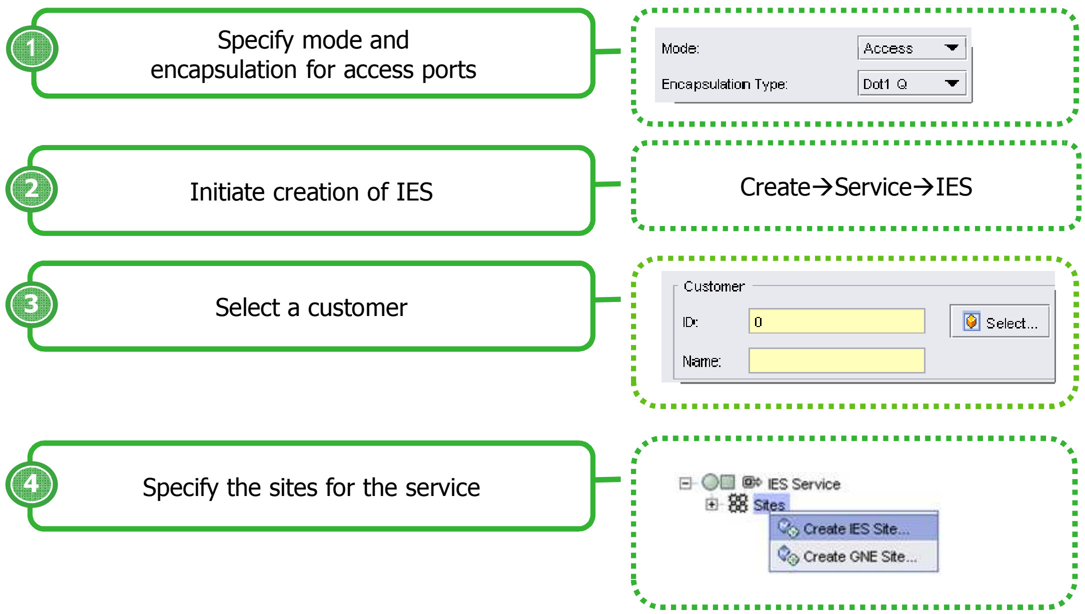
An IES supports the following routing protocols.

a. RIP, OSPF, and IS-IS.
b. BGP, RIP, and LDP.
c. LDP, IS-IS, and OSPF.
d. OSPF, RSVP, and L2TP.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.4 IES configuration workflow



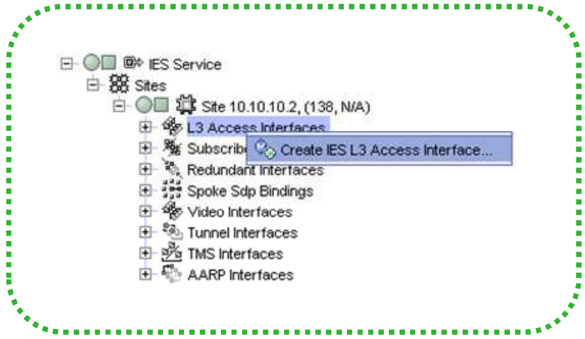
The workflow illustrated above describes the steps for a network administrator or operator to configure a Internet Enhanced Service.

As a prerequisite for creating a IES service, this workflow assumes the following:

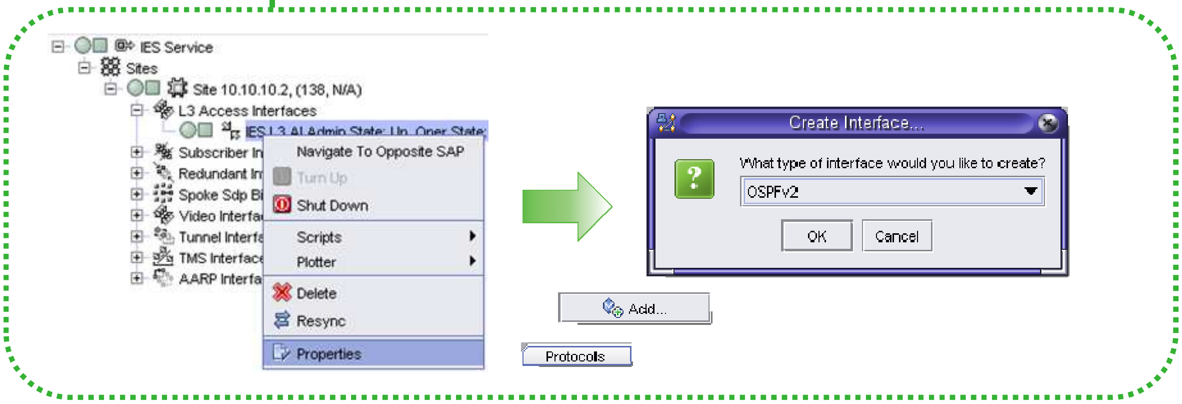
- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured

1.4 IES configuration workflow [cont.]

5 Configure the L3 Access Interfaces



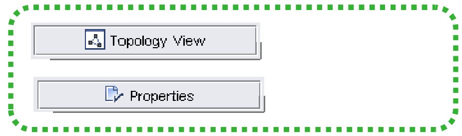
6 Create OSPF interface



Alcatel·Lucent
UNIVERSITY

1.4 IES configuration workflow [cont.]

7 Manage Service



Alcatel·Lucent
UNIVERSITY

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of an IES

Lab Exercises
Create an IES service

Time allowed: 15 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

End of module
IES

Alcatel·Lucent
UNIVERSITY

Section 3
Service Types

Module 4
VPRN

TOS36042_V3.0-SG-English-Ed1 Module 3.4 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to:

- Identify the need for L3 VPNs
- Describe the characteristics of a L3 VPN
- Explain Packet Walkthrough
- List the steps in configuring a VPRN

This page is left blank intentionally

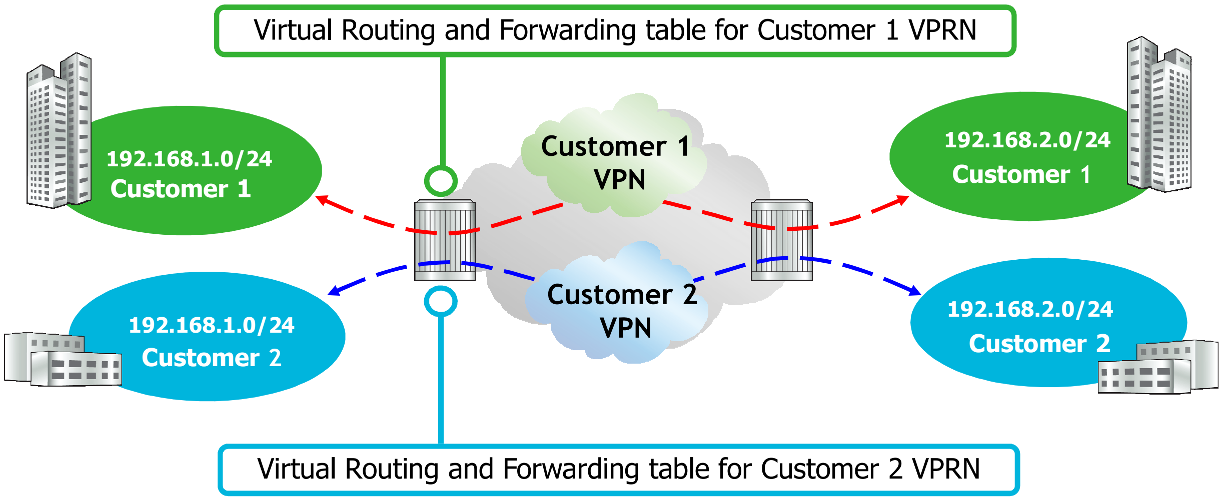
Table of Contents

This page is left blank intentionally

1 Virtual Private Routed Networks

1.1 Virtual Private Routed Networks overview

VPRN services use Virtual Routing and Forwarding tables (VRF) within a PE device to maintain forwarding information on a per site basis. A VRF is a logical private forwarding table created within a PE router.



3 · 4 · 8
Service Types · VPRN
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

RFC2547bis is an extension to the original RFC 2547, which 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 VPN label/ MPLS label for that route. On the SR Series, 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 VPN/ 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 or GRE tunnel header, so that it gets tunneled across the backbone to the proper PE router. Each route exchanged by the MP-BGP protocol includes a route distinguisher (RD), which identifies the VPRN association. Thus the backbone core routers do not need to know the VPN routes.

1.1 Virtual Private Routed Networks overview [cont.]

Challenge

- Duplicate subnets are mixed together in a single PE Routing table
- Only the best route is selected in routing table
- Large amount of information may be exchanged when routing changes

Solution

- Isolation of different VPN traffic
- Connectivity between customer sites
- Use of private address spaces in each site

Without the L3 VPN:

- Each customer must use a separate IP address range
- All customer routes are carried natively in the provider core
- Large amount of information may be exchanged when routing changes

With VPRN:

- Each PE router maintains a separate logical routing table for each VPRN
- This table is referred to as a Virtual Routing and Forwarding Table (VRF)
  - May maintain multiple VRFs depending on the number of customers connected
- Contains customer destination routes
  - local sites
  - remote sites
- MP-BGP is used to carry the VPN routes

1.2 Basic Requirements

Customer Perspective

- Customer can choose their IP addressing scheme
- Private addresses and overlapping addresses
- Transparency; for example, customer equipment is unaware of VPN
- Security; for example, separation of routing information and data among customers
- QoS as defined in an SLA
- Different sites may use different layer-2 access technologies

Provider Perspective

- Scalability of backbone network (signalling, and state)
- Scalability of the number of VPNs/backbone, sites/VPN, and routes/VPN
- Ease of provisioning; for example, addition of a site to a VPN, creation of a new VPN, merging of VPNs

Knowledge Verification – VPRN definition

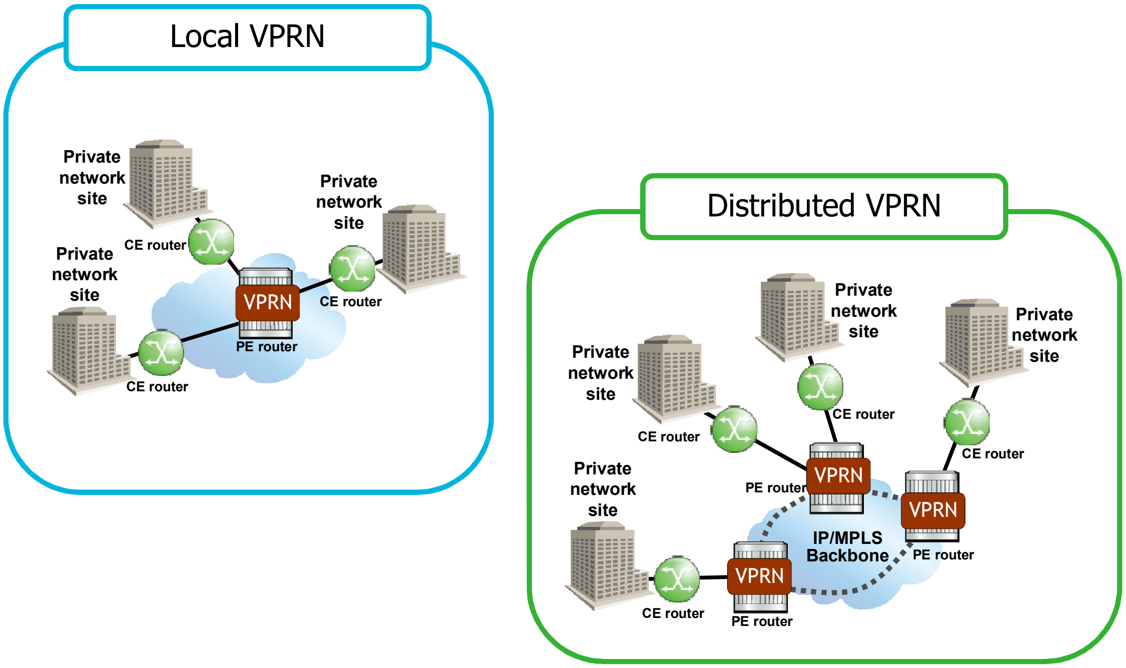
What is the best definition of Virtual Private Routed Network.

a. A type of VPN where IP is transported in a point-to-point manner. CPE devices are connected through nodes, and the nodes are connected to an IP tunnel.
b. A host communicates with an IP router interface to send and receive Internet traffic.
c. A network exhibiting at least some of the characteristics of a private network, even though it uses the resources of a public switched network.
d. A type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. The services may be from different locations, but appear to be on the same LAN.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.3 Local Vs. distributed VPRN



Alcatel·Lucent UNIVERSITY

A VPRN can be **local** (only one PE provides the service) or **distributed** (two or more PEs collaborate to provide the service)

In a **distributed** VPRN, each PE needs to:

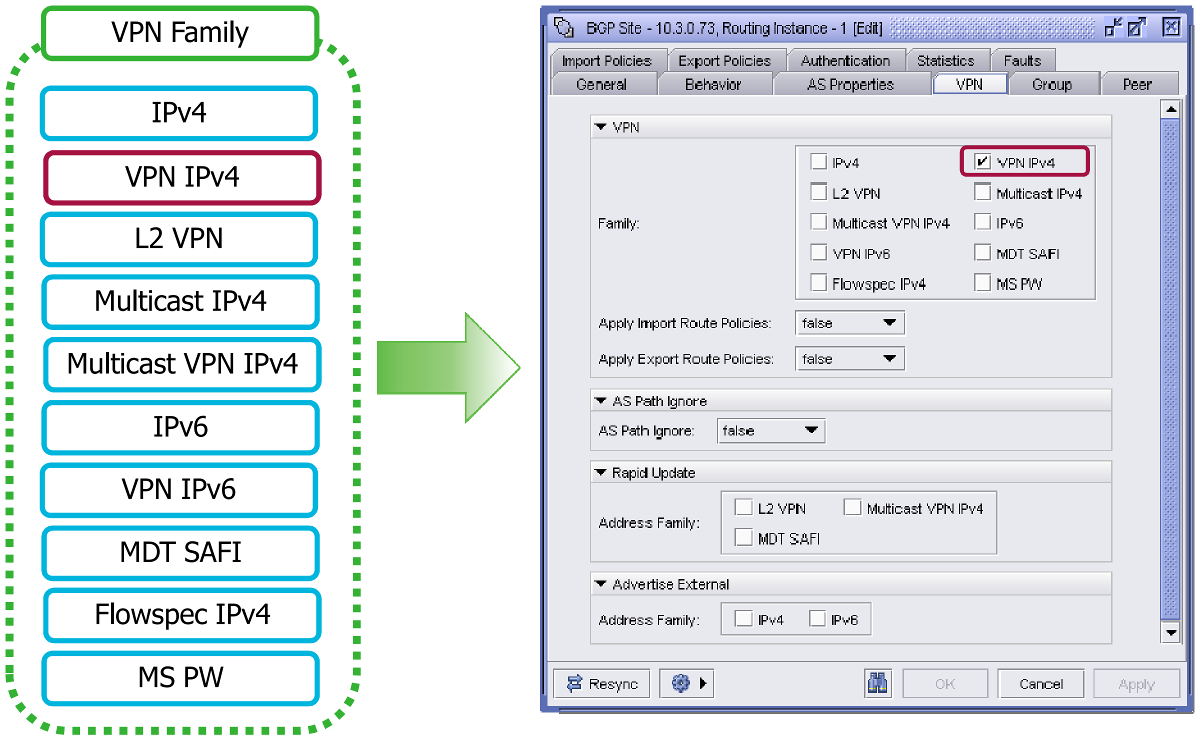
- establish **MP-BGP** sessions with the other PEs to exchange routing information residing in their respective VRFs
- create **SDPs** towards the other PEs to carry the customer data

In a **local** VPRN, however, there is no requirement for the following configuration:

- to run **MP-BGP** or
- to create **SDPs**

In a local service, the PE may still need to run BGP (not MP-BGP) on one or more VPRN interfaces if that is the protocol that the PE and the CE agree to use to exchange local routing information relative to the specific location where the subscriber is situated.

1.4 VPN IPv4

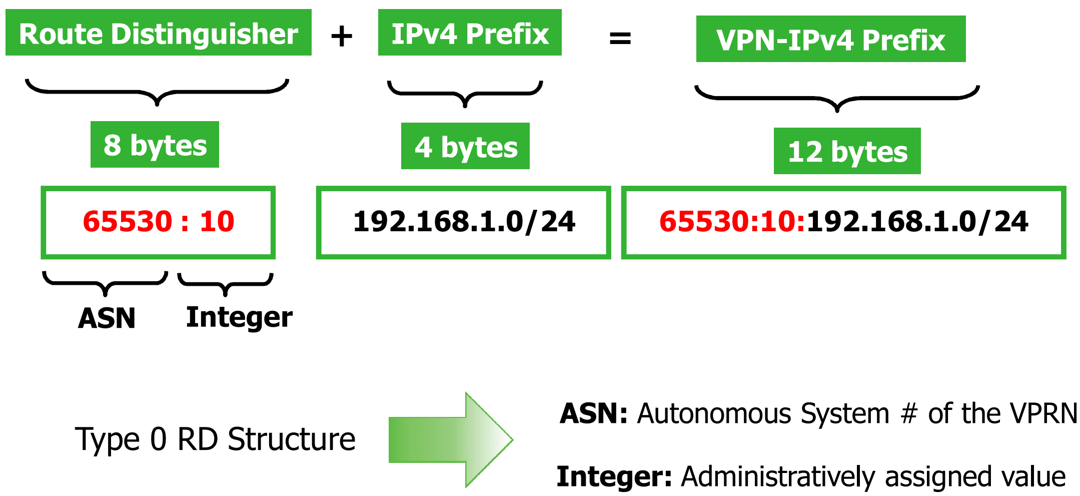


Alcatel·Lucent
UNIVERSITY

- Isolation of overlapping IP addressing schemes is achieved using VPN-Internet Protocol version 4 (IPv4) address family
- The BGP address family VPN-IPv4 is an extension to the BGP protocol
- In VPN-IPv4 addressing, a route distinguisher is prefixed to the private IPv4 address uniquely identifying the private IPv4 address, even if that address is used in another customer’s network
- The capability of transporting VPN-IPv4 routes comes along with the support for Multiprotocol Extensions for BGP-4.
- By default, BGP-4 can handle only the native IPv4 routes. To enable the transport of different address families such as VPN-IPv4, Multicast-IPv4 and IPv6, explicit configuration has to be made under the global BGP context.
- SAR>configure router bgp family ipv4 vpn-ipv4
- The Route Distinguisher (RD) is needed to make the VPN routes unique. This is necessary because all VPN routes are carried in the same routing protocol (MP-BGP).
- Different customers may use the same IP addresses within their respective networks. A method is needed to ensure that the IP addresses remain unique when they are distributed across the service provider network. This is achieved by pre-pending the 4-byte IPv4 address with an 8-byte Route Distinguisher to form a new address called the “VPN-IPv4 address”.
- All routes that are originating from a certain VRF on a particular PE have the same and only one RD value associated with them.

1.5 Route Distinguisher

An identifier called the Route Distinguisher (RD) is added to all IPv4 prefixes in order to be able to represent them as unique entities inside the BGP RIB.



Alcatel·Lucent UNIVERSITY

Both Type 0 and Type 1 RD formats are supported on the 7x50. The common convention is Type 0, where the first part of the RD (before the colon) is represented by the AS (Autonomous System) number of the VPRN and the second part (after the colon) is an administratively defined and managed integer.

The RD value associated with the VRFs belonging to the same customer on different PE's may be chosen to be the same or different depending on design requirements.

Both register and private AS numbers can be used, depending on the requirements at customer side.

1.6 Route Target

Route Target Characteristics

- Another identifier called the Route Target (RT) is used to distribute the routes in between the VRFs dispersed over several PEs
- While exporting a particular route from a VRF, one or more Export Route Target(s) are associated with that route
- A particular route originating from a VRF on a certain PE can have only one Route Distinguisher value, but it can have multiple Route Target values
- Route Targets are part of the Extended Community Attributes inside the BGP Updates and can be used in Route Policies
- On the receiving PE, if the Import RT value matches the RT field of an incoming BGP Update, then the associated prefix is populated (imported) into the appropriate VRF
- In a simplistic full-mesh VPRN topology, all the import and export Route Targets associated with the VRFs belonging to the same customer on all PEs are typically set to the same value

The same set of PE routers may need to exchange routes corresponding to different VPRN service instances. In addition to that, to improve scalability PE routers establish a single MP-BGP session for the VPN-IPv4 family of prefixes.

Some mechanism is needed to determine to which VRF a route belongs. A Route Target was defined to address this issue. The Route Target (RT) is the closest approximation to a VPN membership identifier in the VPRN architecture, and identifies to the receiving PE the VRF table that a prefix is associated with.

Route Target is a MP-BGP extended community. One or more MP-BGP community attributes may be associated to any route, therefore one or more Route Targets may be associated to any route.

In simple VPN cases and for provisioning consistency, the Route Target value chosen is often the same as the Route Distinguisher value, however they should not be interpreted as meaning the same thing.

1.7 Route Distinguisher Vs. Route Target

Characteristic	Route Target (RT)	Route Distinguisher (RD)
Part of VPN-IPv4 prefix	N	Y
Part of BGP attributes	Y	N
Makes a route unique	N	Y
Unique per VRF /VPRN	N	N
Unique per VRF/VPRN per node	N	Y
Only one per VPNv4 route	N	Y
Can be used in policies	Y	N

Alcatel·Lucent
UNIVERSITY

The route-target is part of the BGP attributes, whereas the route-distinguisher is part of the prefix, also known as Network Layer Reachability Information (NLRI).

RD + subnet/mask makes the NLRI unique. Route-targets can be used by multiple VRFs and thus do not make the NLRIs unique.

One VRF, spread over multiple PEs, can make use of more than one RD and more then one RT. VRF A on PE-1 can have a different RT and RD compared to VRF A on a different PE (PE-B).

On a PE, a single VRF/VPRN can only assign one RD, but it is possible to use more then one RT.

One VPNv4 route, has only one RD, as part of the NLRI, but can have more then one RT (multiple extended communities can be sent with one NLRI).

Routing policies can check (match) on extended communities and/or add communities as a result of a match condition. RDs can not be used in policies.

Knowledge Verification – Local Vs. Distributed VPRN

You must establish MP-BGP sessions and create SDPs as part of the configuration process for a VPRN.

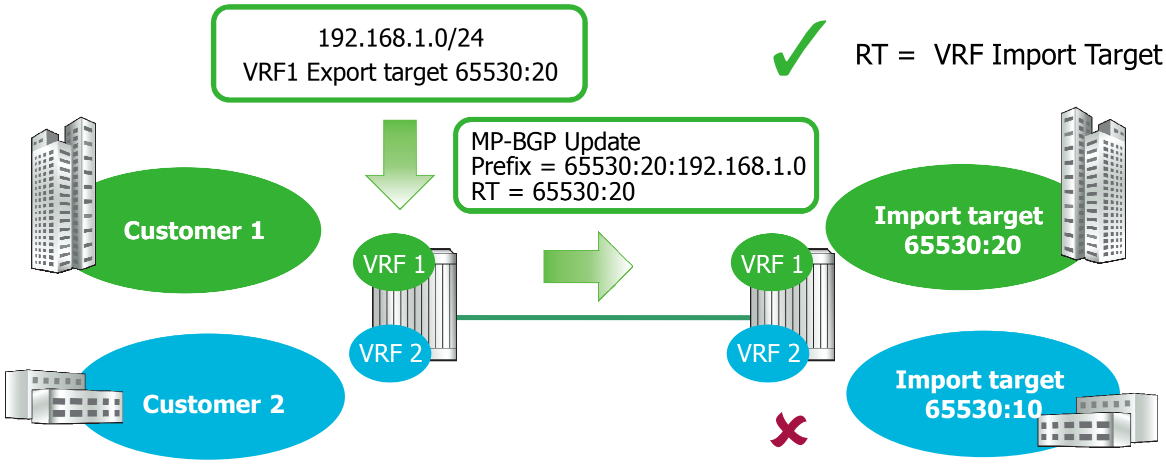
a. True.
b. False.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.8 Import/Export Policy

Routes are tagged with one or more RTs. Routes are carried as VPN-IPv4 routes using MP-BGP to the remote PE



Alcatel·Lucent UNIVERSITY

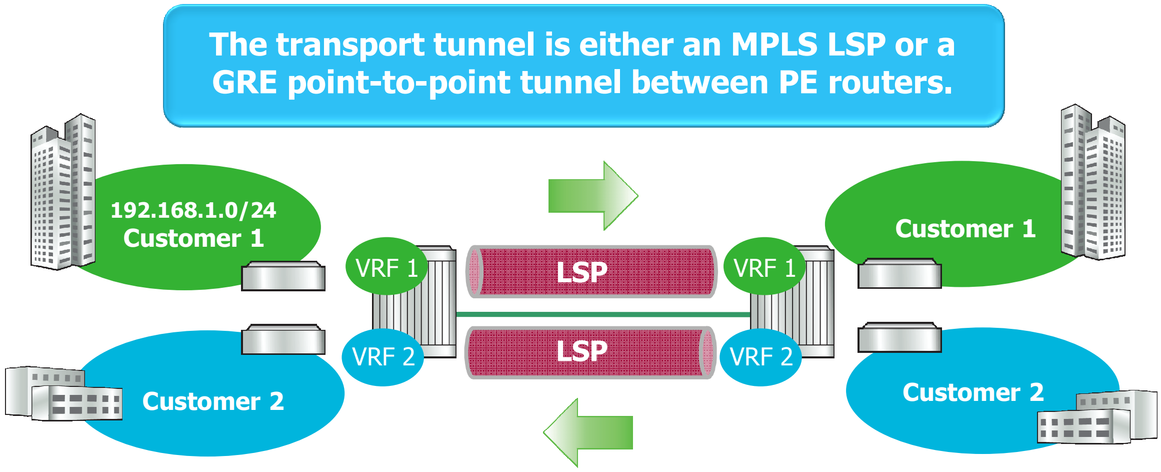
Routes are tagged with a route target value before sharing them with remote PEs due to the VPRN configuration (vrf-target parameter). Alternatively, export policies can be defined to add route target values (community attribute) to a route advertised to remote PEs. Upon receipt of a VPN-IPv4 route, a PE router will by default add the route to the VRF associated to the route target value received with the route. Import policies can be used to decide whether to add a given route to a VRF.

Route isolation between VRFs is accomplished through careful policy administration. An administrator determines the appropriate export and import target relationships.

Since RTs are applied at the time the route is exported, they are called export-RT. In the above example, a single RT is attached to each route.

The decision to import the route into the VRF is done by matching the received routes against locally defined per-VRF import policies expressed in terms of RTs (import-RT). If the Router import RT matches the update RT, it is stripped of the RD and imported into the VRF.

1.9 Data Plane – Transport Tunnel



Alcatel·Lucent UNIVERSITY

After the establishment of the routing topology in the provider core, a full mesh of transport tunnels must be created between the PE's. In other words, each PE involved in a given VPRN service must be configured with a tunnel to every other PE participating in the same VPRN service in order to transport a customer's VPN traffic from one site to another. The transport tunnel is either an MPLS LSP or a GRE point-to-point tunnel between PE's.

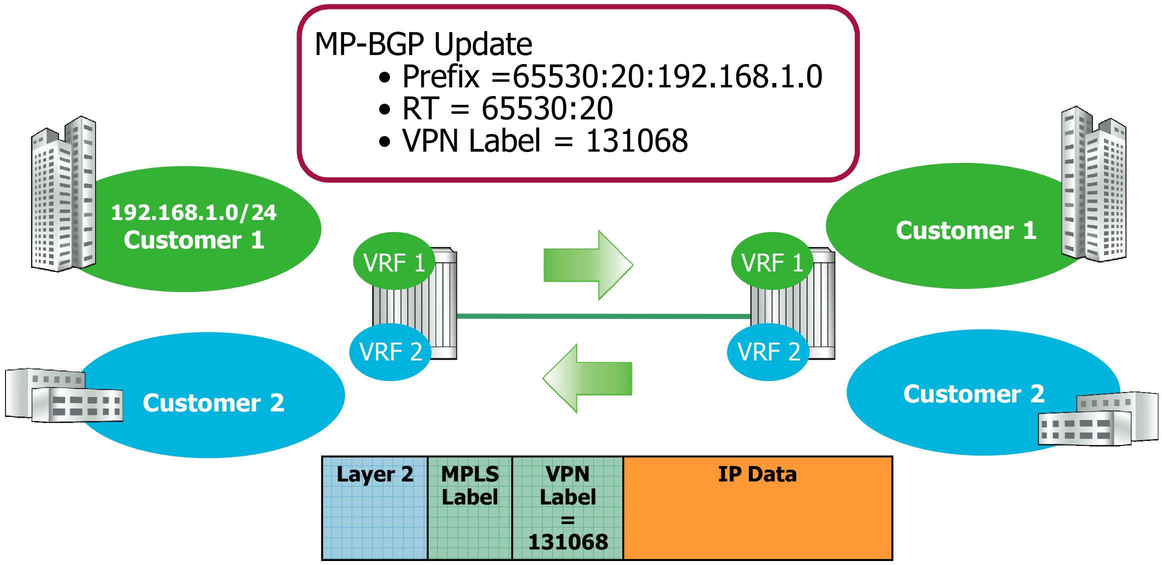
The tunnels serve as the label switched paths the customer packets will take as they cross the provider core network.

The tunnel is created either through the configuration of an SDP that is bound to the service or using the auto-bind option when creating a VPRN service instance. The auto-bind option is possible for VPRN, and not for the other service types, because in this case an MP-BGP session is established between every pair of PE routers that participate in the service in order for them to exchange routing information (VPN prefixes). So, its peers have been identified. Therefore, when the auto-bind command is issued, SDPs are automatically created from the router to each of the other routers with which there exists an MP-BGP session for the VPN family of prefixes.

If SDP tunnels are used, they must be created prior to the creation of the VPRN services.

1.10 VPN Label

The purpose of the VPN label is to demultiplex VPN traffic arriving at the PE.



Alcatel·Lucent UNIVERSITY

VPN label characteristics:

- The purpose of the VPN label is to demultiplex VPN traffic arriving at the PE.
- The distribution of the VPN label is done using BGP along with the VPN route information.
- The distribution of the VPN tunnel information is automatic and does not require manual intervention.
- The forwarding at the egress PE is based on:
  - an MPLS lookup on the VPN label to determine the appropriate VRF
  - followed by an IP lookup in that VRF.

VPN label workflow:

1. Associate a VPN label with a VPN route at the ingress PE.
2. Demux the traffic based on VPN label at egress PE.
3. Distribute the VPN label with VPN Route information (MP-BGP).

Knowledge Verification – VPN label function

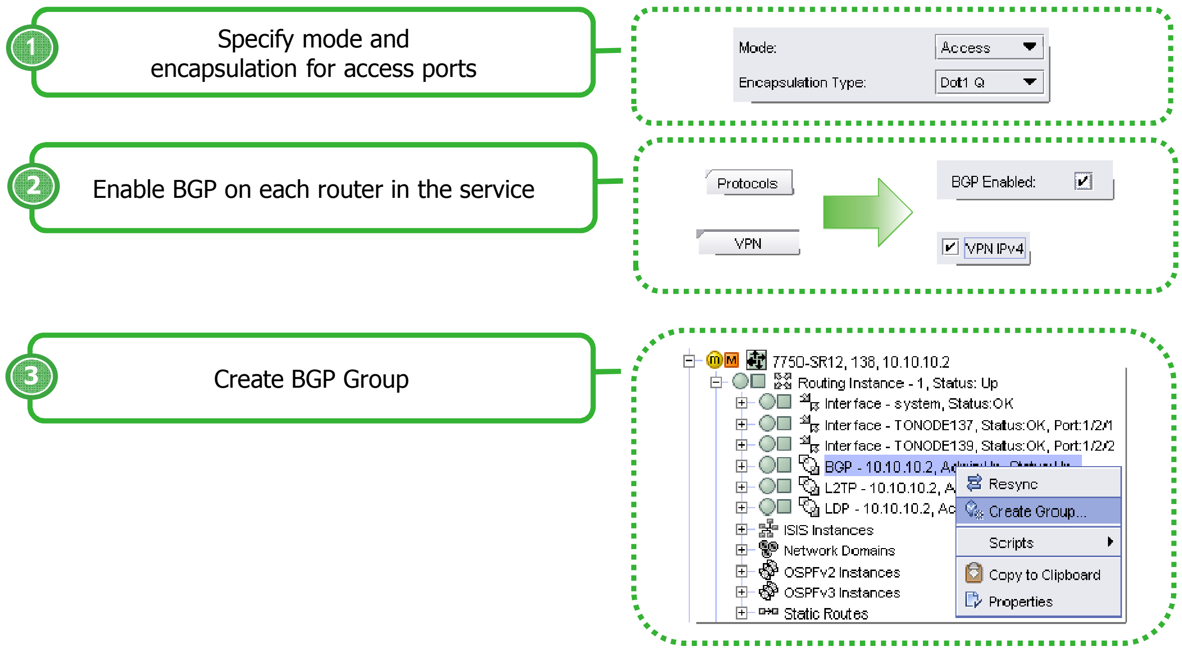
The purpose of the VPN label is to demultiplex VPN traffic arriving at the PE.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.11 VPRN configuration workflow



Alcatel·Lucent UNIVERSITY

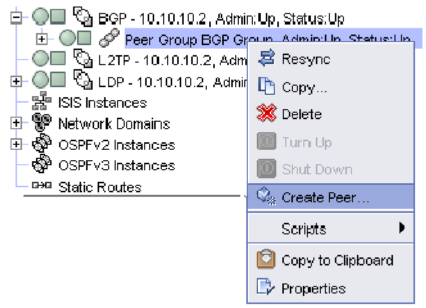
The workflow illustrated above describes the steps for a network administrator or operator to configure a VPRN Service.

As a prerequisite for creating a VPLS service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured

1.11 VPRN configuration workflow [cont.]

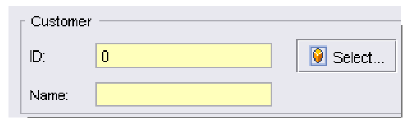
4 Create BGP peers



5 Initiate the creation of the VPRN service

Create→Service→VPRN

6 Select a customer



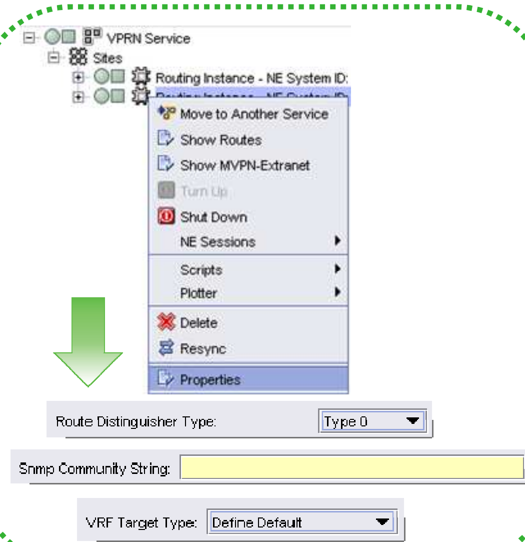
Alcatel·Lucent UNIVERSITY

1.11 VPRN configuration workflow [cont.]

7 Specify the sites for the service

8 Configure the route distinguisher/target, binding, and SNMP Community for each site

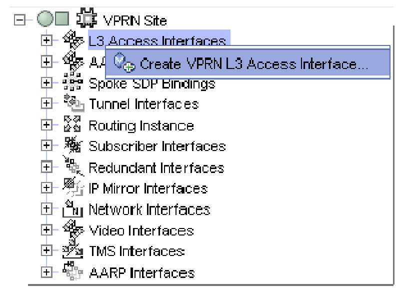
9 Configure the route target



Alcatel·Lucent UNIVERSITY

1.11 VPRN configuration workflow [cont.]

10 Configure the L3 Access Interfaces



11 Manage Service

Alcatel·Lucent UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a VPRN

Lab Exercises
Create a VPRN service

Time allowed: 20 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

This page is left blank intentionally

End of module
VPRN

Section 3
Service Types

Module 5
Composite

TOS36042_V3.0-SG-English-Ed1 Module 3.5 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you will be able to:

- Define the function of a composite service
- List the components of a composite service
- Describe the connection types and where they are used

This page is left blank intentionally

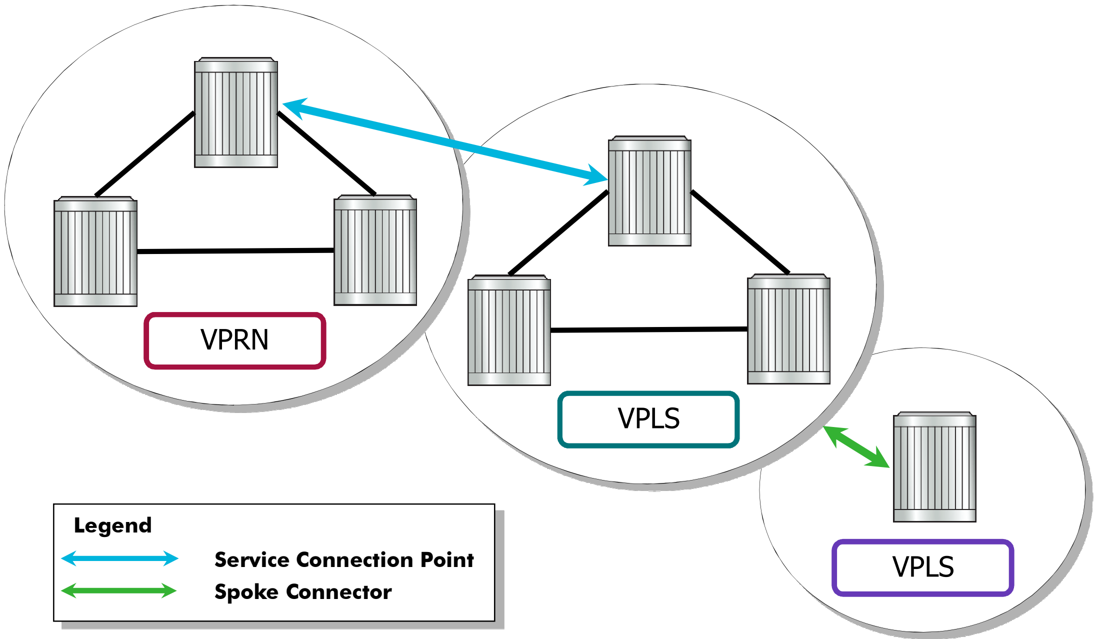
Table of Contents

This page is left blank intentionally

1 Composite Services

1.1 Composite Services Overview

A composite service is a 5620 SAM concept links multiple services and service types using Service Connectors



Alcatel·Lucent UNIVERSITY

A composite service is a set of linked services whose function supports complex applications that require a combination of services, such as VLAN connections to an HVPLS, an IES spoke into a VPLS, or a VPRN-to-VPLS interconnection.

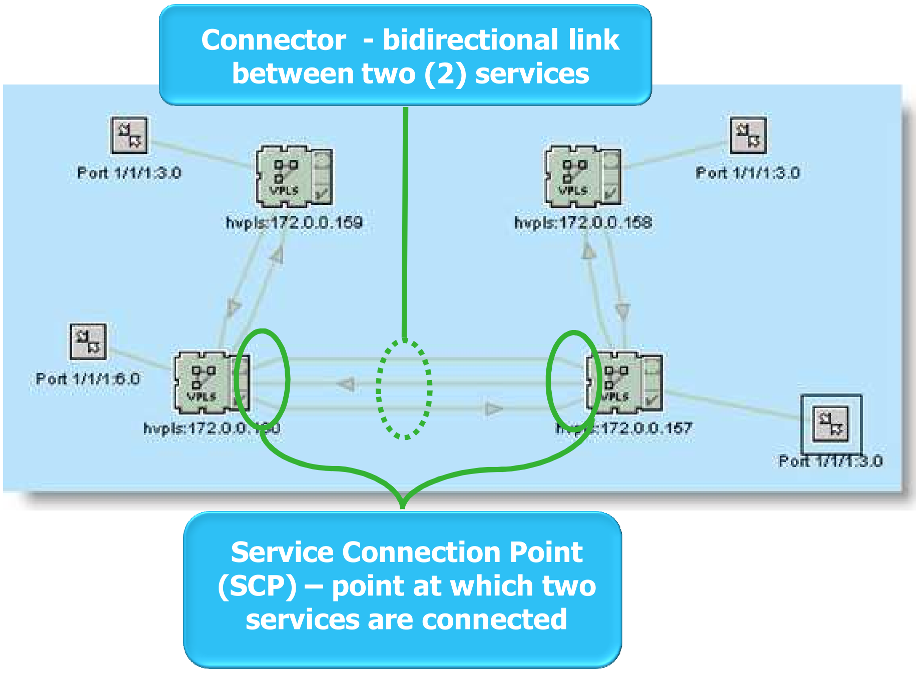
Composite services exist only in the context of the 5620 SAM and are configured through the 5620 SAM GUI or an OSS application. They are unknown to individual network devices.

Composite services consist of customer services, called Service Components (SC) in the context of a composite service, and connectors. In the example above, the SCs are represented by the individual VPRN, VPLS and VLL services. A connector is a bidirectional logical link between two SCs, such as a pair of PW spokes that carry traffic in opposite directions between VLL and VPLS instances, a dot1Q-encapsulated link between a VLAN and a VPLS, or an internal cross-connect.

The term SCP describes a type of connector endpoint. In the case of the services that are available on the 7450 ESS, 7710 SR, or the 7750 SR, an SCP is a service interface or SAP. For L2 switches, such as the 7250 SAS or Telco, an SCP may be a network interface, such as an uplink port.

Services that are owned by different customers can be connected to form a composite service. An example is an HVPLS in which the core VPLS belongs to one customer and the satellite VPLS instances belong to other customers.

1.2 Connector and Connection Point



Alcatel·Lucent UNIVERSITY

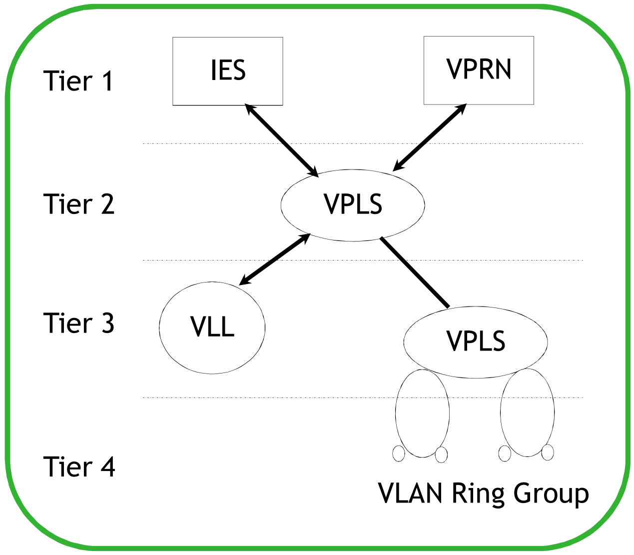
A **Connector** is a bidirectional logical link that exists between to SCs. In the diagram above, the connectors are represented by two spoke SDPs between two VPLS SCs, thus forming a HVPLS (Hierarchical VPLS). The third line (at the top) is the logical representation of the SC itself, the details of which will be discussed later in this course.

The **Service Connection Point**, or **SCP**, describes a type of connector endpoint. In the case of services available on the 7750SR, 7710SR or 7450ESS, an SCP is a service interface or SAP. For L2 switches, such as the 7250 or Telco T5C, an SCP may be a network interface, such as an uplink port.

1.3 Service Tier

A service tier Defines order of traffic flow through SCs within composite service

Service type	Default tier
IES, VPRN	1
VPLS, MVPLS	2
VLL	3
VLAN	4



Alcatel·Lucent UNIVERSITY

Each SC is considered to be at a certain tier, or level, depending upon its proximity to the core of the composite service. This determines the order for traffic flow within the composite service. Traffic flows from lower levels (Tier 4) to higher levels (Tier 1) within the composite service. The chart above lists the default Tier assignment for each of the service types.

Using the diagram above, assume that a subscriber with access to on of the VLAN Ring Groups requests information from a server that is connected to the composite service through the IES service. The request starts at the Tier 4 service (VLAN Ring Group), to the associated VPLS (Tier 3) to the next VPLS (Tier 2) and out the IES (Tier 1). The response will flow in the reverse order (Tier 1 to Tier 4).

The default tier value is configurable through the GUI, permitting service provisioning personnel to structure traffic flow, as required.

1.4 Connector Types

SpokeConnector

- interconnect Layer 2 services or Layer 2 and IES
- Join using Spoke SDPs
- Endpoints must be on different devices
- Operational state dependant upon SDP bindings
- Alarms aggregated within composite service

Service type	Encapsulation type
VLL	IES, VPLS
VLAN	—
VPLS	IES, VLL, VPLS
MVPLS	MVPLS
IES	VLL, VPLS
VPRN	—

There are three types of connectors that join SCs in a composite service:

- Pseudowire spoke (SpokeConnector)
- SCP-to-SCP (Scp Connector)
- Internal cross-connect (CrossConnector)

Pseudowire Spoke (SpokeConnector)

A SpokeConnector is used to interconnect Layer2 services or Layer2 and IES services and the SCPs must be on different devices and are connected through spoke SDPs. SpokeConnectors are subject to restrictions on the SC types they can connect, as shown in the chart above.

The operational state of a SpokeConnector depends upon the operational state of the underlying SDP bindings. An alarm raised against one of the SDP bindings causes an alarm to be raised against the connector. These alarms will be aggregated within the composite service.

1.4 Connector Types [cont.]

ScpConnector

- interconnect service interfaces (i.e. SAP to SAP)
- Endpoints may be on same device or different devices
- Operational state dependant upon endpoints
- Alarms aggregated within composite service

SAP type	Supported PW spoke service interconnections
Ethernet	Dot1 Q Q in Q Null
ATM	VPI/ VCI VPI
FR	DLCI
SONET/SDH	BCP Null Bcp Dot1 Q IPCP PPP Auto cHDLC WAN Mirror
LAG	Null Dot1 Q

Alcatel·Lucent UNIVERSITY

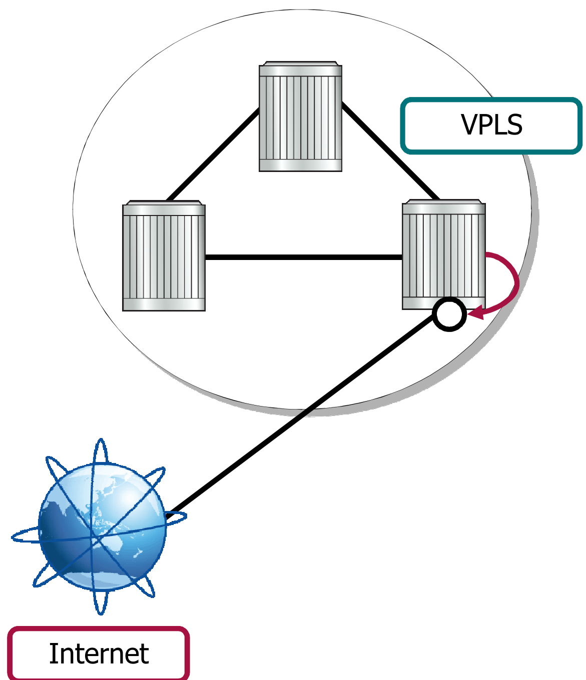
SCP-to-SCP (ScpConnector) connectors can join any two SC types that have service interfaces on the same device or on different devices. A connector between VPLS and VPRN SAPs is an SCP-to-SCP connector, as is a connector between a dot1Q-encapsulated VPLS SAP and L2 switch uplink port in a VLAN ring group. The chart above defines the valid encapsulation types for a ScpConnector.

The operational status of an SCP-to-SCP connector depends on the operational status of its endpoints. An alarm raised against one of the endpoints causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

1.4 Connector Types [cont.]

CrossConnect

- Join any SC types
- Uses CCAG to join SAPs or network interfaces on same device
- Requires Versatile Services Module (VSM)
- Operational state dependant upon CCAG
- Alarms aggregated within composite service



Alcatel·Lucent UNIVERSITY

An internal cross-connect connector can join any SC types. It uses a CCAG to join two SCs that have SAPs or network interfaces on the same device. This functionality is available in the 7450 ESS, 7710 SR, and 7750 SR. The following rules apply to internal cross-connect connectors:

- A SAP can be connected to another SAP or to a network interface using a CCAG.
- When a SAP or network interface is deleted, the connector associated with it is also deleted.
- The deletion of an internal cross-connect connector causes the associated interfaces and SAPs to be deleted.

The operational state of an internal cross-connect connector depends on the operational state of the CCAG. An alarm raised against the CCAG causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

1.5 Composite Service Rules

Composite Services

- A composite service exists only in the context of the 5620 SAM.
- A composite service may have zero SCs and zero connectors.
- Any two SCs may belong to only one composite service.
- An SC may be moved from one composite service to another.
- A connector may belong to only one composite service.
- The connector must first be removed before an SC may be removed.
- All SCs and connectors must be removed before a composite service may be deleted.

Alcatel·Lucent UNIVERSITY

To simplify composite service configuration and to ensure that non-5620 SAM device configuration does not disrupt the management of composite services, the following rules apply to the creation, deletion, modification, and presentation of composite services:

- A composite service can have zero SCs.
- A composite service can have zero connectors.
- Two connected SCs can belong to only one composite service.
- A connector between two SCs belongs to only one composite service.
- An SC cannot be removed from a composite service until its connector to the composite service is removed.
- A group of connected services can be moved from one composite service to another.

Knowledge Verification – Service Connectors

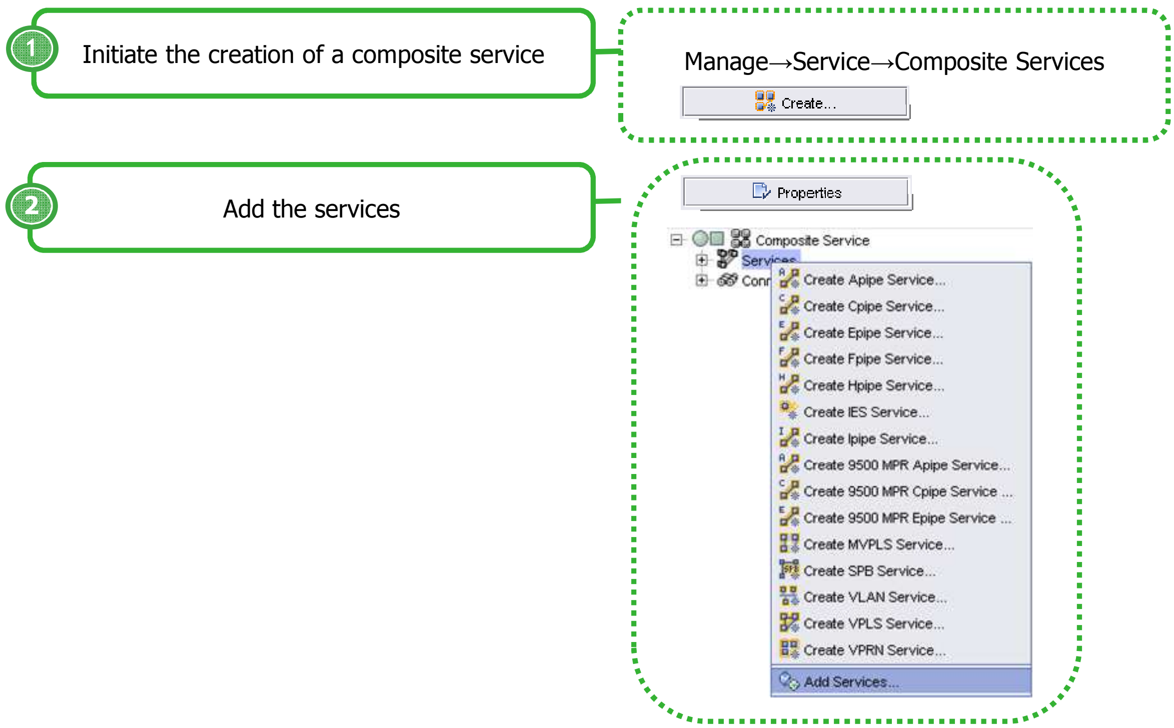
What is the best definition of Pseudowire Spoke Connector (SpokeConnector).

a. Joins any two SC types that have service interfaces on the same device or on different devices.
b. Interconnects Layer2 services or Layer2 and IES services and the SCPs must be on different devices and are connected through spoke SDPs.
c. Join any SC types.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.6 Composite service configuration workflow



Alcatel·Lucent UNIVERSITY

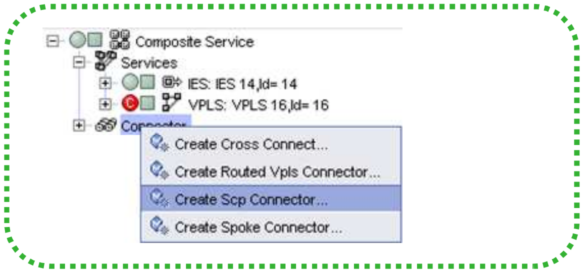
The workflow illustrated above describes the steps for a network administrator or operator to configure a Composite Service.

As a prerequisite for creating a composite service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured
- the other network services that are to be the SCs of the composite service are created

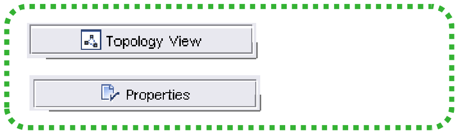
3.9 Composite service configuration workflow [cont.]

3 Add connection between services



4 Configure Mesh SDP bindings, including manual or auto selection of SDP

5 Manage Service



Alcatel·Lucent UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a composite service

Lab Exercises
Create a composite service

Time allowed: 10 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

This page is left blank intentionally

End of module
Composite

Section 3
Service Types

Module 6
Mirror

TOS36042_V3.0-SG-English-Ed1 Module 3.6 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you will be able to:

- Define the function of a service mirror
- List the components of a service mirror

This page is left blank intentionally

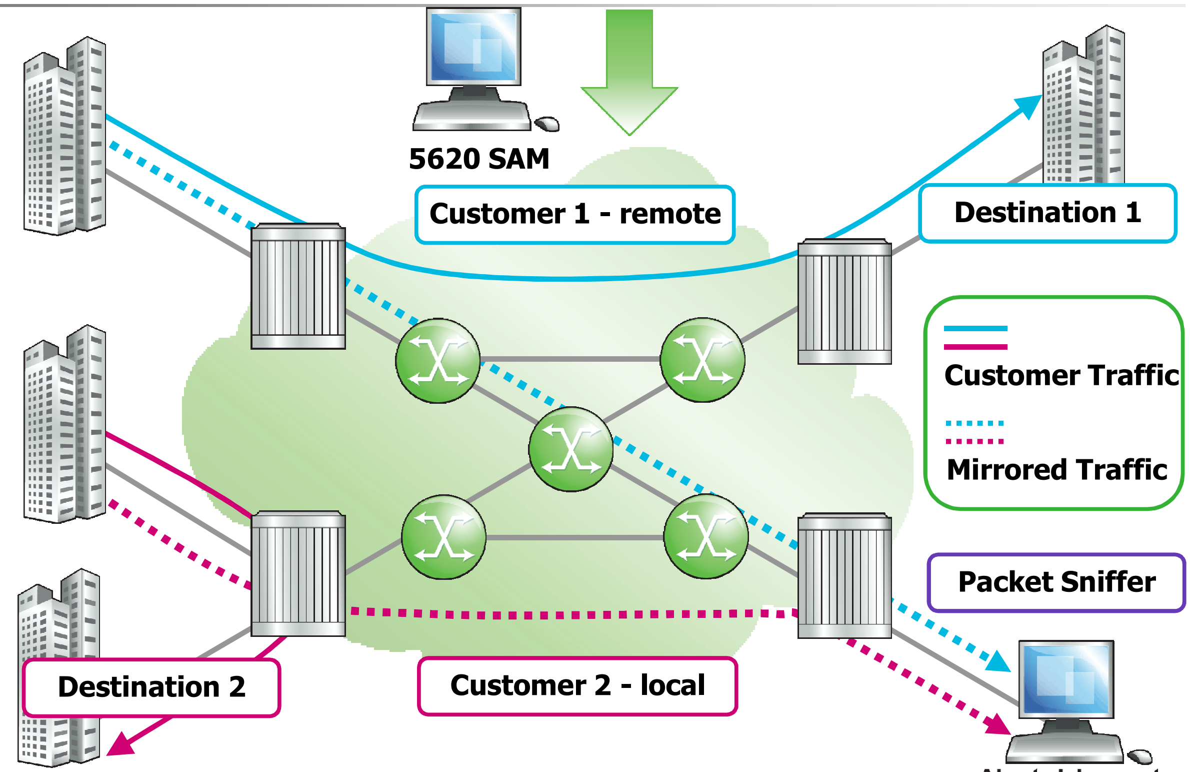
Table of Contents

This page is left blank intentionally

1 Mirror Service

1 Mirror Service

1.1 Mirror service overview



3 · 6 · 8
Service Types · Mirror
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

The 5620 SAM GUI implementation of service mirroring provides mirroring of service traffic packets from any service type.

In a mirror service, packets from one or more sources are forwarded to their normal destinations and a copy of the entire packet, or a specified portion of the packet, is sent to the mirror destination. The mirrored packet can be viewed using a packet-decoding device, typically called a sniffer, that is attached to the destination port. The 5620 SAM does not limit the number of destination and source sites added under a mirror service. The mirrored packets are transported in one direction through the core network using IP or MPLS tunneling.

Note
Service mirroring can affect performance across the network and in the source and destination devices, so must be planned accordingly.

1.1 Mirror service overview [cont.]

Features and benefits

- **Troubleshoot problems with customer packet delivery and content**
- **Help service providers meet regulations by providing itemized call records and wiretaps, as authorized by investigative authorities**
- **Simplify the complex traffic-analysis networks that are often implemented as overlays to the customer-facing network**
- **Option to specify full or sliced packet mirroring**

Service mirroring allows service providers to examine customer packets that traverse a network. This activity assists in troubleshooting complex network problems and can also be used for surveillance purposes when authorized by legal agencies. In the past, network surveillance required complex configuration with the service mirror restricted between ports on the same device.

Service Mirroring on the 7750 SR and 7450 ESS supports the mirroring of traffic on a per-service basis. You can monitor traffic specific to a port, SAP, or SDP. Mirrored traffic can be monitored using the following methods:

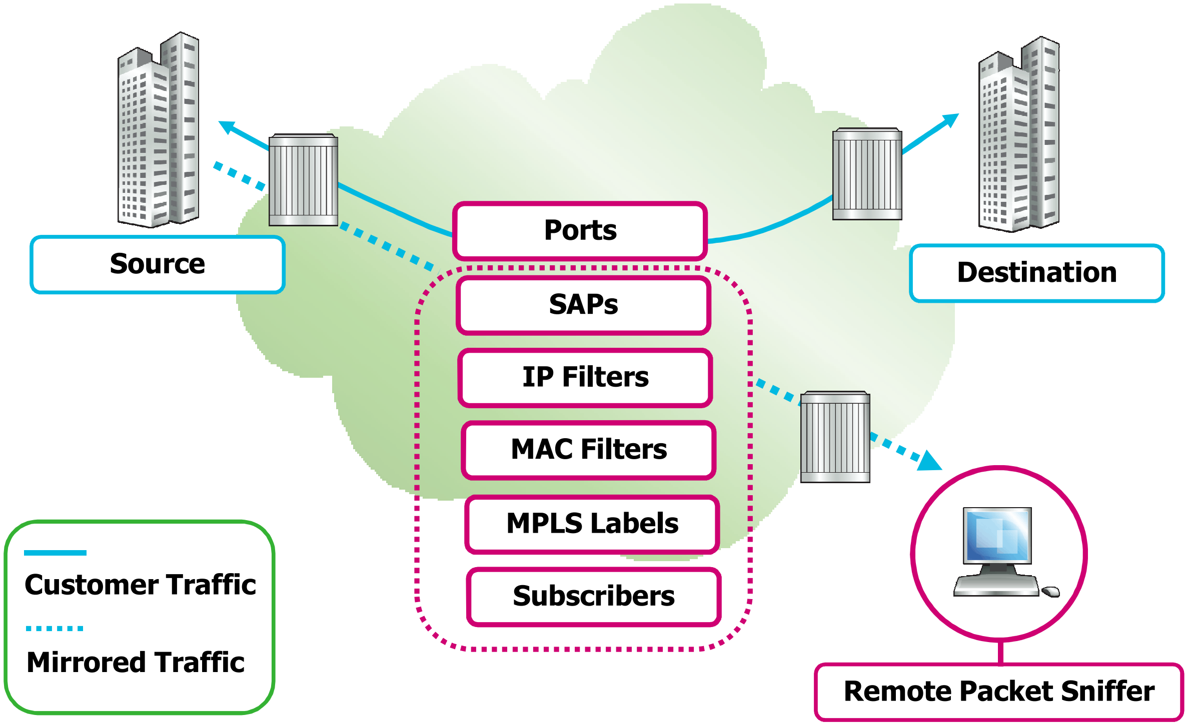
- Local; on the same node where the traffic source is located
- Remote; on a different node than the traffic source) in which case the traffic is re-encapsulated and transported through the core network to another location, using either GRE or MPLS tunnelling.

In addition, it is possible to select portions or ‘slices’ of customer traffic packets. This level of granularity saves resources by transporting the portions of a packet that are required for analysis. Service mirroring is supported on all interface types. Accordingly, a service that uses only Ethernet links end-to-end can be mirrored to a SONET/SDH network port, transported across the core network, and delivered on either Ethernet or SONET/SDH egress ports at the location that performs the service analysis.

Service mirror feature summary:

- Service-based
- Slicing – only a specified portion of each packet is mirrored
- Any interface, mixed interfaces (encapsulation translation) – traffic from an Ethernet port can be mirrored to a SONET/SDH port or vice-versa
- Implemented on ingress/egress SAPs or ingress/egress network interfaces
- Local and remote mirroring

1.2 The Alcatel-Lucent difference



Alcatel·Lucent UNIVERSITY

There are Layer 3 switches and routers from other vendors that provide service mirroring on a per-port basis within the device. The additional functionality provided by Alcatel-Lucent service routers is the ability to mirror on an n-to-1 unidirectional service basis and re-encapsulate the mirrored data for transport through the core network to another location using IP or MPLS tunnels.

Service mirroring can be implemented on the following interfaces:

- service access points (SAPs)
- IP filters
- MAC filters
- MPLS labels
- Subscribers

You can also specify multiple SAPs for inclusion in the service mirror.

Knowledge Verification – Service Mirror Destination

You can view a service mirror packet using the following equipment.

a. RADIUS server.
b. TACACS+ server.
c. Packet sniffer/packet-decoding device.
d. Auxiliary server.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.3 Configuration options

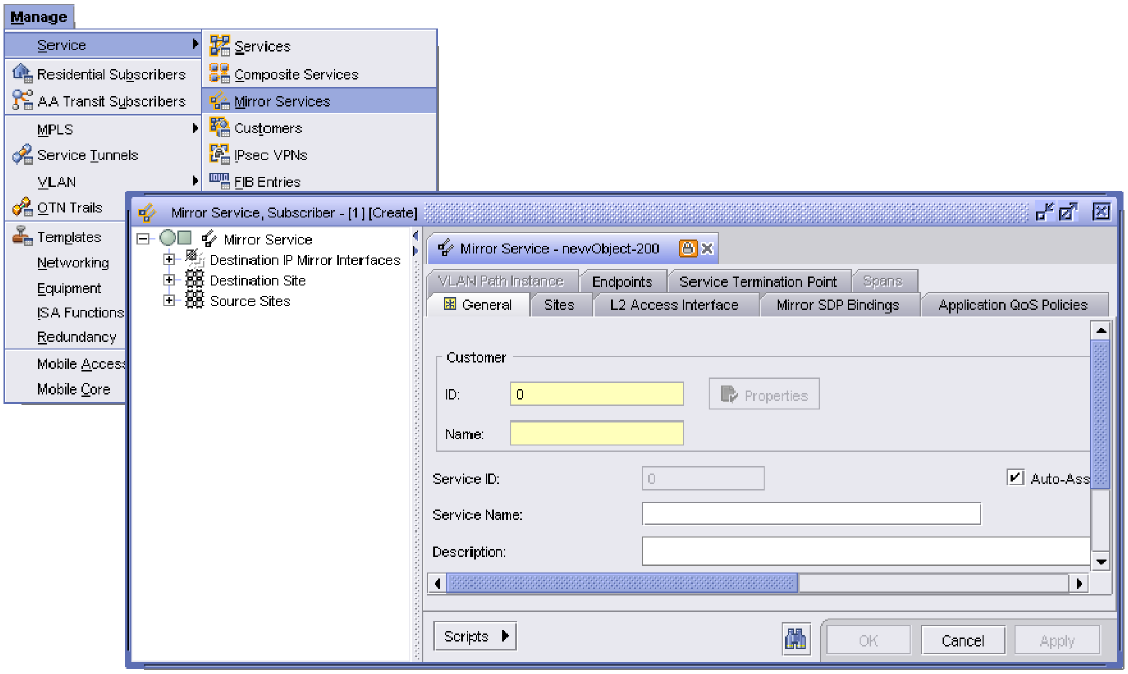
The 5620 SAM supports end-to-end mirror service configuration using the following methods:

1. Tabbed configuration form with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.

2. Preconfigured template. A user that has the Administrator scope of command role, or the Mirror Service Management and Template Script Management roles, can create a mirror service template.

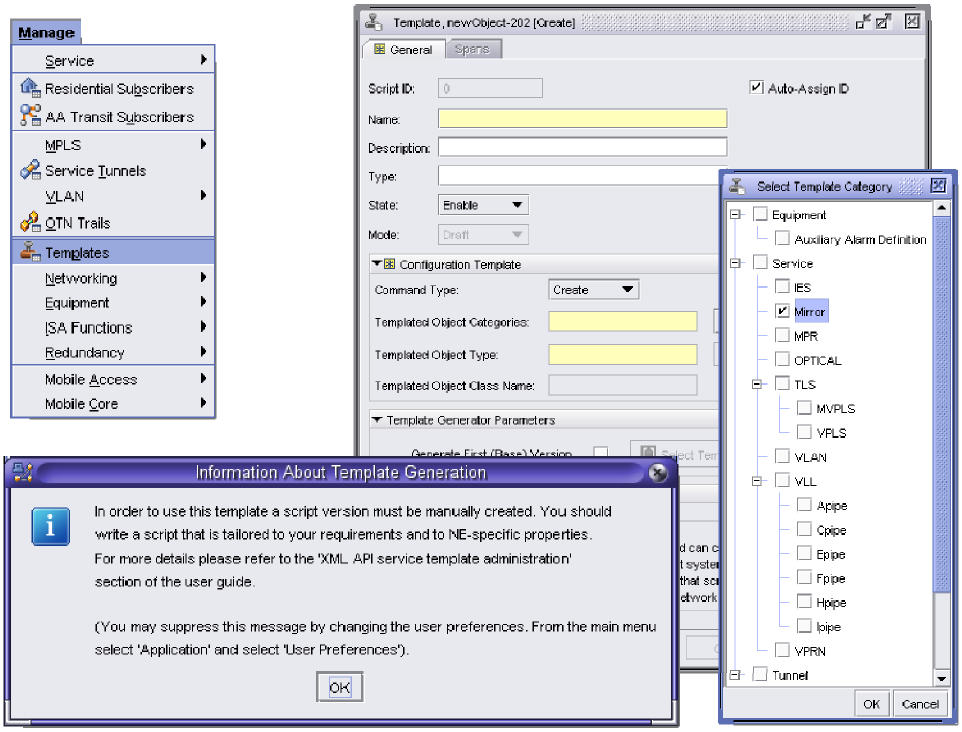
3. The Lawful Interception Management scope of command role allows an LI user to view and configure LI sources on existing mirror services. Information that is mirrored is hidden from all users who do not have LI user privileges.

1.3.1 Configuration options — tabbed configuration form



Alcatel·Lucent
UNIVERSITY

1.3.2 Configuration options — preconfigured template



Alcatel·Lucent UNIVERSITY

Technical References

See the 5620 SAM Scripts and Templates Developer Guide for information on how to develop, manage, and execute CLI-based or XML-based scripts or templates.

1.3.3 Configuration options — LI scope of command

NE LI configuration

Create LI user profile and account on NEs

```
configure system security profile li-prof ↵
configure system security snmp ↵
```

Enable LI discovery on NE

+

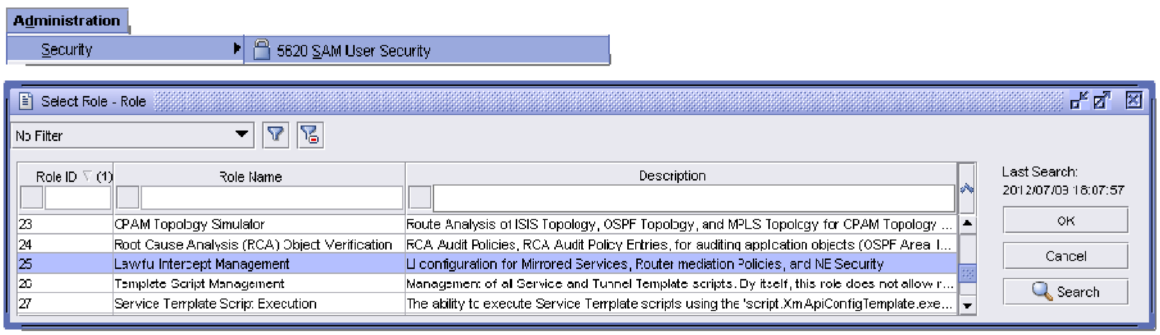
5620 SAM LI configuration

Create LI user

Configure LI source IP and MAC filters

LI source subscriber

Configure LI mirrored subscriber hosts configured with a RADIUS server

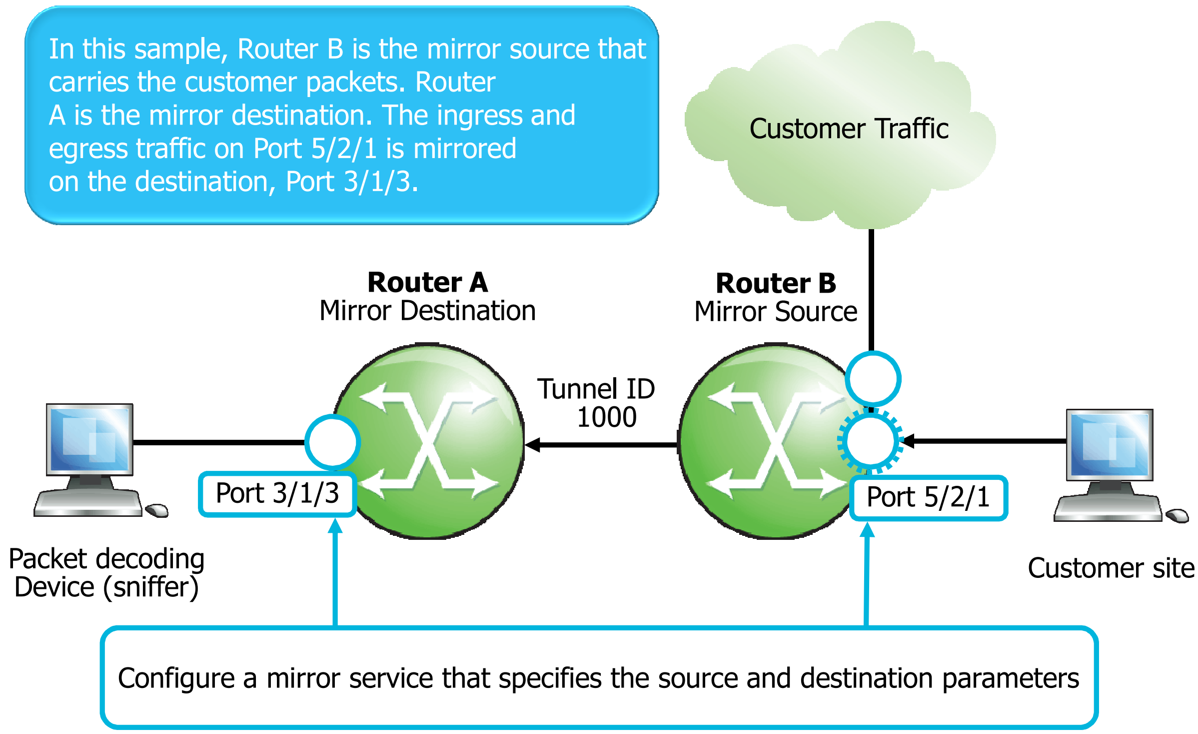


Alcatel·Lucent UNIVERSITY

For LI source configuration:

- You must be assigned the Lawful Interception Management scope of command role to view, create or modify any LI-related objects in the 5620 SAM
- LI source configurations are saved on an NE when the poller policy for the NE specifies LI Local Save Allowed

1.4 Sample mirror service configuration



3 · 6 · 16
Service Types · Mirror
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

1. Connect the packet sniffer to the mirror destination. The packet sniffer is attached to Router A, Port 3/1/3.

2. Configure the mirror destination parameters.
   - Port 3/1/3 on Router A is the mirror destination
   - Tunnel ID 1000 is the transport tunnel to the mirror destination
   - All the parameters required to configure the type of mirroring; for example, slicing and mirror classification, are specified in the destination parameters

3. Specify the source entity that you want to mirror. The egress and ingress traffic on Port 5/2/1 is mirrored in this example.

Knowledge Verification – Service Mirror Destination

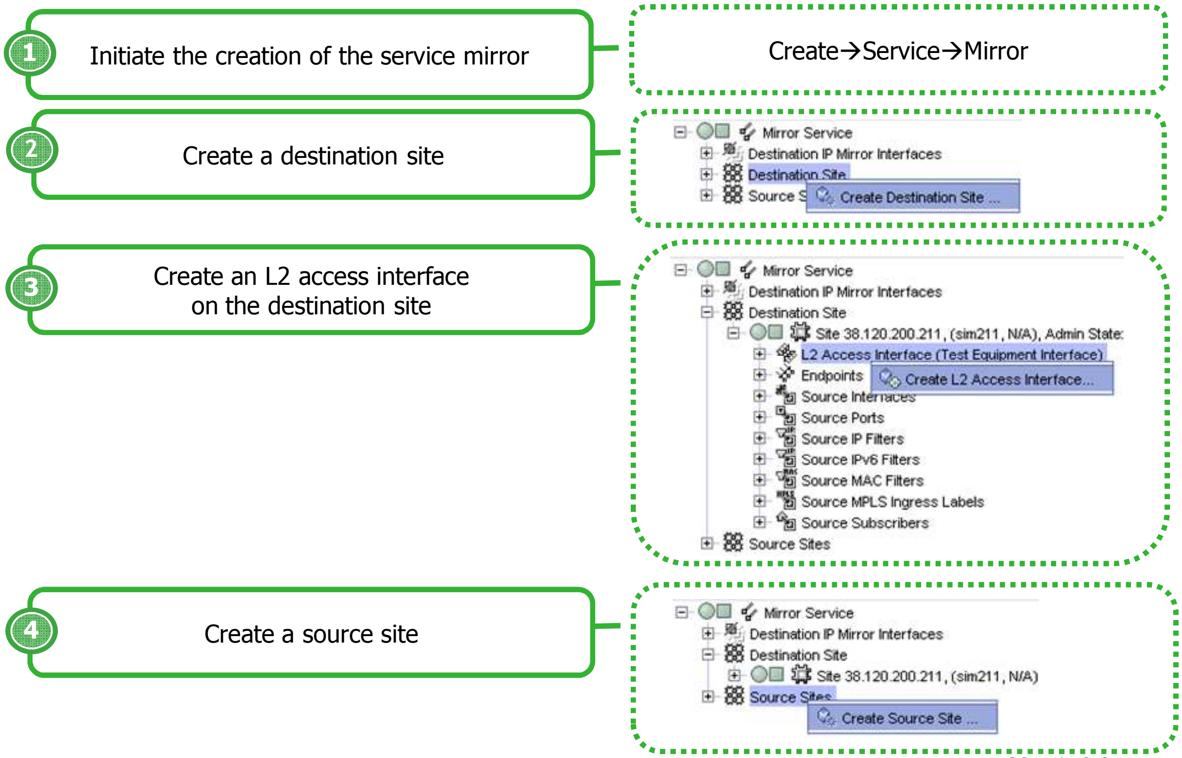
Viewing or retrieving LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope applies to the records of all users.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.5 Workflow to create a mirror service

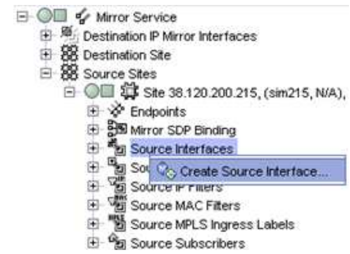


The above workflow lists the high-level steps required to create a mirror service. As a prerequisite for creating a mirror service, this workflow assumes the following:

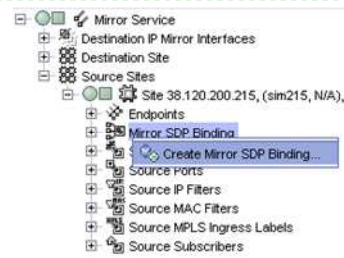
- a group or customer with the required user access privileges has been set up
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; you do not have to create pre-defined policies if policies are created on a per-service basis
- any required MP-BGP for PE-to-PE routing is configured
- the network services the mirror service will use are created
- a packet-sniffing device at the L2 SAP that is the destination of the mirror service is configured
- the SAP with the attached packet-sniffing device as the mirror destination is specified
- the source of the packets to be mirrored is configured

1.5 Workflow to create a mirror service [cont.]

5 Create a source interface (SAP) on the source site



6 Create a mirror SDP binding on the source site



7 Manage Service

Alcatel·Lucent UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to initiate the creation of a composite service

Lab Exercises
Create a mirror service

Time allowed: 10 mins

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

This page is left blank intentionally

End of module
Mirror

Section 4
OAM diagnostics

Module 1
OAM Diagnostics

TOS36042_V3.0-SG-English-Ed1 Module 4.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to describe:

- OAM tests available for a service network

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 OAM diagnostic tools

1.1 OAM diagnostic tests

Features and benefits

- Multiple test types to verify service integrity
- Tests can be performed on a per-service basis
- Configuration using the network object property form, Manage Tests form, or from the service and composite service flat topology maps
- OAM diagnostics can be grouped into a test suite using the 5620 SAM Service Test Manager

The proper delivery of services requires that a number of operations must occur correctly at different levels in the service. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel, must be performed successfully for the service to pass traffic to subscribers as agreed to according to SLAs.

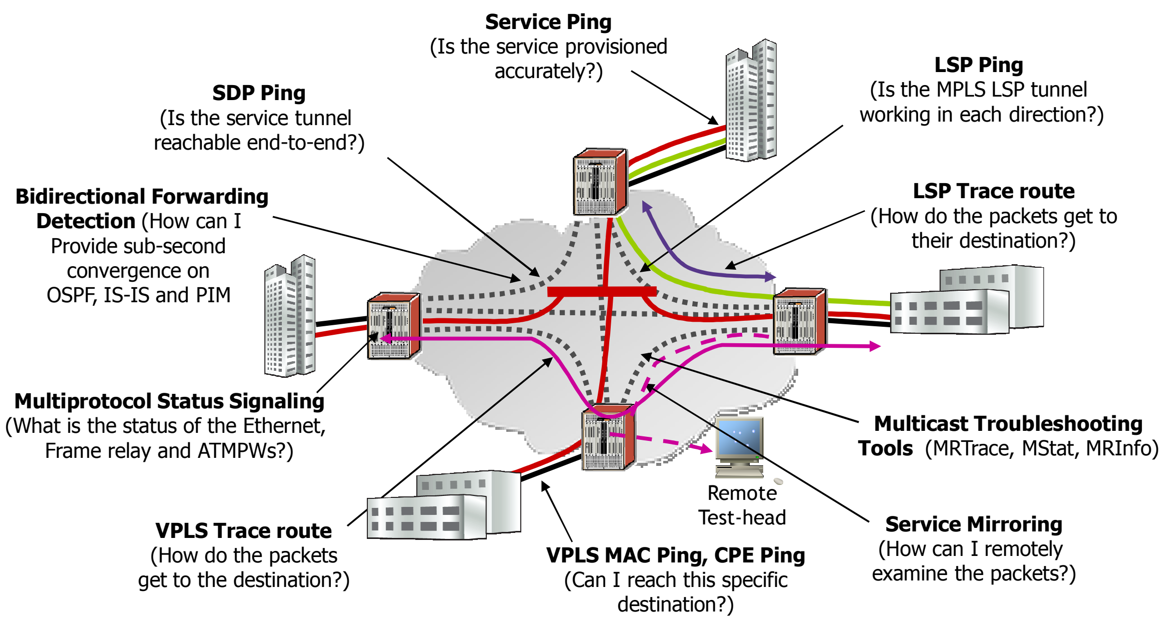
Even when tunnels are operating correctly and are correctly bound to services, incorrect information may cause connectivity issues.

To verify that a service is operational and that configuration information is correct, a set of configurable in-band or out-of-band, packet-based OAM tools is available.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the forwarding path. However, these packets are distinguishable from customer packets, so they are kept within the service provider network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across a portion of the transport network, for example, across LSPs to test reachability.

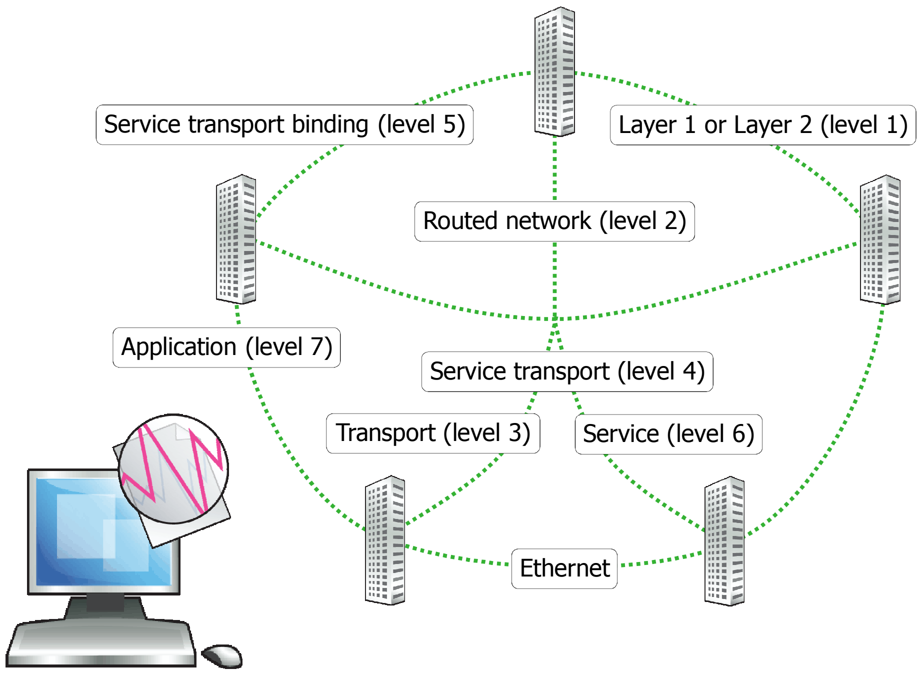
1.3 OAM Toolkit

Service-aware OAM for the efficient maintenance of SLA-based services



Alcatel·Lucent
UNIVERSITY

1.4 Network levels for OAM test types



Alcatel·Lucent UNIVERSITY

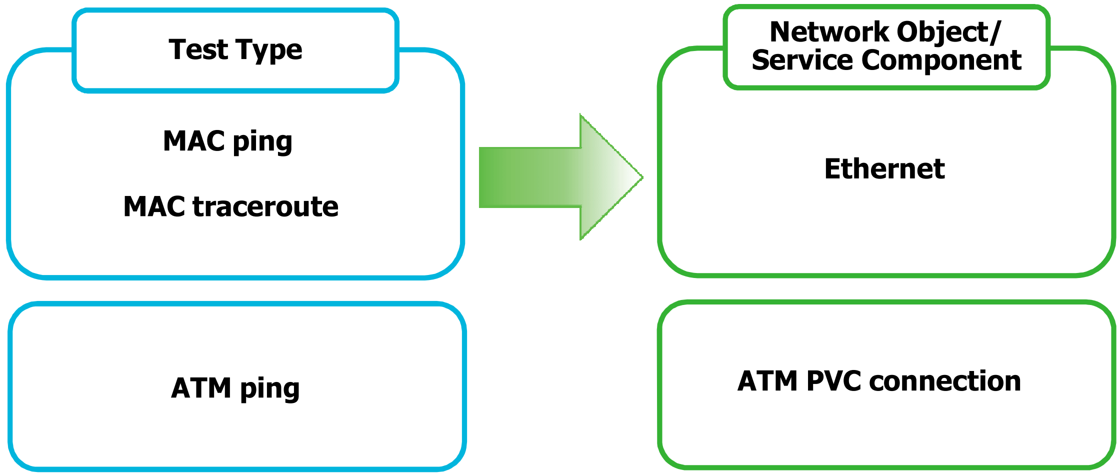
Knowledge Verification – Service Tunnel Diagnostic

Which of the following OAM diagnostics is used to detect if the service tunnel
Is reachable end-to-end.

a. Service Ping.
b. LSP Ping.
c. SDP Ping.
d. LSP Traceroute.

Choose the correct answer for the knowledge verification question above.

1.5 Layer 1 or Layer 2 test types — level 1



MAC ping

The MAC ping OAM tool, which is called mac-ping in CLI, is used to test connectivity in a VLL or VPLS by verifying a remote MAC address at the far end of a service.

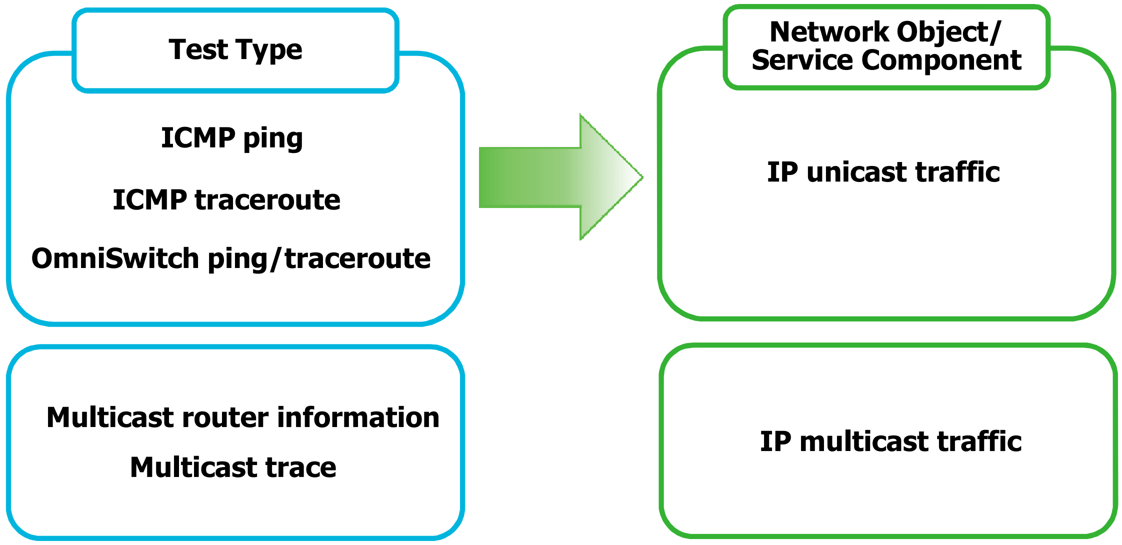
MAC traceroute

The MAC trace OAM tool, which is called mac-trace in CLI, displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end of a service. MAC traces can be sent in-band or out-of-band.

ATM ping

The ATM OAM ping tool, which is called atmoam-ping in CLI, performs an ATM ping on an existing ATM PVC from the PVC endpoint using ATM OAM loopback cells. An ATM ping tests VC integrity and endpoint connectivity for PVCs using OAM loopback capabilities.

1.6 Routed network test types — level 2



ICMP ping
The ICMP ping OAM tool, which is called icmp-ping in CLI, identifies the reachability of a remote host across the IP network. The tool is used with ICMP trace to detect and localize faults in IP networks.

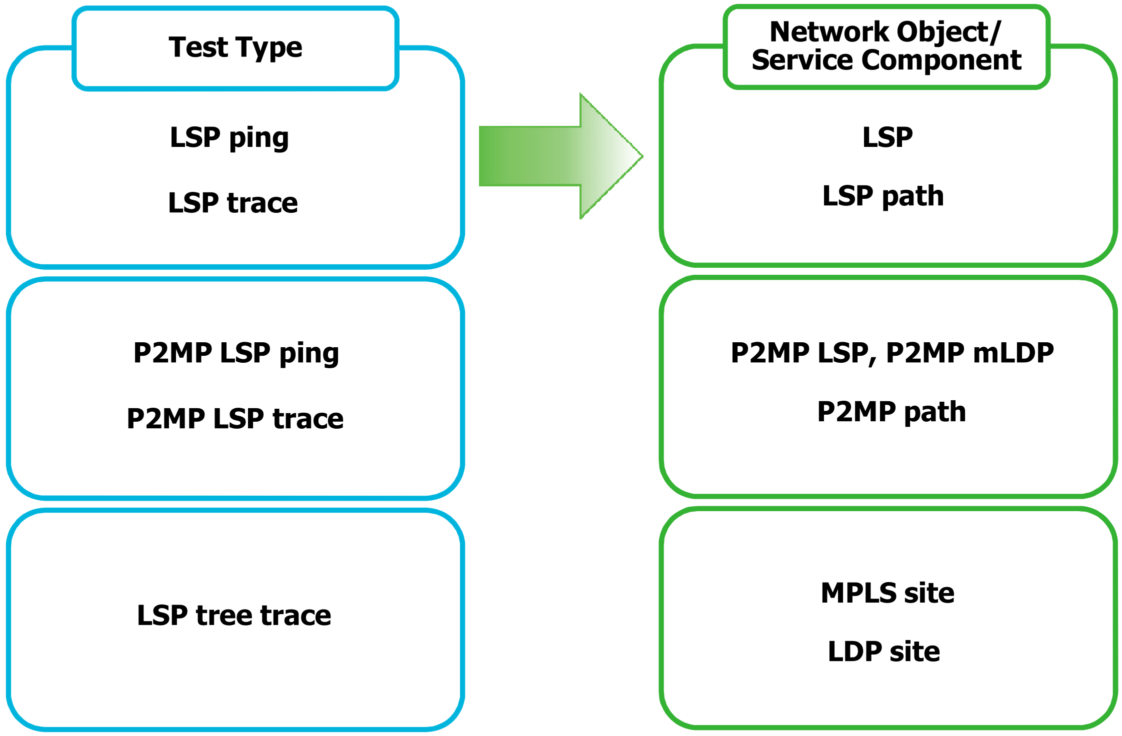
ICMP traceroute
The ICMP trace OAM tool, which is called icmp-trace in CLI, identifies the diagnostic used to trace the ICMP traceroute control table. The tool is used with ICMP ping to detect and localize faults in IP networks.

OmniSwitch ping/traceroute
The 5620 SAM supports OmniSwitch ping and traceroute by using user-defined CLI scripts.

Multicast router information
The multicast router information OAM tool, which is called mrinfo in CLI, identifies VPRN multicast information for the target router. The information includes details that are related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

Multicast trace
The multicast trace OAM tool, which is called mtrace in CLI, identifies the hop-by-hop route used by VPRN multicast traffic to reach the target router. This diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. The 5620 SAM attempts to trace the receiver-to-sender route for the traffic. The destination of the diagnostic can be any PIM-enabled interface in the routing instance.

1.7 Transport test types — level 3



Alcatel·Lucent UNIVERSITY

LSP ping
The LSP Ping OAM diagnostic tool, which is called lsp-ping in CLI, performs in-band LSP connectivity tests. The test identifies data plane failures in LSPs and whether the LSP tunnels are working in both directions

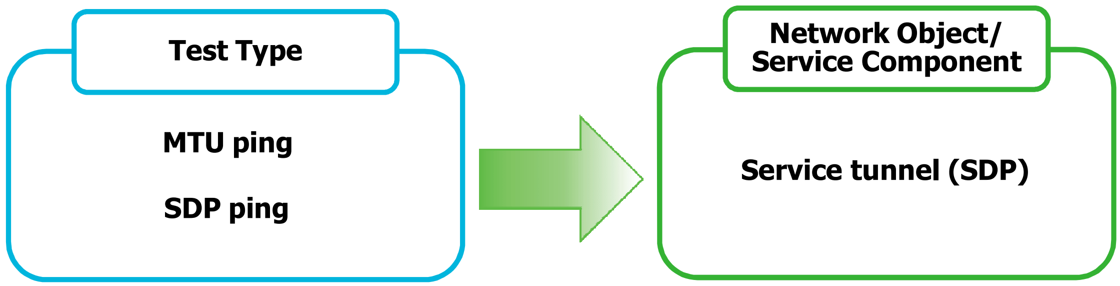
LSP trace
The LSP Trace OAM diagnostic tool, which is called lsp-trace in CLI, displays the hop-by-hop route used by the LSP.

P2MP LSP ping
The PSMP LSP Ping OAM diagnostic tool, which is called p2mp-lsp-ping in CLI, performs in-band LSP connectivity tests.

P2MP LSP trace
The PSMP LSP Trace OAM diagnostic tool, which is called p2mp-lsp-trace in CLI, performs in-band LSP connectivity tests.

LSP tree trace
The LDP Tree Trace OAM diagnostic tool, which is called ldp-treetrace in OAM level of the CLI, is used to detect and discover the ECMP routing paths for a LSP between egress and ingress routers.

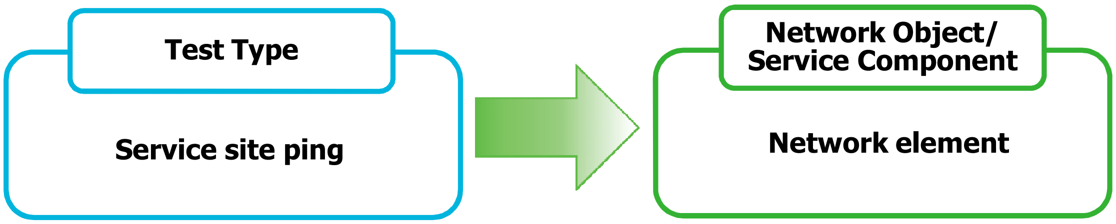
1.8 Service transport test types — level 4



MTU ping
The MTU Ping OAM diagnostic tool, which is called sdp-mtu in the CLI, provides a tool for service providers to determine the exact frame (MTU) size that is supported on a service tunnel (also called an SDP), to within one byte.

SDP ping
The Tunnel Ping OAM tool, which is called sdp-ping in the CLI, performs in-band unidirectional or bidirectional connectivity tests on service tunnels (also called an SDP). The OAM packets are sent in-band in the tunnel encapsulation, so they follow the same path as the service traffic. The response can be received out-of-band in the control plane or in-band using the data plane for a bidirectional test.

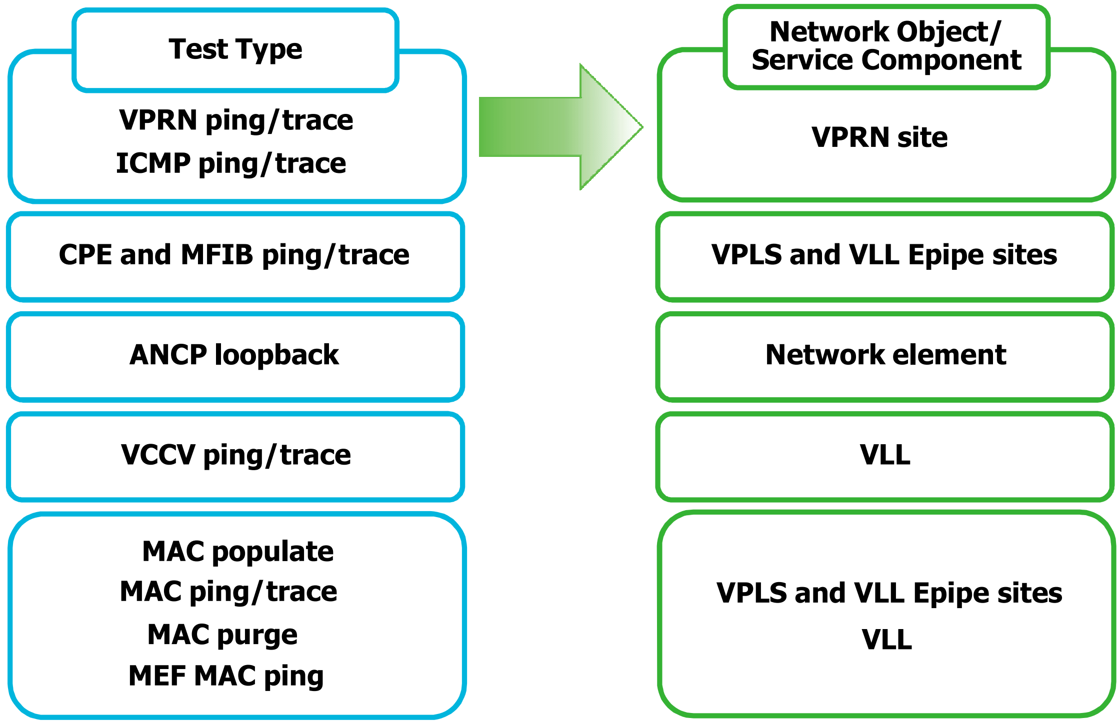
1.9 Service transport binding test types — level 5



Service site ping

The Service Site Ping OAM diagnostic tool, which is called svc-ping in the CLI and was formerly called the circuit ping, provides end-to-end connectivity testing for an individual service. This diagnostic operates at a higher level than the tunnel OAM ping because it verifies connectivity for an individual service rather than connectivity across the service tunnel. This allows you to isolate a problem within the service rather than at the port, which is the endpoint of the service tunnel.

1.10 Service test types — level 6



Alcatel·Lucent UNIVERSITY

VPRN ping/trace
The VPRN ping and VPRN trace OAM tools are enabled from the VRF site of the subscriber's VPRN service. The VPRN ping determines the existence of the far-end egress point of the service.

The VPRN trace displays the hop-by-hop path for a destination IP address within a VPRN service.

ICMP ping/trace
The ICMP ping OAM tool, which is called icmp-ping in CLI, identifies the reachability of a remote host across the IP network.

The ICMP trace OAM tool, which is called icmp-trace in CLI, identifies the diagnostic used to trace the ICMP traceroute control table.

CPE and MFIB ping
The CPE ping tool, which is called cpe-ping in the CLI, is used to trace the end-to-end switching of specified MAC addresses of customer premises equipment. This ping extends the functionality of the MAC ping beyond the egress (customer-facing) port by allowing a ping to the SAP of a VPLS or a VLL Epipe service over a VPLS PBB backbone.

ANCP loopback
The ANCP loopback test, which is called oam ancp in the CLI, is used to send DSL OAM commands to complete an OAM test from a centralized point or when operational boundaries prevent direct access to the DSLAM. The ANCP loopback test raises an alarm that generates a log event displaying both successful and failed results.

1.10 Service test types — level 6 [cont.]

VCCV ping/trace

The VCCV Ping OAM diagnostic tool, which is called vccv-ping in the CLI, performs in-band VLL connectivity tests. It can be used for all types of VLLs and supports cross-circuit tests as long as the circuit types match; for example, an Epipe to Epipe connector.

The VCCV Trace OAM diagnostic tool, which is called vccv-trace in the CLI, displays the hop-by-hop path used by the VLL.

MAC populate

The MAC populate OAM tool, which is called mac-populate in CLI, is used to:

- Know whether the FIB table is accurate by testing forwarding plan correctness. This is done by populating a service FIB with an OAM-tagged MAC entry. This MAC entry indicates that the node is the egress node for the MAC address of a service. You can then use the FIB manager to see the OAM-tagged MAC entry.
- Send a message through the flooding domain to learn a MAC address, as if a customer packet with that source MAC address had flooded the domain from that ingress point of the service.

MAC ping/trace

The MAC ping OAM tool, which is called mac-ping in CLI, is used to test connectivity in a VLL or VPLS by verifying a remote MAC address at the far end of a service.

The MAC trace OAM tool, which is called mac-trace in CLI, displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end of a service. MAC traces can be sent in-band or out-of-band.

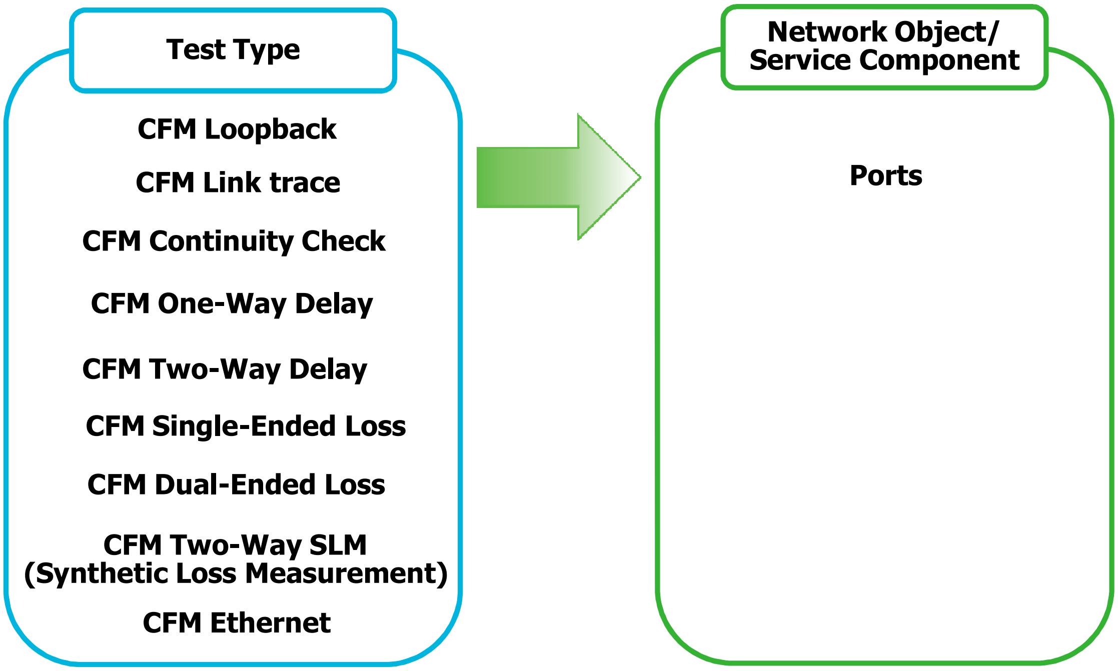
MAC purge

The MAC purge OAM tool, which is called mac-purge in CLI, is used to delete an OAM-tagged entry from a FIB, which was generated using the MAC populate OAM tool. This clears the FIB of any learned information for a specific MAC address, allows the FIB to be populated only by a MAC populate request, and can be used to flush all devices in a service domain.

MEF MAC ping

The MEF MAC ping OAM tool to test connectivity in a 7250 SAS- ES or 7250 SAS-ESA, Release 3.0, VPLS site. The MEF MAC ping verifies a remote MAC address at the far end of the service. MEF MAC ping must run simultaneously in both directions between the VPLS sites being tested.

1.11 Ethernet test types



Alcatel·Lucent UNIVERSITY

CFM Loopback
CFM loopback messages are sent to a unicast destination MAC address. The MEP at the destination responds to the loopback message with a loopback reply. A MEP or a MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. CFM loopback tests verify connectivity to a specific MEP or MIP.

CFM Link trace
CFM link trace messages that contain a target unicast MAC address are sent to multicast destination MAC addresses. Each MIP at the same MD level replies with a link trace response. Messages are forwarded to the next hop until they reach the destination MAC address. The originating MEP collects the replies to determine the path.

CFM Continuity Check
CFM continuity check, or CC, messages, are multicast messages that a MEP transmits periodically to remote MEPs in the same MEG. CC tests are used to discover a remote end point, check the health of a site, and detect cross-connect misconfigurations. The loss of three consecutive CCM messages, or the receipt of a CCM with incorrect information, indicates a fault.

1.11 Ethernet test types [cont.]

CFM One-Way Delay
The CFM one-way delay test applies only to Y.1731 MEPs. The test originates on one MEP and terminates on a target MEP. The results are read from the target MEP. In the test, frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source site until the frame is received by the destination site. The frame delay represents the one-way trip time between the source and destination sites.

CFM Two-Way Delay
The CFM two-way delay test applies only to Y.1731 MEPs. In this test, the frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by the source site until the frame is received by the same site after passing through the destination site. The frame delay represents the round-trip time between the source and destination sites.

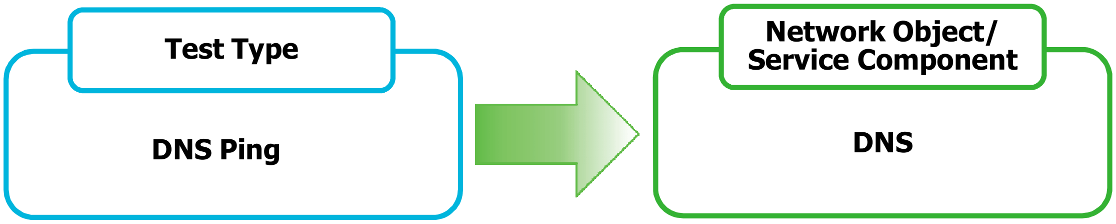
CFM Single-Ended Loss
The CFM single-ended loss test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a single-ended loss test is a destination MAC address. The test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between the two MEPs.

CFM Dual-Ended Loss
A CFM dual-ended loss test functions as an optional extension of a CC test. It applies only to Y.1731 MEPs. This type of test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between two MEPs. When a CC test is executed with the dual-ended loss option enabled, the option is replicated on all participating MEPs that support the test, along with the accompanying alarm threshold values. If a MEP detects that the local or remote frame loss ratio has exceeded the alarm threshold for a remote MEP, the MEP raises an alarm against the remote MEP.

CFM Two-Way SLM
The CFM two-way SLM test provides Synthetic Loss Measurement and it is used to check the packet loss.

CFM Ethernet
The CFM Eth test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a CFM Eth test is a MAC address. The test is used to perform one-way in-service diagnostics that include verifying bandwidth throughput, frame loss, and bit errors. To perform the test, a MEP inserts frames with Eth-test information that includes specific throughput, frame size, and transmission patterns. A MIP is transparent to Eth-test frames.

1.12 Application test types — level 7



DNS Ping

The DNS ping OAM tool, which is called dns-ping in CLI, identifies the diagnostic used to ping the DNS name, if DNS name resolution is configured

Knowledge Verification – Ethernet OAM Tests

Ethernet CFM tests are used on which one of the following network objects/service components.

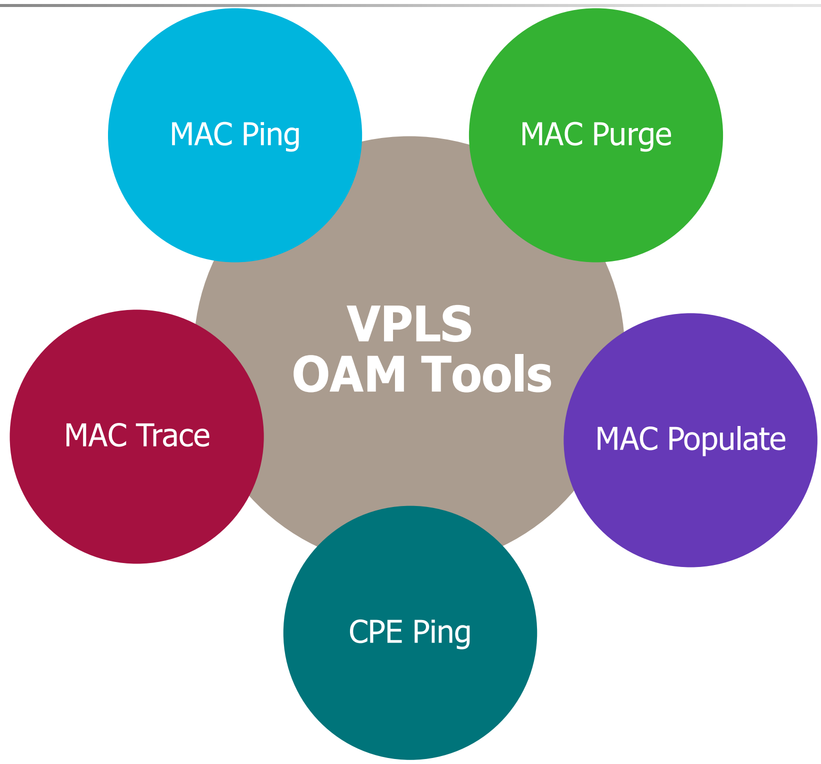
a. Cards.
b. Ring groups.
c. Ports.
d. Channels.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

2 VPLS OAM example

2.1 VPLS Operations, Administration, and Maintenance



VPLS MAC Diagnostics
While the LSP ping, SDP ping and Service ping tools enable transport tunnel testing and verify whether the correct transport tunnel is used, they do not provide the means to test the learning and forwarding functions on a per-VPLS-service basis.

Tunnels can be operational and correctly bound to a service, however, an incorrect Forwarding Information Base (FIB) table for a service can cause connectivity issues in the service, undetected by the ping tools. Alcatel-Lucent has developed VPLS OAM functionality to specifically test all the critical functions on a per-service basis.

The VPLS OAM tools are:

- **MAC Ping** — Provides the ability to trace end-to-end switching of specified MAC addresses. MAC ping provides an end-to-end test to identify the egress customer-facing port where a customer MAC was learned. MAC ping can also be used with a broadcast MAC address to identify all egress points of a service for the specified broadcast MAC;

- **MAC Trace** — Provides the ability to trace a specified MAC address hop-by-hop until the last node in the service domain;

- **CPE Ping** — Provides the ability to check network connectivity to the specified client device within the VPLS. CPE ping will return the MAC address of the client, as well as the SAP and PE at which it was learned;

- **MAC Populate** — Allows specified MAC addresses to be injected in the VPLS service domain. This triggers learning of the injected MAC address by all participating nodes in the service. This tool is generally followed by MAC ping or MAC trace to verify if correct learning occurred;

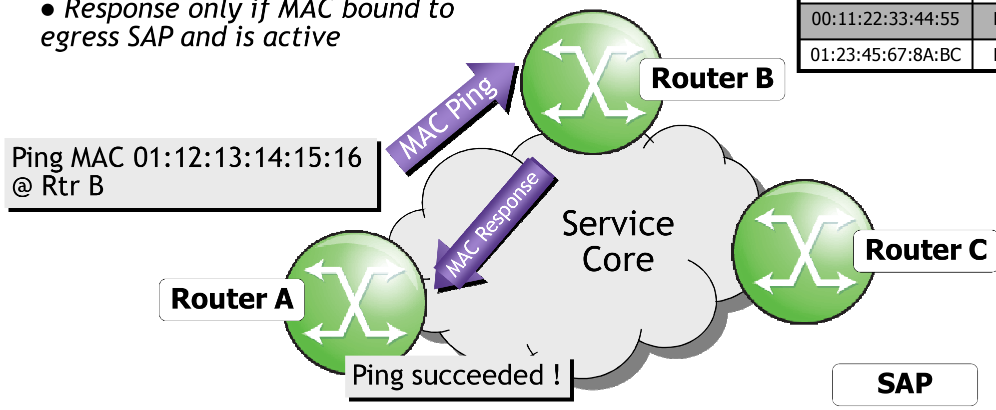
- **MAC Purge** — Allows MAC addresses to be flushed from all nodes in a service domain.

2.2 MAC Ping

- Control Plane forwarding
  - *Forwarded to system through IGP*
  - *Response only if MAC bound to egress SAP and is active*

SAP (Router B)

MAC	Location
01:12:13:14:15:16	Local
00:11:22:33:44:55	Remote
01:23:45:67:8A:BC	Remote



SAP (Router C)

MAC	Location
01:12:13:14:15:16	Remote
00:11:22:33:44:55	Local
01:23:45:67:8A:BC	Remote

- Data Plane Forwarding
  - *Sent with VC label (ttl = 255), MPLS label, etc…*
  - *TTL = 0, passed to management plane for processing*
  - *At egress node, passed to management plane*
  - *Response via data plane or control plane*

Alcatel·Lucent
UNIVERSITY

For a MAC ping test, the destination MAC address (unicast or multicast) to be tested must be specified. A MAC ping packet can be sent through the control plane or the data plane. When sent by the control plane, the ping packet goes directly to the destination IP in a UDP/IP OAM packet. If it is sent by the data plane, the ping packet goes out with the data plane format.

In the control plane, a MAC ping is forwarded along the flooding domain if no MAC address bindings exist. If MAC address bindings exist, then the packet is forwarded along those paths (if they are active). Finally, a response is generated only when there is an egress SAP binding to that MAC address. A control plane request is responded to via a control reply only.

In the data plane, a MAC ping is sent with a VC label TTL of 255. This packet traverses each hop using forwarding plane information for next hop, VC label, etc. The VC label is swapped at each service-aware hop, and the VC TTL is decremented. If the VC TTL is decremented to 0, the packet is passed up to the management plane for processing. If the packet reaches an egress node, and would be forwarded out a customer facing port, it is identified by the OAM label below the VC label and passed to the management plane.

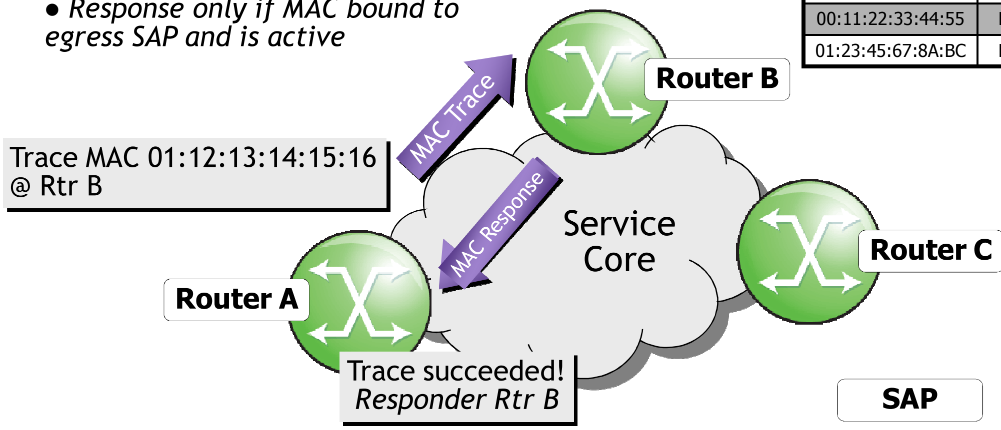
MAC pings are flooded when they are unknown at an intermediate node. They are responded to only by the egress nodes that have mappings for that MAC address.

2.3 MAC Trace

- Control Plane forwarding
  - *Forwarded to system through IGP*
  - *Response only if MAC bound to egress SAP and is active*

SAP

MAC	Location
01:12:13:14:15:16	Local
00:11:22:33:44:55	Remote
01:23:45:67:8A:BC	Remote



SAP

MAC	Location
01:12:13:14:15:16	Remote
00:11:22:33:44:55	Local
01:23:45:67:8A:BC	Remote

- Data Plane Forwarding
  - *Sent with VC label (ttl = 255), MPLS label, etc…*
  - *TTL = 0, passed to management plane for processing*
  - *At egress node, passed to management plane*
  - *Response via data plane or control plane*

Alcatel·Lucent
UNIVERSITY

A MAC trace functions like an LSP trace with some variations. Operations in a MAC trace are triggered when the VC TTL is decremented to 0. Like a MAC ping, a MAC trace can be sent either by the control plane or the data plane. For MAC trace requests sent by the control plane, the destination IP address is determined from the control plane mapping for the destination MAC. If the destination MAC is known to be at a specific remote site, then the far-end IP address of that SDP is used. If the destination MAC is not known, then the packet is sent unicast, to all SDPs in the service with the appropriate squelching.

A control plane MAC traceroute request is sent via UDP/IP. The destination UDP port is the LSP ping port. The source UDP port is whatever the system gives (note that this source UDP port is really the demultiplexer that identifies the particular instance that sent the request, when correlating the reply). The source IP address is the system IP of the sender.

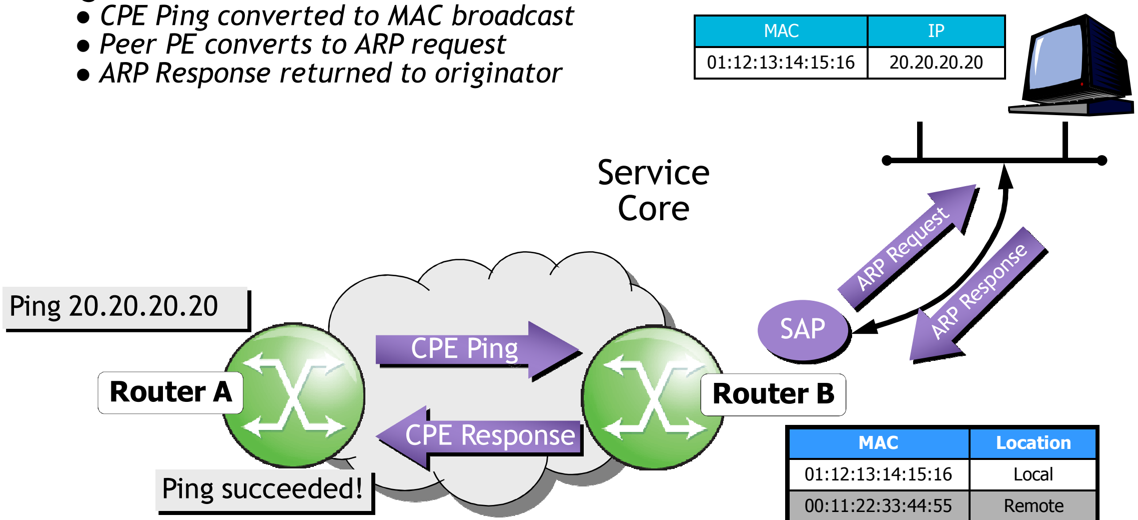
When a traceroute request is sent via the data plane, the data plane format is used. The reply can be via the data plane or the control plane. A data plane MAC traceroute request includes the tunnel encapsulation, the VC label, and the OAM, followed by an Ethernet DLC, a UDP and IP header. If the mapping for the MAC address is known at the sender, then the data plane request is sent down the known SDP with the appropriate tunnel encapsulation and VC label. If it is not known, then it is sent down every SDP (with the appropriate tunnel encapsulation per SDP and appropriate egress VC label per SDP binding).

The tunnel encapsulation TTL is set to 255. The VC label TTL is initially set to the min-ttl (default is 1). The OAM label TTL is set to 2. The destination IP address is the all-routers multicast address. The source IP address is the system IP of the sender. The destination UDP port is the LSP ping port. The source UDP port is whatever the system gives (note that this source UDP port is really the demultiplexer that identifies the particular instance that sent the request, when correlating the reply).

The Ethernet DLC header source MAC address is set to either the system MAC address (if no source MAC is specified) or to the specified source MAC. The destination MAC address is set to the specified destination MAC. The EtherType is set to IP.

2.4 CPE Ping

- Tests for learned MAC
- Ping destination host
  - *CPE Ping converted to MAC broadcast*
  - *Peer PE converts to ARP request*
  - *ARP Response returned to originator*



MAC	IP
01:12:13:14:15:16	20.20.20.20

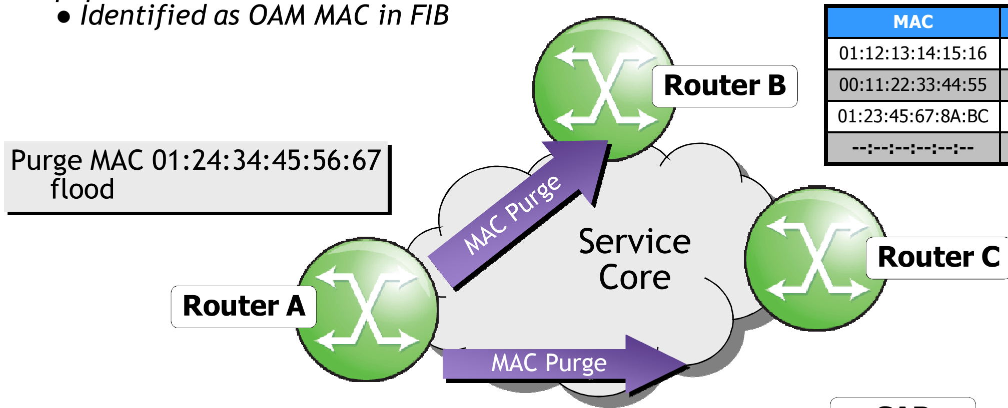
MAC	Location
01:12:13:14:15:16	Local
00:11:22:33:44:55	Remote
01:23:45:67:8A:BC	Remote

The MAC ping OAM tool makes it possible to detect whether a particular MAC address has been learned in a VPLS.

The **cpe-ping** command extends this capability to detecting end-station IP addresses inside a VPLS. A CPE ping for a specific destination IP address within a VPLS will be translated to a MAC-ping towards a broadcast MAC address. Upon receiving such a MAC ping, each peer PE within the VPLS context will trigger an ARP request for the specific IP address. The PE receiving a response to this ARP request will report back to the requesting 7750 SR.

2.5 MAC Purge

- Remove Test MAC Addresses from FIB
  - *Same forwarding mechanism as MAC populate*
  - *Identified as OAM MAC in FIB*



SAP

MAC	Location
01:12:13:14:15:16	Local
00:11:22:33:44:55	Remote
01:23:45:67:8A:BC	Remote
--:--:--:--:--:--	**OAM**

SAP

MAC	Location
01:12:13:14:15:16	Remote
00:11:22:33:44:55	Local
01:23:45:67:8A:BC	Remote
--:--:--:--:--:--	**OAM**

Alcatel·Lucent UNIVERSITY

MAC Purge is used to clear the FIBs of any learned information for a particular MAC address. This allows one to do a controlled OAM test without learning induced by customer packets.

In addition to clearing the FIB of a particular MAC address, the purge can also indicate to the control plane not to allow further learning from customer packets. This allows the FIB to be clean, and be populated only via a MAC Populate.

MAC Purge follows the same flooding mechanism as the MAC Populate. A UDP/IP version of this command is also available that does not follow the forwarding notion of the flooding domain, but the control plane notion of it.

Knowledge Verification – MAC Ping

You must specify the destination MAC address (unicast or multicast) for a MAC ping test.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

3 VLL Epipe OAM example

3.1 SDP Diagnostics – SDP-Ping

SDP-Ping

- Tests for uni-directional or round trip connectivity
- Performs SDP MTU path tests
- Configurable parameters:
  - Message size (default is 40 bytes)
  - Timeout (default is 5 seconds)
  - Interval (default is 1 second)
  - Number of messages to send (default is 1)
  - Originating SDP ID
  - Responding SDP ID (optional)
  - Forwarding class and in/out-of-profile of the OAM message

SDP Ping performs in-band uni-directional or round-trip connectivity tests on SDPs. The SDP Ping OAM packets follow the same path as traffic within the service. The SDP Ping response can be received out-of-band in the control plane, or in-band using the data plane for a round-trip test.

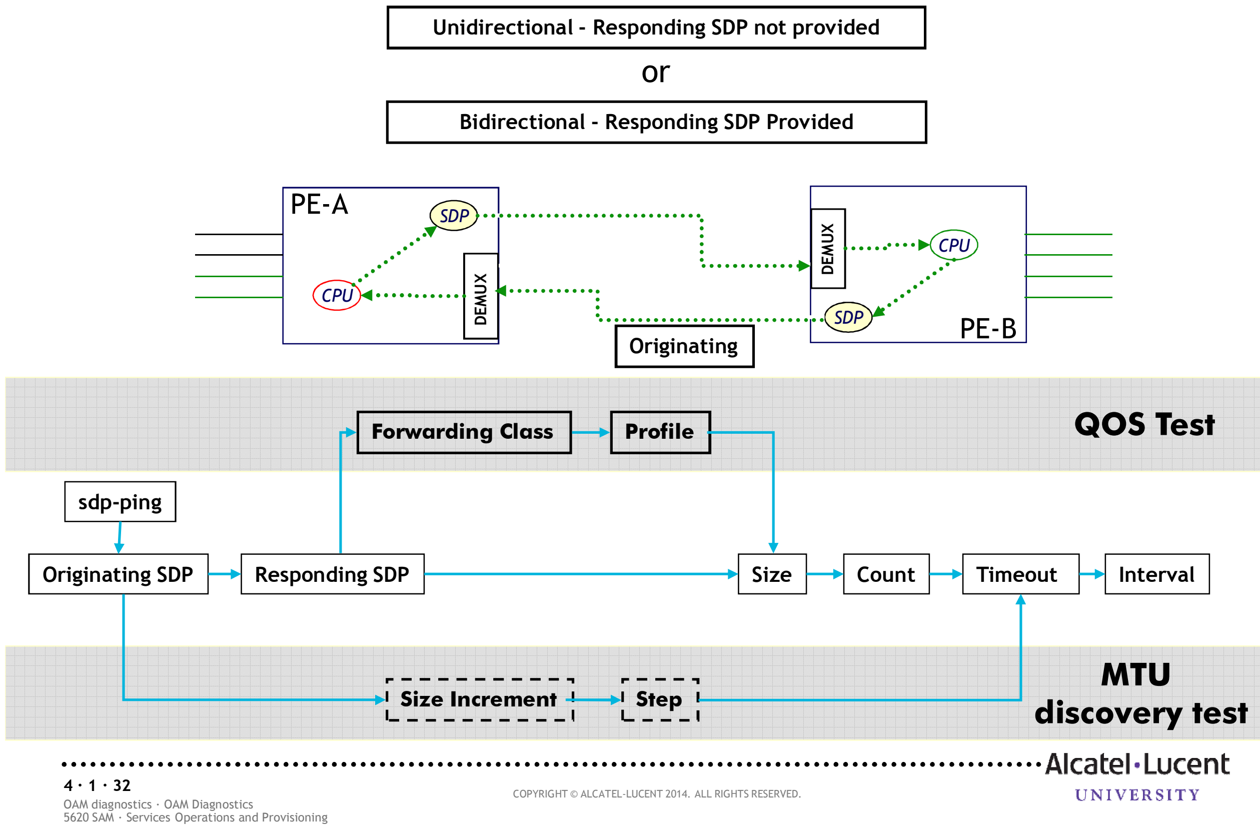
A unidirectional SDP Ping tests:

- Egress SDP ID encapsulation
- Ability to reach the far-end IP address of the SDP ID within the SDP encapsulation
- Path MTU to the far-end IP address over the SDP ID
- Forwarding class mapping between the near-end SDP ID encapsulation and the far-end
- tunnel termination

A round-trip SDP Ping specifies a local egress SDP ID and an expected remote SDP ID. SDP round trip testing is an extension of SDP connectivity testing with the additional ability to test:

- Remote SDP ID encapsulation
- Potential service round trip time
- Round trip path MTU
- Round trip forwarding class mapping

3.2 SDP-Ping

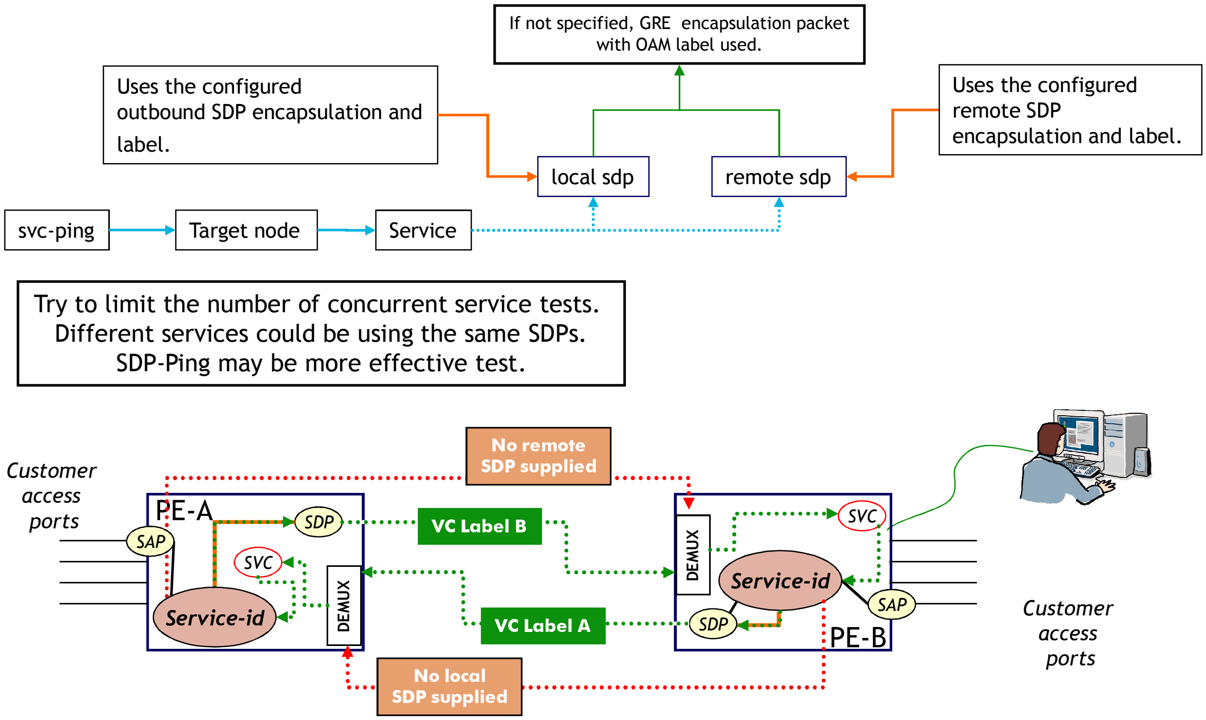


- **Originating SDP ID:** The SDP-ID to be used by SDP-Ping. The far-end address of the specified SDP-ID is the expected **responder-id** within each reply received. The specified SDP-ID defines the encapsulation of the SDP tunnel encapsulation used to reach the far end, IP/GRE or MPLS.
- **Responding SDP ID:** Optional parameter is used to specify the return SDP-ID to be used by the far-end for the message reply for round trip SDP connectivity testing.
- **Forwarding Class Name:** The forwarding class of the SDP encapsulation. The state can be specified as in or out-of-profile.
- **Timeout:** The amount of time that the device will wait for a message reply after sending a message request.
- **Interval:** Defines the minimum amount of time that must expire before the next message request is sent.
- **Size:** OAM message size in octets.
- **Count:** The number of messages to send. Each message request must either timeout or receive a reply before the next message request is sent. The message interval value must be expired before the next message request is sent.

Note

You can terminate an SDP-Ping test from the CLI using the Ctrl-C keyboard combination.

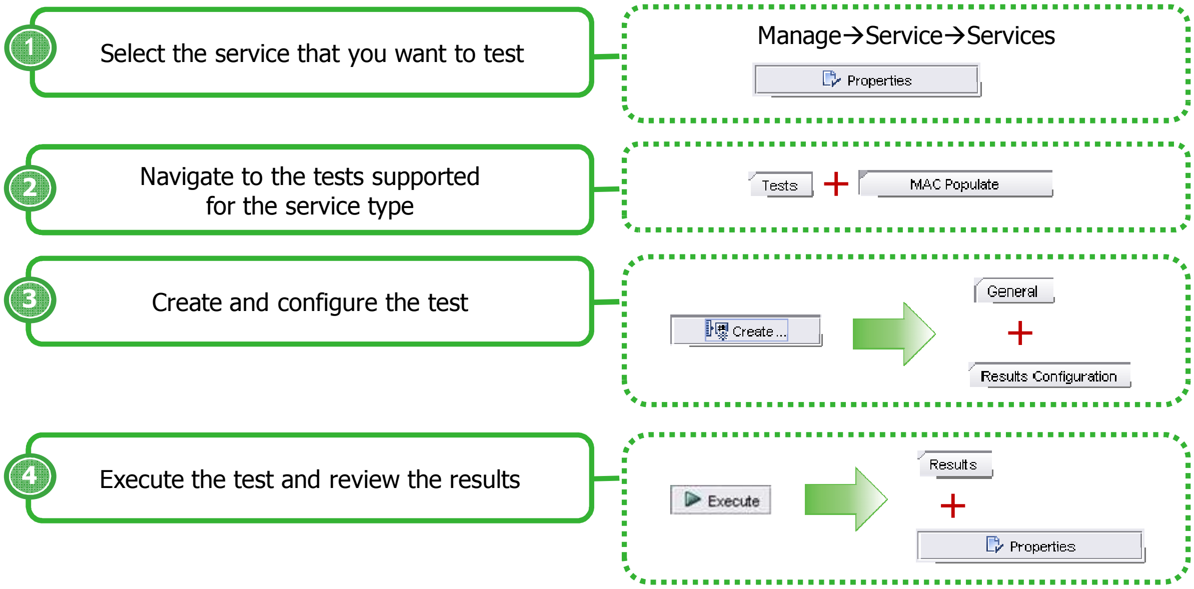
3.3 Service Ping (Svc-Ping)



Alcatel·Lucent UNIVERSITY

- **Far-End IP Address:** The far end IP address that the service ping packet will be sent to.
- **DNS-Name:** The Domain Name Server (DNS) name of the far end device that the service ping packet will be sent to.
- **Service-ID:** The service ID of the service being tested.
- **Local-SDP:** Specifies that the SVC-Ping request message should be sent using the same service tunnel encapsulation labeling as service traffic; IP/GRE or MPLS. If the local-SDP parameter is not used, the SVC-Ping message is sent using GRE encapsulation with an OAM label.
- **Remote-SDP:** Specifies that the SVC-Ping reply message from the far-end should be sent using the same service tunnel encapsulation labeling as service traffic. If the remote-SDP parameter is not used, the SVC-Ping reply message is sent using GRE encapsulation with an OAM label.

3.4 Service OAM validation workflow



Alcatel·Lucent UNIVERSITY

The workflow illustrated above describes the steps for a network administrator or operator to run an OAM diagnostic test on an existing service. The following information provides more specific details on the prerequisites for executing a test, and how a test can be used to troubleshoot a service. A VPLS is described in this example.

1. Create an MPLS network and LSPs for use by the service tunnels connecting the VPLS sites. Test the validity of the LSPs using LDP tree trace or LSP ping. If the results indicate a problem with the path, use LSP trace to check the specific MPLS path for the device causing the ping failure.

2. Create a service tunnel that uses the MPLS LSP created earlier and perform a tunnel ping on the service tunnel to verify tunnel connectivity. Create all tunnels necessary to interconnect the VPLS sites, and repeat the tunnel ping to ensure tunnel connectivity. After all of the tunnels are created, use the tunnel ping remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity.

3. Create a service using the service tunnels to interconnect the VPLS sites, either using mesh or spoke service tunnel bindings.
   Use a service site ping between each VPLS site device and its neighboring sites to verify service configuration consistency.

4. Connect the CPE devices to the VPLS and verify traffic.
   Use MAC trace from the edge devices to verify MAC address learning by the VPLS sites and to ensure that the correct associations are made between MAC addresses and the service tunnels or SAPs to which they are bound.
   Use MAC ping against an unknown MAC address to verify that no response is returned.
   Use MAC populate to create an OAM-specific MAC address. Use MAC ping and MAC trace against the created MAC address to verify that customer traffic is not affected by the additional MAC address.
   Use MAC purge to remove the created OAM MAC address.

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to perform OAM service diagnostics

Lab Exercises
Create OAM diagnostic tests for a Virtual Private LAN Service (VPLS)
Create OAM diagnostic tests for a Virtual Leased Line (VLL)

Time allowed: TBD

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

End of module
OAM Diagnostics

Alcatel·Lucent
UNIVERSITY

Section 5
Service and Network Tests

Module 1
Service Test Manager

TOS36042_V3.0-SG-English-Ed1 Module 5.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, the student will be able to:

- Explain the purpose of the Service Test Manager;
- Explain the function of the Test Policy and Test Suite;
- Identify and explain the function of Test Groups;
- Identify user scope of command.

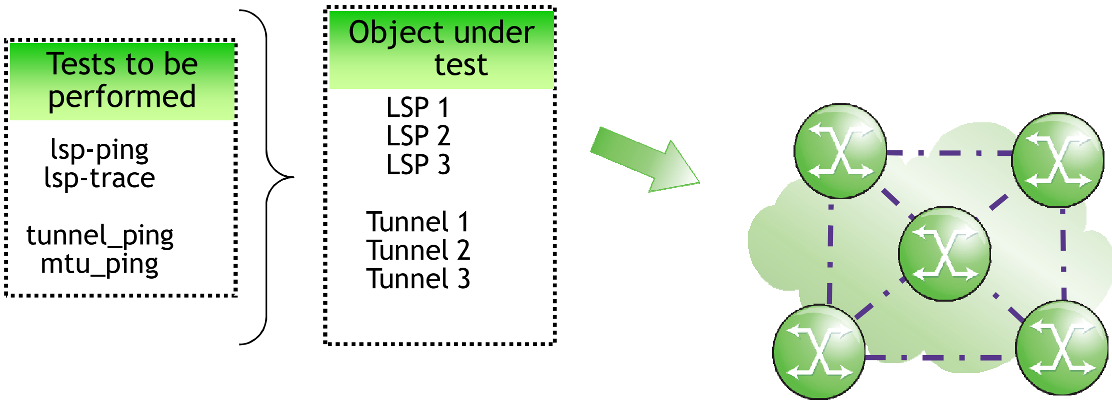
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Service Test Manager

1.1 Service Test Manager Overview



- Group OAM tests into Test Suites
- Useful for troubleshooting and SLA compliance
  - *Scheduled for continual performance feedback*
  - *On demand for investigative purposes*
- May be configured with threshold-crossing alarms

The 5620 SAM service test manager (STM) system provides the ability to group various OAM tests into test suites for network troubleshooting and for verifying compliance with SLAs. You can schedule the execution of a test suite to provide continual performance feedback, or run a test suite on demand to investigate service issues. The test results are logged for monitoring and trend analysis.

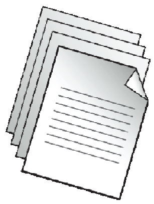
The grouping of tests into a test suite allows a 5620 SAM operator to use one schedule for the periodic execution of multiple OAM diagnostics against multiple network objects; for example, services, NEs, or transport components. They may choose to include existing tests, use the 5620 SAM to generate the tests that comprise a test suite, or both. Groups of tests in a suite can be configured to execute sequentially or concurrently. In addition, you can configure a test suite as an OAM validation test to verify the operational status of a service.

Threshold-crossing parameters can be configured to generate alarms when rising or falling threshold values are reached due to time-to-live failures, latency, or jitter issues discovered by the OAM tests.

Technical References

See Alcatel-Lucent 5620 Service Aware Manager, User Guide, Section 78 – Service Test Manager for detailed information including; policy overview, create and assign policies and policies procedures.

1.2 Test Policy and Test Suite



Test Policy

- *Contains a set of test definitions and pre- and post-processing rules*
- *Can be configured to display test results only if a test fails or generates a threshold crossing alarm*
- *Specific to one suite*

Test Suite

- *Defines network entities (objects) to be tested*
- *Three groups of tests: First Run, Generated, and Last Run*
- *Specifies the order of execution for tests*
- *Associated to one policy*

A test policy contains a set of test definitions and pre- and post-processing rules. A test policy is specific to one type of entity; for example, a VLL service or service tunnel. The test definitions in the policy are restricted to the tests that apply to the entity type specified in the policy. A test policy is applied to a test suite during test suite creation.

Test policy parameters can be configured to display test results only if a test fails or generates a threshold crossing alarm. In large networks, this can substantially reduce the amount of test data that the 5620 SAM needs to collect.

A test suite contains a set of network entities, or objects, that are to be tested. There are three (3) groups of tests within a test suite that define the order in which tests will be executed. Groups of tests in a suite can be configured to execute sequentially or concurrently.

A test suite may be associated to one policy, only.

1.3 Test Suite Test Groups

First-run tests

- First tests executed in test suite
- Chosen from list of existing tests
- Typically, high-level test, such as service ping

Generated tests

- Created by 5620 SAM against particular network entity
- Network entity based defined in Test Policy
- Regenerate tests if entity configuration changed

Last-run tests

- Executed after tests in the other groups
- Chosen from list of existing tests
- Typically, transport-layer test, such as LSP Ping

A test suite contains three test groups:

- First-run tests
- Generated tests
- Last-run tests

First-run tests are the tests in a suite that the 5620 SAM executes before the tests in the other groups. First-run tests are chosen from a list of existing tests and might typically include high-level diagnostics; for example, a service site ping or VPRN ping. No restrictions apply to the types of tests that are selectable as first-run tests.

Generated tests are created by the 5620 SAM for use against a particular network entity, based on the entity type specified in the suite and the specific tested entities that are named in the associated test policy. For example, a service site ping test policy associated with a three-site VPRN test suite causes the 5620 SAM to generate six tests: one site ping test from each site in the VPRN to the other two sites. When you change the configuration of a network entity, such as a service, you must regenerate the generated tests that apply to the entity. Test regeneration removes previously generated tests from a test suite.

Last-run tests are the tests in a suite that the 5620 SAM executes after the tests in the other groups. Last-run tests are chosen from a list of existing tests and might typically include transport-layer diagnostics; for example, an LSP trace or a tunnel ping. No restrictions apply to the types of tests that are selectable as last-run tests.

1.4 Test Execution

Scheduled

Periodic execution of multiple OAM diagnostics against multiple network objects

Execute

Run a test suite on demand to investigate service issues.

The execution of a test suite can be scheduled to provide continual performance feedback, or run a test suite on demand to investigate service issues. The test results are logged for monitoring and trend analysis.

1.5 User Scope of Command

admin or QoS/ ACL

Create and modify all tests, test policies and test suites

Service management

Create and modify STM components related to services

Topology management

Create and modify STM components related to network transport such as LSPs and service tunnels

A 5620 SAM user that is assigned the admin or QoS/ACL management scope of command role can create and modify all tests, test policies, and test suites. A user that is assigned the service management scope of command role can create and modify only STM components that are related to services. A user that is assigned the topology management role can create and modify only STM components that are related to network transport elements.

Knowledge Verification – Service Test Manager

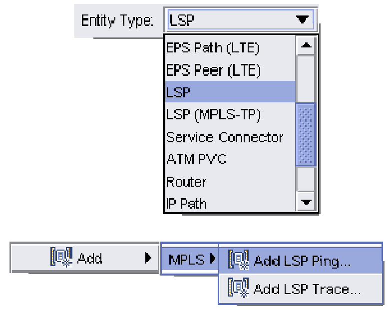
Which of the following items is **not** a characteristic of a Test Policy.

a. Contains a set of test definitions and pre- and post-processing rules
b. Can be configured to display test results only if a test fails or generates a threshold crossing alarm
c. Specific to one suite.
d. Defines network entities (objects) to be tested.

Choose the correct answer for the knowledge verification question above.

1.6 Generated STM configuration workflow

1. Initiate the creation of the test policy — Tools→Service Test Manager (STM)→ Create→Test Policy
2. Define the test policy



3. Initiate the creation of the test suite — Tools→Service Test Manager (STM)→ Create→Test Suite

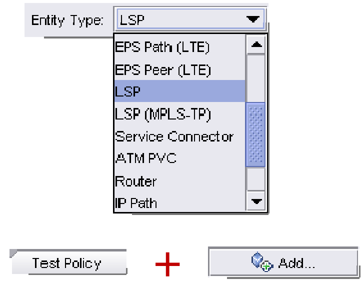
The workflow illustrated above describes the steps for a network administrator or operator to configure a generated STM test.

As a prerequisite for creating a VPLS service, this workflow assumes the following:

- a group or customer with the required user access privileges has been configured.
- the IP or IP/MPLS core network exists
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel
- the access ports for the service are created
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured

1.6 Generated STM configuration workflow [cont.]

4 Define the test suite



5 Launch tests

Generate Tests

6 Create a schedule

Tools→Schedule→Schedule→Create

7 Assign the schedule to the test suite

Tools→Service Test Manager (STM)

Properties + Schedule...

Alcatel·Lucent
UNIVERSITY

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to run a generated STM tests

Lab Exercises
Configure a generated STM test

Time allowed: TBD

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

This page is left blank intentionally

End of module
Service Test Manager

Alcatel·Lucent
UNIVERSITY

Section 5
Service and Network Tests

Module 2
Service Throughput Tests

TOS36042_V3.0-SG-English-Ed1 Module 5.2 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you will be able to:

- Describe the function of a Service Throughput Test
- Explain the port option for the test
- Describe the required environment for the test
- Identify node and service types that support the feature
- Explain the workflow for how to implement a test

Alcatel·Lucent UNIVERSITY

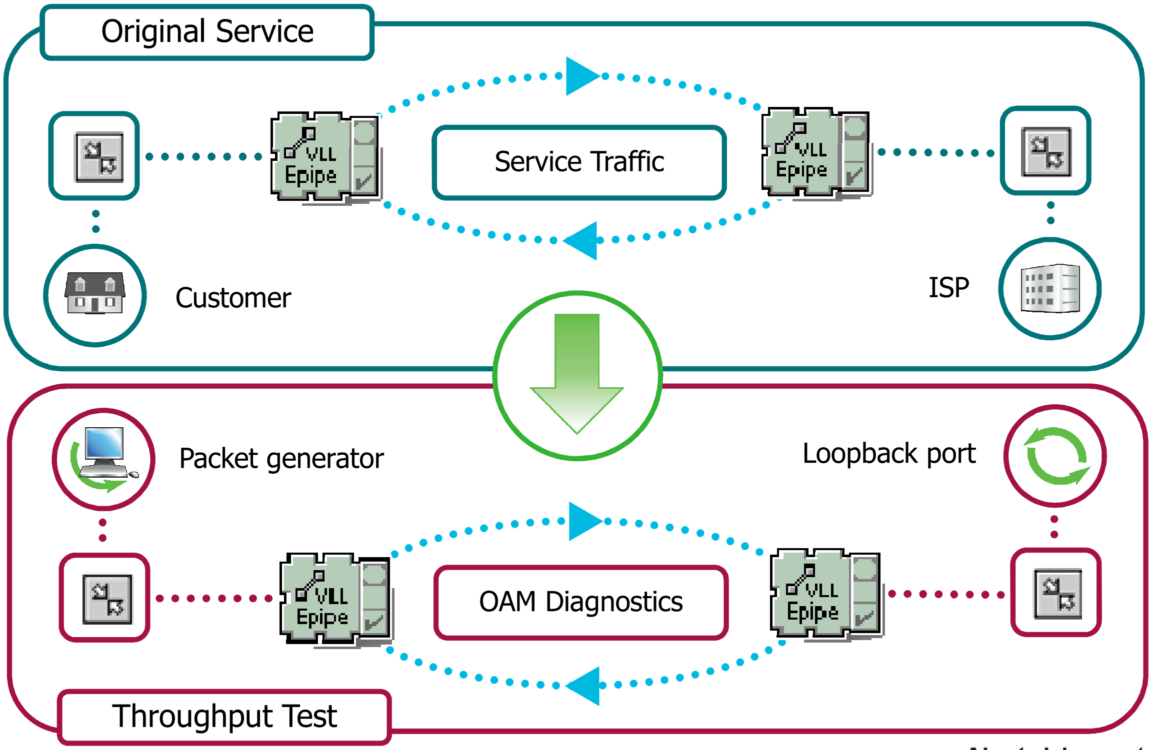
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Service Throughput Test

1.1 Service Throughput Test overview



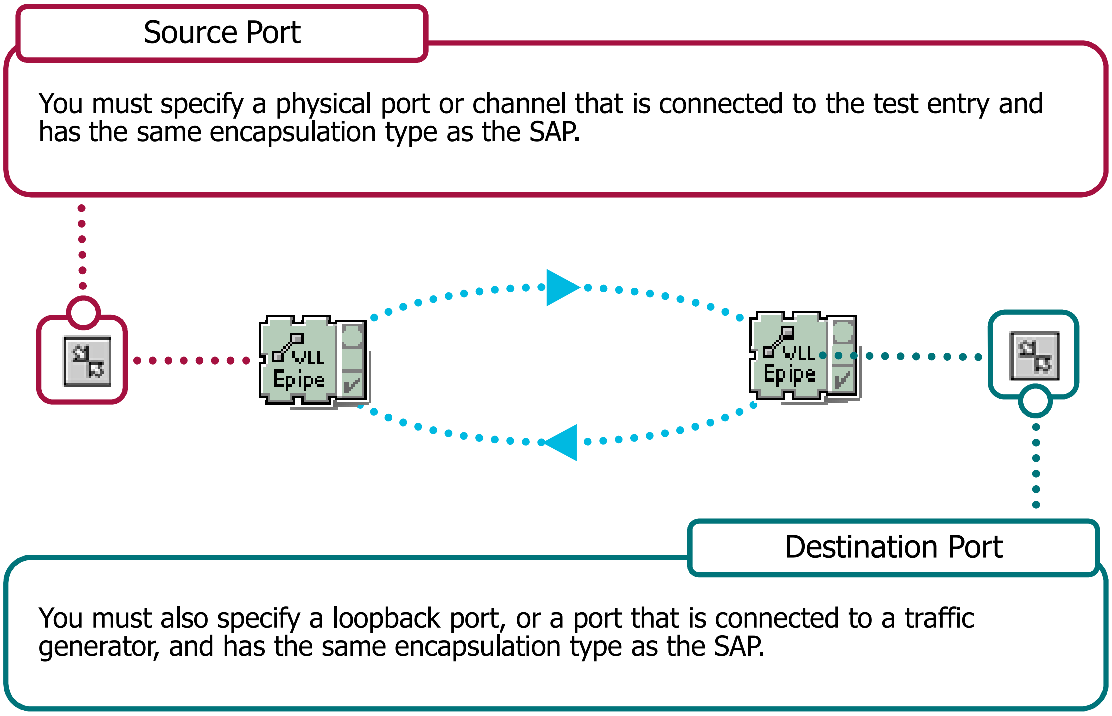
Alcatel·Lucent UNIVERSITY

You can emulate a customer service, in which you perform OAM diagnostics to test conformance with the customer SLA.

The 5620 SAM allows you to create a copy of the SAP configuration of an end-user service that emulates the bandwidth, throughput, and QoS requirements of the service. You can perform any required OAM diagnostics on the service while sending the traffic through the NEs, to compare the customer SLA with current measurements and report the results.

The 5620 SAM operator can prepare a throughput test between two endpoints of a service or composite service using an external test packet generator, in combination with the SAP loopback function. This can be done by temporarily moving one or two SAPs to the new ports. One of the new temporary SAPs can be used to inject packets, while the other temporary SAP can be in loopback mode. When the test is completed, the operator can easily restore the service by clicking a button in the GUI. The service throughput test preparation can be initiated and restored from the service list or the service form itself.

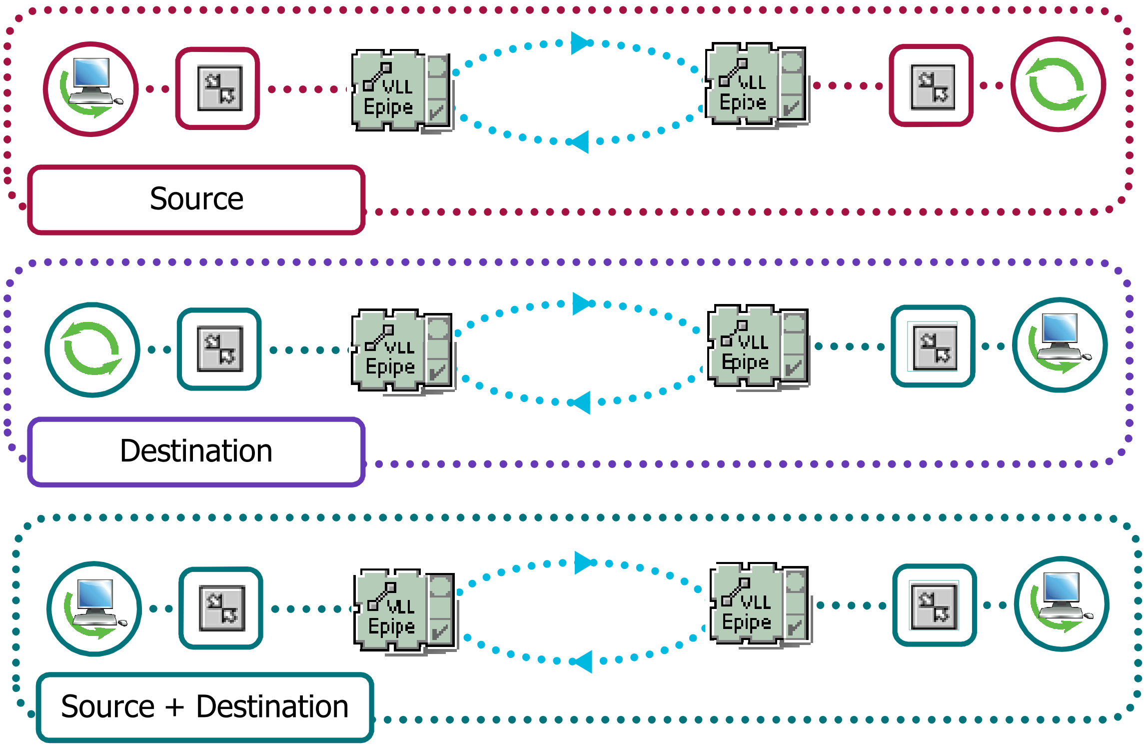
1.2 Port options for the Service Throughput Test



Alcatel·Lucent UNIVERSITY

By default, the displayed source and destination ports are the underlying ports of the selected SAPs. If you do not use the default ports, the 5620 SAM creates a SAP on the selected port by copying the configuration from the original SAP during the test preparation. E-OAM objects are not copied to the SAP.

1.3 Options for the location of packet generator



Alcatel·Lucent UNIVERSITY

You can put the traffic generator on the source SAP, destination SAP, or both the source and destination SAPs if you are troubleshooting directional faults in your network.

1.4 Considerations for Service Throughput Test environments

The SAP to be replaced must reside under a Epipe site, including PBB Epipes, or a VPLS site including I-VPLS and B-VPLS.

The following SAPs are not supported for the throughput test:

- CCAGs
- LAGs
- SAPs that reside on an Ethernet tunnel element
- SAPs that reside on an Ethernet ring element
- SAPs used by a mirror service

You can prepare only one test for each service. If a service is a member of a composite service and is modified for a throughput test, you cannot prepare a new test on the associated composite service.

E-OAM objects, such as MEPs, are not copied to the test SAP.

Knowledge Verification – valid test configurations

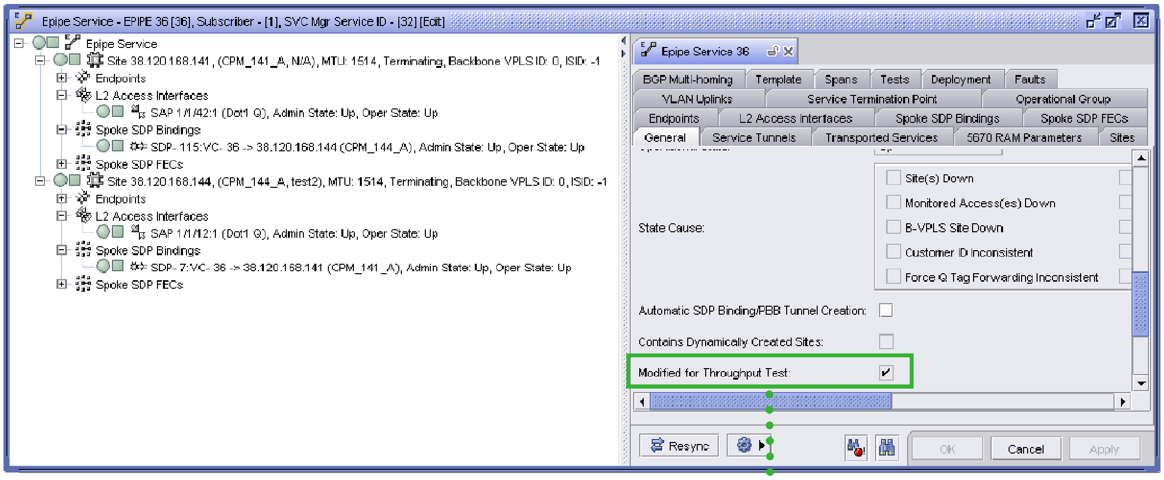
Which one of the following options is not a valid configuration for service throughput tests.

a. Source = traffic generator, destination = loopback.
b. Source = loopback, destination = traffic generator.
c. Source = loopback, destination = loopback.
d. Source = traffic generator, destination = traffic generator.

Alcatel·Lucent
UNIVERSITY

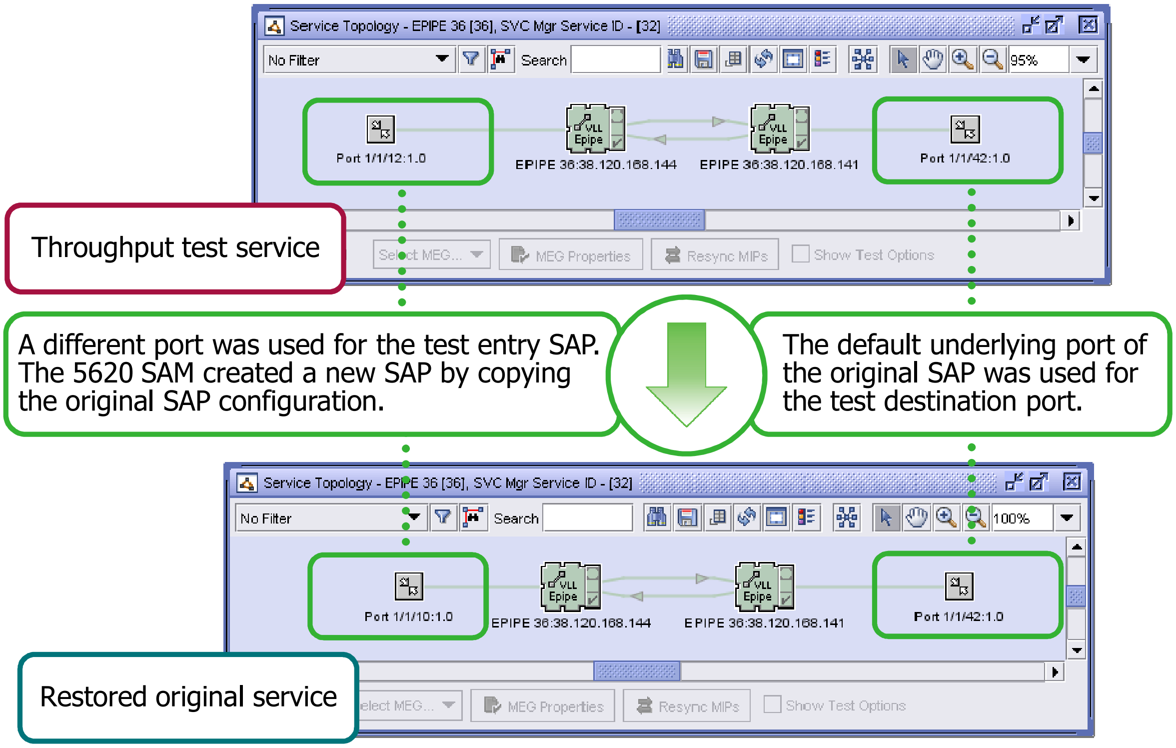
Choose the correct answer for the knowledge verification question above.

1.5 Service status during throughput test



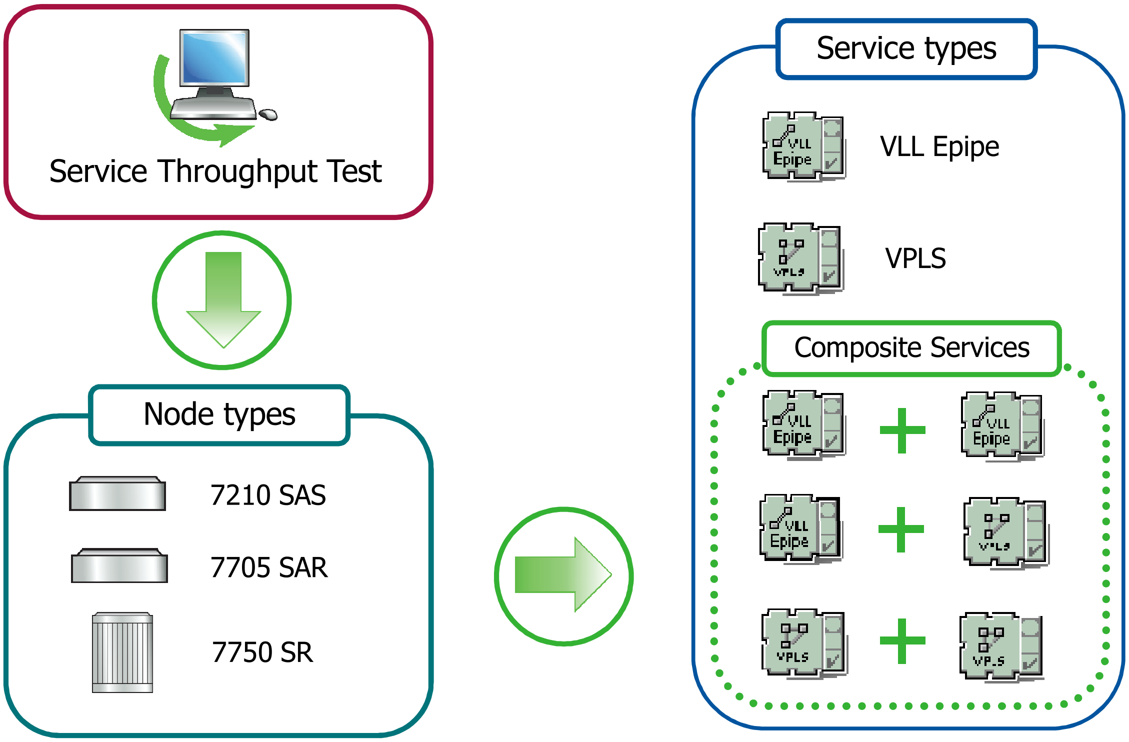
The service properties form identifies if the service is modified for a throughput test.

1.6 Review the restored service on the topology map (optional)



Alcatel·Lucent UNIVERSITY

1.7 Service Throughput Test support



Throughput tests are supported on the 7210 SAS, 7705 SAR, and 7750 SR, on VLL Epipe, VPLS and composite services that contain an Epipe service, a VPLS or both.

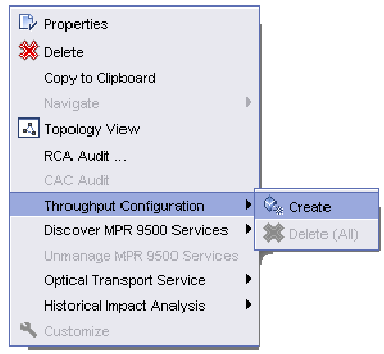
1.8 Workflow to prepare/restore a service throughput test

1. Open the service on which you need to create the test environment.

   Manage → Service → Services → Properties

2. Set the Current OLC State parameter to Maintenance.

3. Initiate the creation of the test



Alcatel·Lucent UNIVERSITY

The above workflow describes the high-level tasks required to prepare a throughput test. The workflow assumes that a 5620 SAM end user is challenging the offered SLA. You can use the VLL service throughput lab in conjunction with the lab for VLL OAM diagnostics.

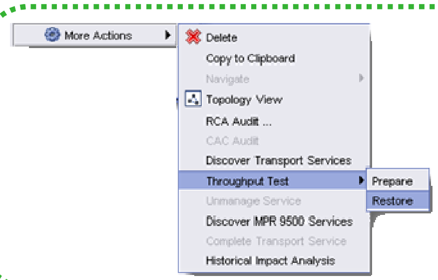
1.8 Workflow to prepare/restore a service throughput test [cont.]

4. Configure the test

5. Perform the OAM diagnostics

Not part of this lab exercise; see VLL OAM lab

6. Restore the service to the original configuration



7. Set the Current OLC State parameter to In Service

How To Do It and Exercises

How to do it
Instructor demonstration on how to use the 5620 SAM GUI to prepare a service throughput test

Lab Exercises
Create a service throughput test

Time allowed: 15

Alcatel·Lucent
UNIVERSITY

Your instructor may perform the above mentioned demonstrations using the 5620 SAM GUI.

In addition, your instructor will point out the appropriate lab module containing the above mentioned hands-on lab exercises, and will indicate the time allowed to perform these hands-on exercises.

This page is left blank intentionally

End of module
Service Throughput Tests

Alcatel·Lucent UNIVERSITY

Section 5
Service and Network Tests

Module 3
RCA Audit

TOS36042_V3.0-SG-English-Ed1 Module 5.3 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you will be able to:

- Explain the purpose of the RCA audit process
- Identify the RCA audit types

Alcatel·Lucent UNIVERSITY

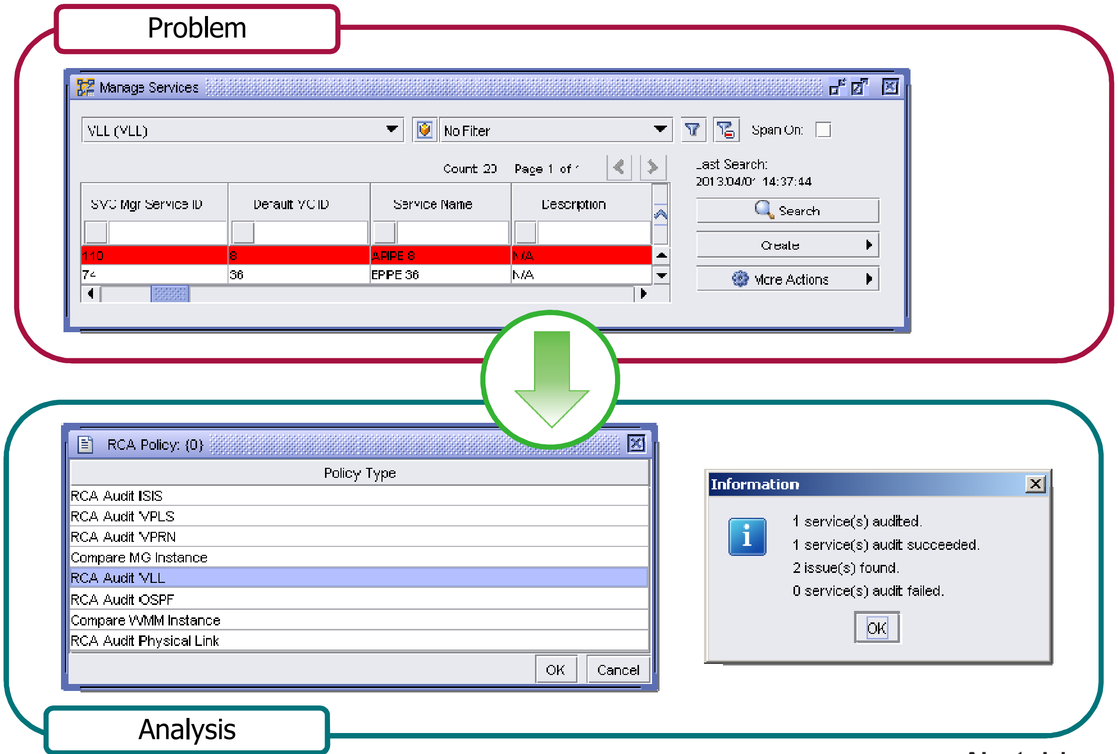
This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 RCA Audit

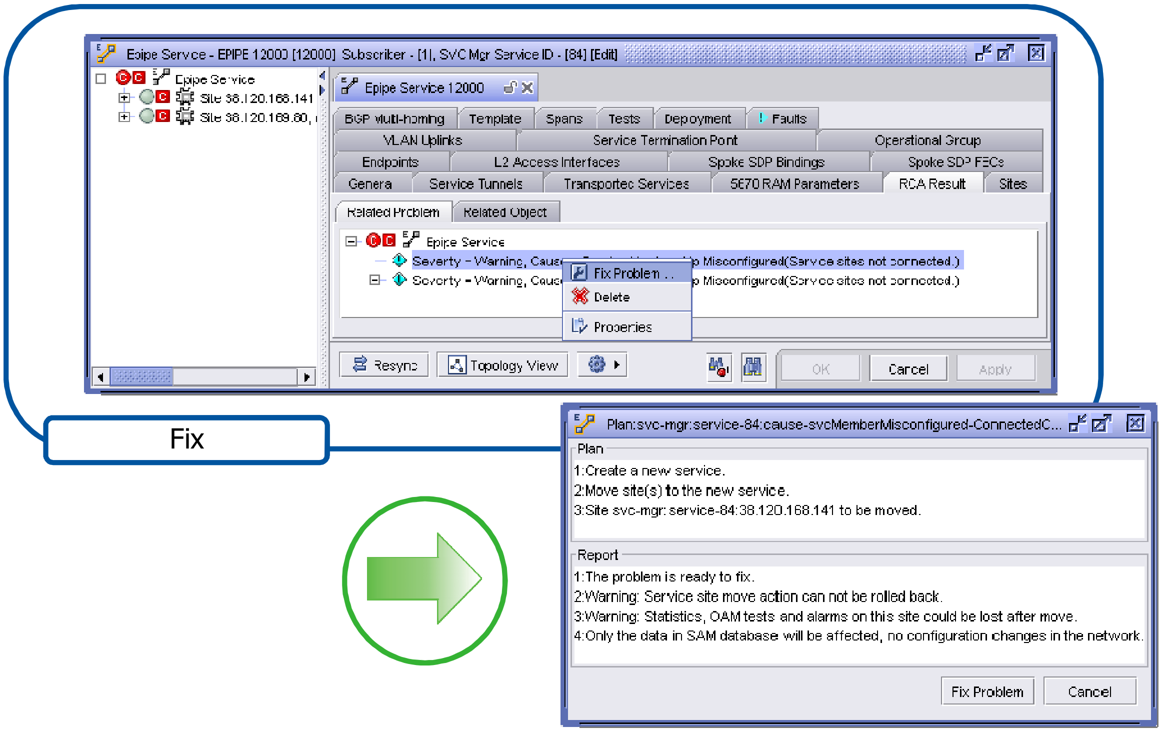
1.1 RCA audit process



Alcatel·Lucent UNIVERSITY

The 5620 SAM RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems.

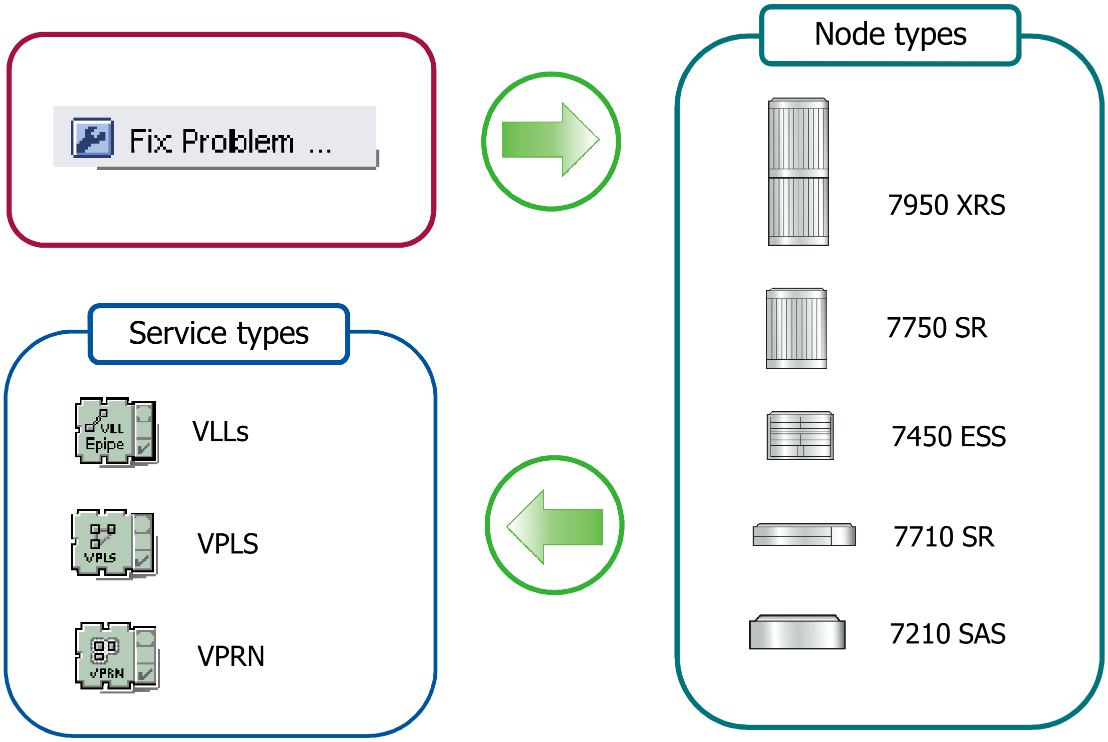
1.1 RCA audit process [cont.]



Alcatel·Lucent UNIVERSITY

Except for physical links, the 5620 SAM provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes. The adjustments are made only to the 5620 SAM database and are not deployed to the network.

1.2 Support for RCA service audits



Alcatel·Lucent UNIVERSITY

The 5620 SAM supports RCA audits for VLL, VPLS, and VPRN services on the following node types:

- 7950 XRS
- 7750 SR
- 7450 ESS
- 7710 SR
- 7210 SAS-M 24F,
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X24F2XFP
- 7210 SAS-E

RCA audit policies allow you to modify the component membership of your 5620 SAM services to detect possible configuration problems. In addition, you can use the RCA audit to correct most configuration problems that are discovered in the audit.

A 5620 SAM user that is assigned the Administrator or RCA scope of command role can create, modify, and execute all RCA audit policies. A 5620 SAM user that is assigned the Administrator or Service scope of command role can execute service audit adjustments.

1.3 Support for RCA physical link audits

The 5620 SAM RCA audit tool allows you to identify configuration errors in physical links. The 5620 SAM does not provide a solution for configuration problems that the RCA audit identifies for physical links.

Physical port parameters

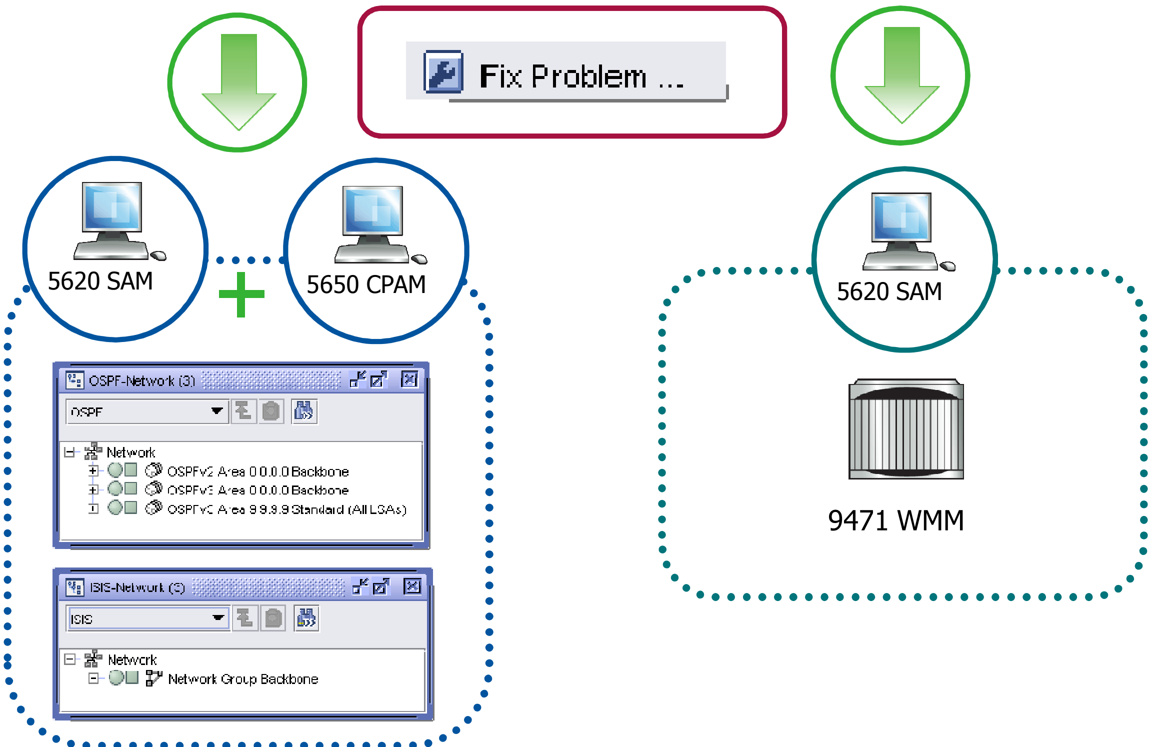
- Mismatched MTU values
- Mismatched speeds

Ethernet port parameters

- Auto-negotiate parameter misconfiguration
- Duplex parameter misconfiguration

Physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the equipment window, physical topology map, and the Manage Equipment list form. Because several key parameters on each end of the physical link depend on each other, configuration errors are possible. The 5620 SAM RCA audit tool allows you to identify configuration errors in physical links. The 5620 SAM does not provide a solution for configuration problems that the RCA audit identifies for physical links.

1.4 RCA audit support for routing protocols and network instance



The 5620 SAM supports RCA audits for the following routing protocols and network instances:

- OSPF interfaces, areas, and area sites (5620 SAM/5650 CPAM integration only)
- IS-IS interfaces and sites (5620 SAM/5650 CPAM integration only)
- 9471 WMM instances and golden configurations

Technical References

You require a 5650 CPAM license to perform the OSPF and IS-IS RCA audits. See the 5650 CPAM User Guide for more information.

You can use the 9471 WMM golden configuration function of the 5620 SAM to capture 9471 WMM configuration states and perform RCA audits in order to identify any MME and SGSN object parameter values that no longer match their equivalents in the specified golden configuration. Audits can validate multiple NEs simultaneously, and can be performed manually or scheduled. Golden configurations cannot be deployed to NEs for provisioning.

Technical References

See the 5620 SAM LTE ePC User Guide for information about performing golden configuration RCA audits on 9471 WMM instances.

Knowledge Verification – manual vs. dynamic services

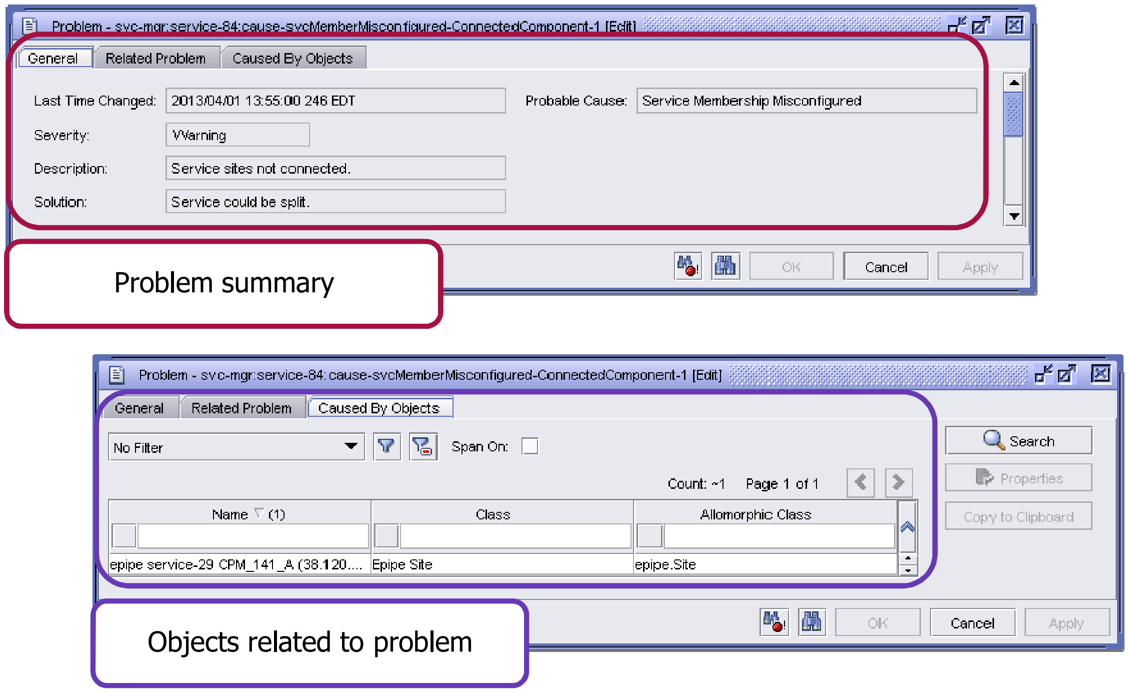
Which one of the following options do you need the 5650 CPAM, in conjunction with the 5620 SAM, to perform an RCA audit.

a. VPRN services.
b. Ethernet ports.
c. 9471 WMM network elements.
d. OSPF interfaces, areas, and area sites.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.5 Viewing the results for an RCA Audit



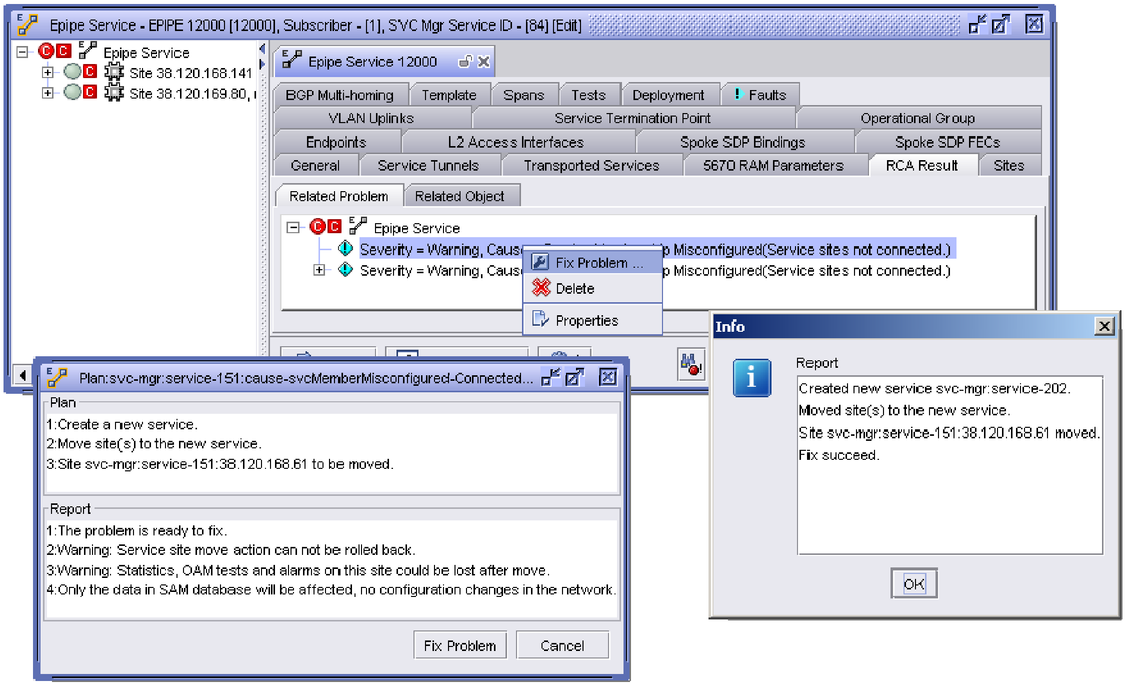
Alcatel·Lucent
UNIVERSITY

The properties form of a problem displays the following information:

- problem severity
- probable cause
- description
- solution

The Caused By Objects tab lists the network objects that caused the problem. For service audits, the sites that should be moved out of a service, and the service they should move to, if there is only one destination service, are listed. If only one group of sites is listed, a new service is created and the sites are moved to the created service.

1.6 Reviewing and implementing the proposed fix for the problem

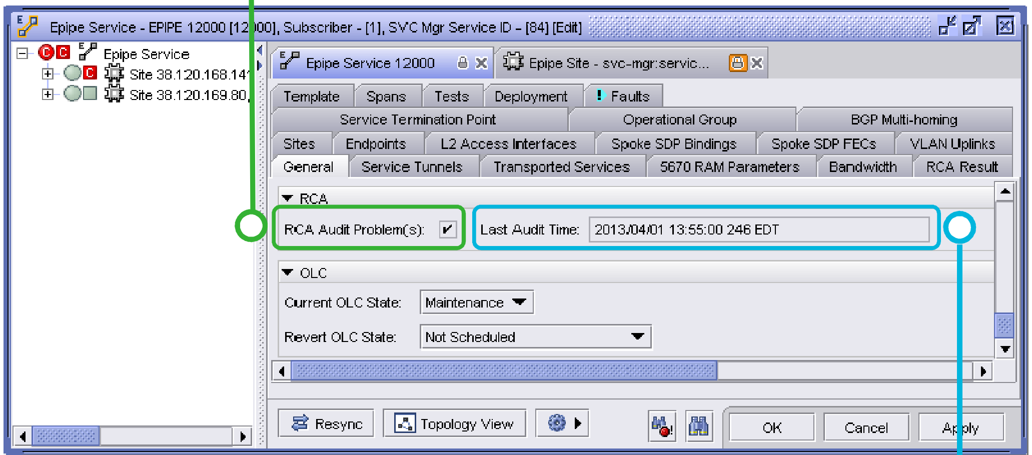


Alcatel·Lucent UNIVERSITY

You can use the RCA audit tool to correct a detected configuration problem from the RCA Result tab on the network object properties form. The 5620 SAM lists the operations to fix the problem. A summary of the correction operation that the 5620 SAM implemented appears when you accept the proposed solution. To view the result in the server or client log, you must enable the logging option in the nms-server.xml or nms-client.xml file. Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

1.7 Viewing previous RCA audit status

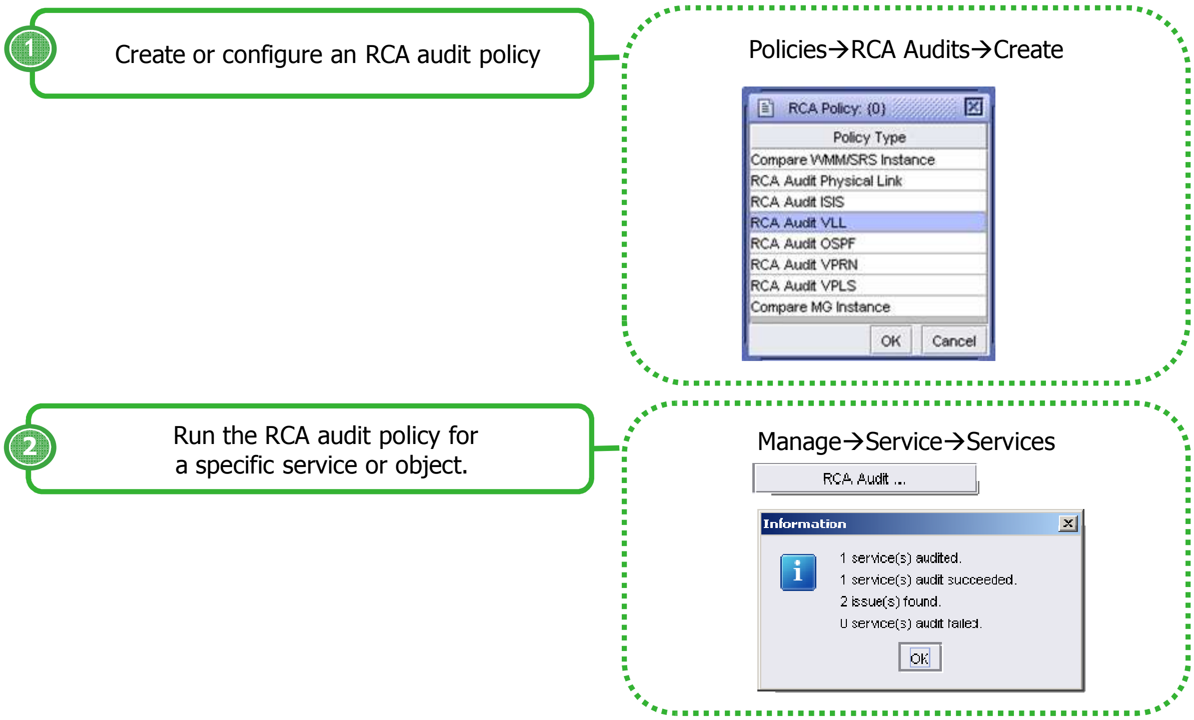
The RCA Audit Problem(s) indicator on the General tab of a network object properties form identifies whether configuration problems were detected in previous audits.



The Last Audit Time indicator displays a timestamp of the last audit that was performed.

Alcatel·Lucent UNIVERSITY

1.8 Workflow to configure RCA audit



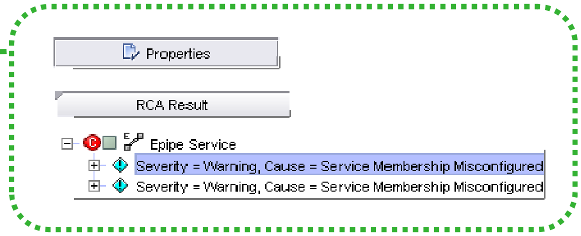
The above workflow describes the high-level tasks required to configure RCA audit for a service or physical link.

In particular, the lab shows how to perform an RCA audit on a VLL service. Consider the following when you perform an audit of a VLL service.

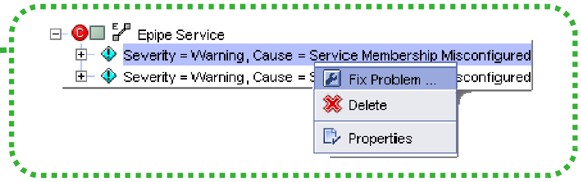
- Service sites with different customer IDs are discovered as two services, and can reconfigured as one service.
- More than two groups of sites that are connected can be detected and can be separated into different services.
- Redundant VLLs are not be affected by the audit and are considered correctly configured.
- If two Epipe sites are connected to the same PBB with same B-VPLS service ID, and the source and destination MAC addresses match, the 5620 SAM determines that the two sites are connected. If they are in different 5620 SAM services, a problem is generated during the audit.

1.8 Workflow to configure RCA audit [cont.]

3 Identify the problems and view the suggested solutions



4 Implement the changes, as required



Alcatel·Lucent UNIVERSITY

End of module
RCA Audit

Alcatel·Lucent
UNIVERSITY

Section 6
Templates

Module 1
Service and Tunnel Templates

TOS36042_V3.0-SG-English-Ed1 Module 6.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to describe:

- Explain features and benefits of templates
- Identify the role of the XML API in the template process
- Identify the template types
- List template management tasks
- Explain how to browse template examples
- Describe how to configure node-specific configuration parameters
- Identify the workflow for how to manage XML API templates

Alcatel·Lucent UNIVERSITY

This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Templates

1.1 Template overview

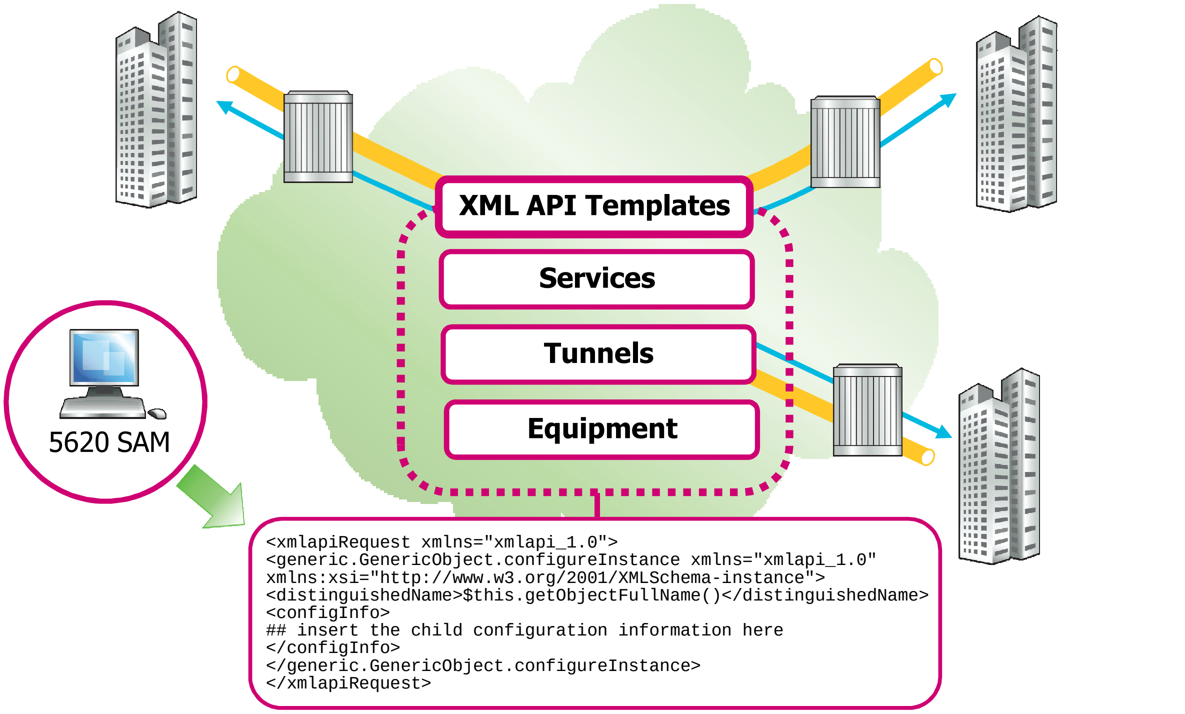
Features and benefits

A template is an object managed by the 5620 SAM that is used as a starting point for configuring complex managed objects such as services and tunnels.

Templates allow users to define common characteristics that can be shared by multiple managed objects by associating them with a template instance at creation time.

Service templates facilitate service creation, including the service itself and sub-components such as service sites, access interfaces, and SDP bindings.

1.2 Templates and the role of XML API



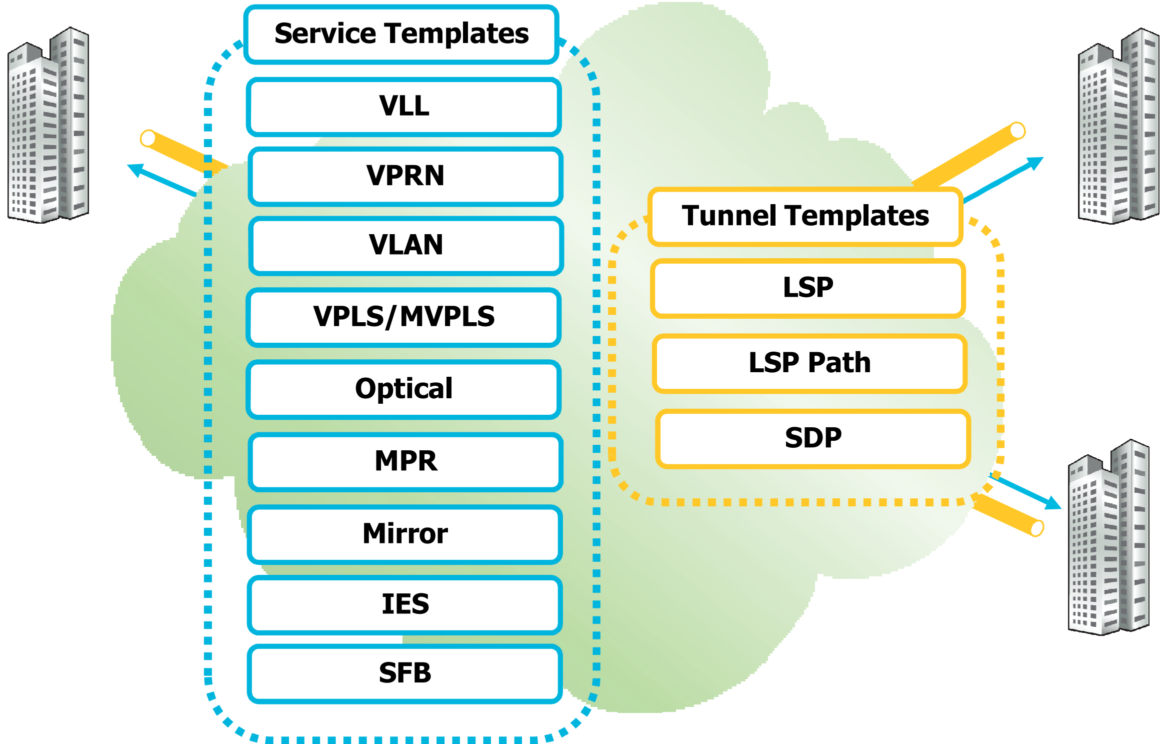
The XML API configuration templates simplify tunnel and service creation or modification by reducing the steps required to create or modify a tunnel or service component. You can use an existing tunnel or service as a starting point to create an XML API template or you can also create a template without using a managed tunnel or service object as a basis.

For tunnel and service template configuration, the 5620 SAM generates an XML API script with Velocity properties which you must modify to generate a UI for the configuration form that is tailored to your requirements and to NE-specific properties and attributes.

Note

Equipment template functionality allows for the creation of auxiliary alarm definitions, which is specific to the 7705 SAR auxiliary alarm daughter card.

1.3 Template types



Alcatel·Lucent UNIVERSITY

Service template configuration supports the configuration of multiple service types using XML API script-based templates.

Tunnel templates allow users to automate the creation and modification of dynamic LSPs, LSP paths, and SDPs as routers and topology changes in the network. You can create XML API configuration templates for LSP and SDP tunnels and child objects of tunnels, such as LSP paths. You can include object categories, class names, object types, and other tunnel-related objects.

Tunnel and service template configuration follows the same rules. The templates allow users to define common characteristics for a service or tunnel, or *templatable* service or tunnel object, and the parameter values that can be configured.

Knowledge Verification – Template creation

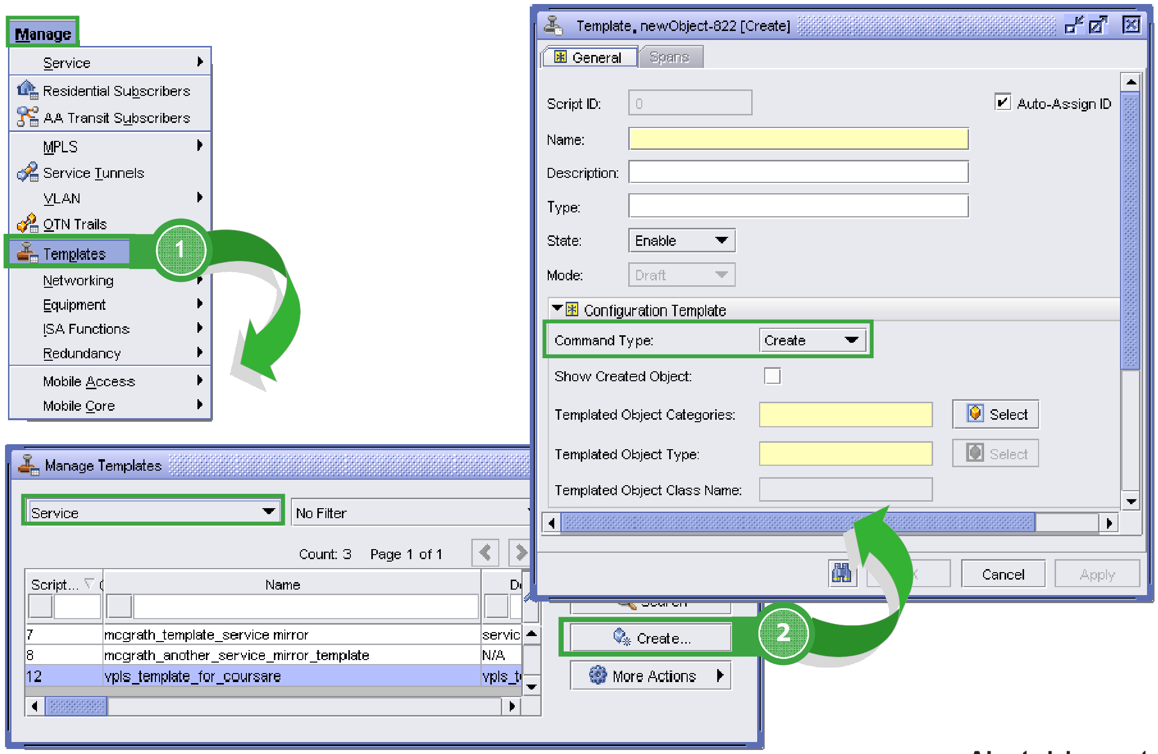
You cannot use an existing tunnel or service as a starting point to create an XML API template.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

1.4 Managing templates



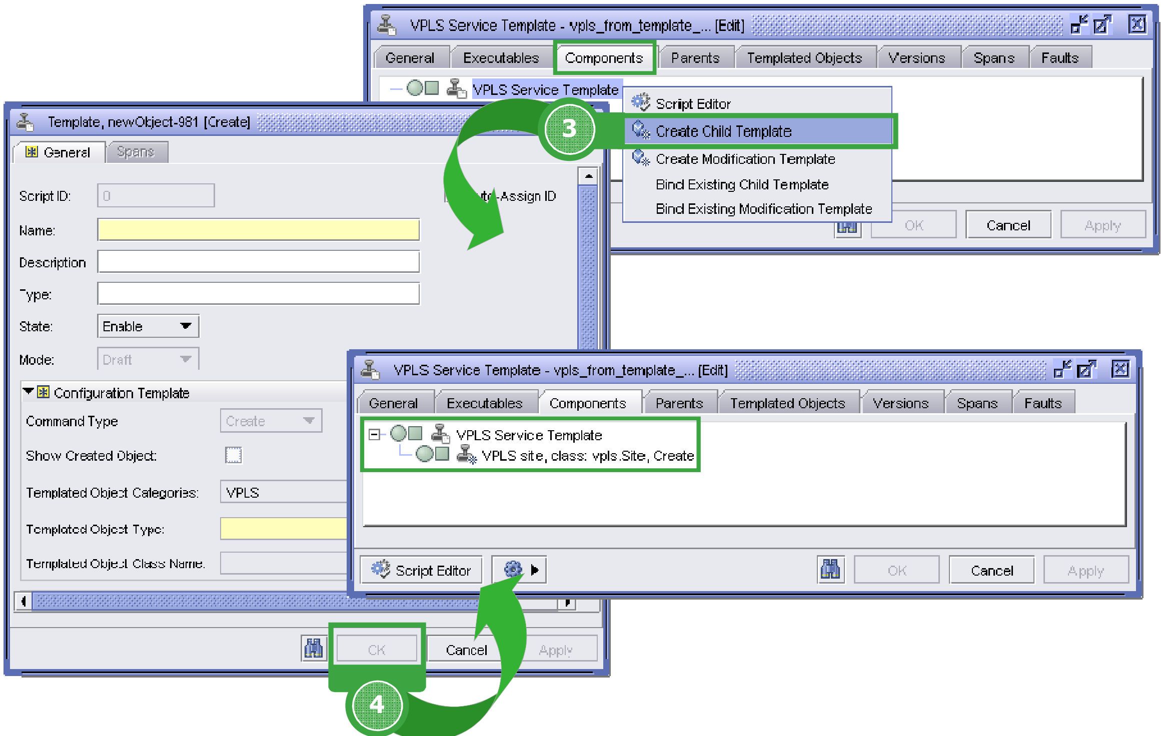
6 · 1 · 12
Templates · Service and Tunnel Templates
5620 SAM · Services Operations and Provisioning

Alcatel·Lucent UNIVERSITY

You can create, modify, or delete XML API configuration templates using the Manage Templates form. The form allows you view all templates for tunnels, services, sites, and templatable child network objects. You can also use the form to convert standard service templates that were created in earlier releases to XML API templates.

A configuration template can be used to create new network objects, or modify existing ones. You use the Command Type parameter to specify the type of template—creation or modification. Modification templates are secondary templates that can be bound to the creation templates. Multiple modification templates can be bound to multiple creation templates.

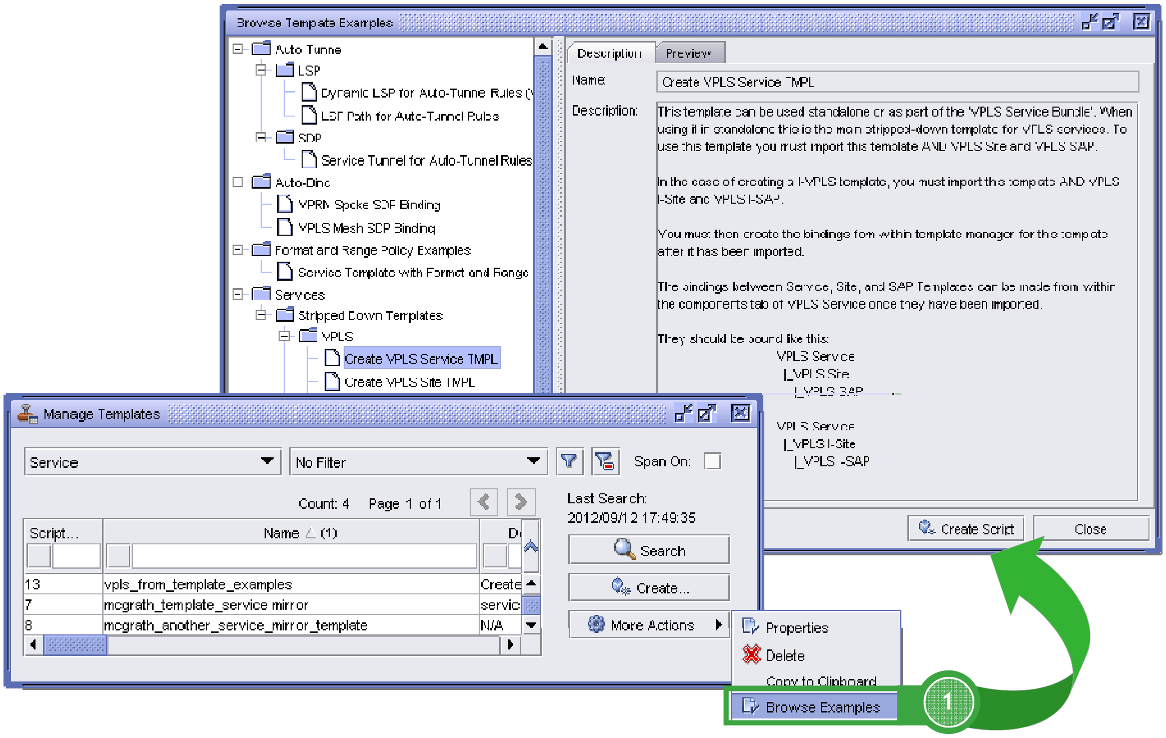
1.4 Managing templates [cont.]



Alcatel·Lucent UNIVERSITY

A service template can use secondary, or child, templates to further define the configuration information for the created service. Templates for sites can be bound to the service template. Network objects, such as SDP bindings and interfaces, are considered child templates which can be bound to the site template. Only site templates can be bound to service templates. When you create an XML API configuration template for a service, you can choose to create templates for child objects of the service and to bind the child templates to the service template. You can bind a child template to multiple parent templates. For example, a site template can be bound to several service templates.

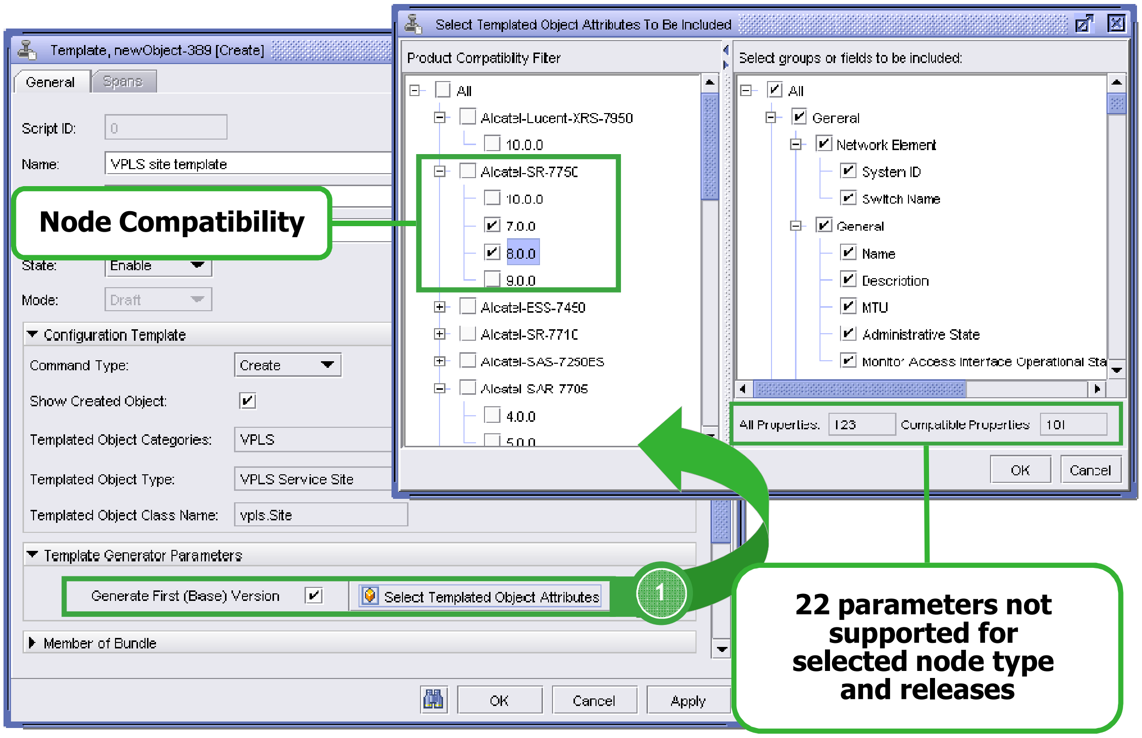
1.5 Browse template examples



Alcatel·Lucent UNIVERSITY

Service template examples provide a way for users to learn the procedures, practices and concepts that are required to configure XML API templates; for example, creating a VPLS service template. The preview tab allows you to view the example script.

1.6 Custom node-specific configuration parameters

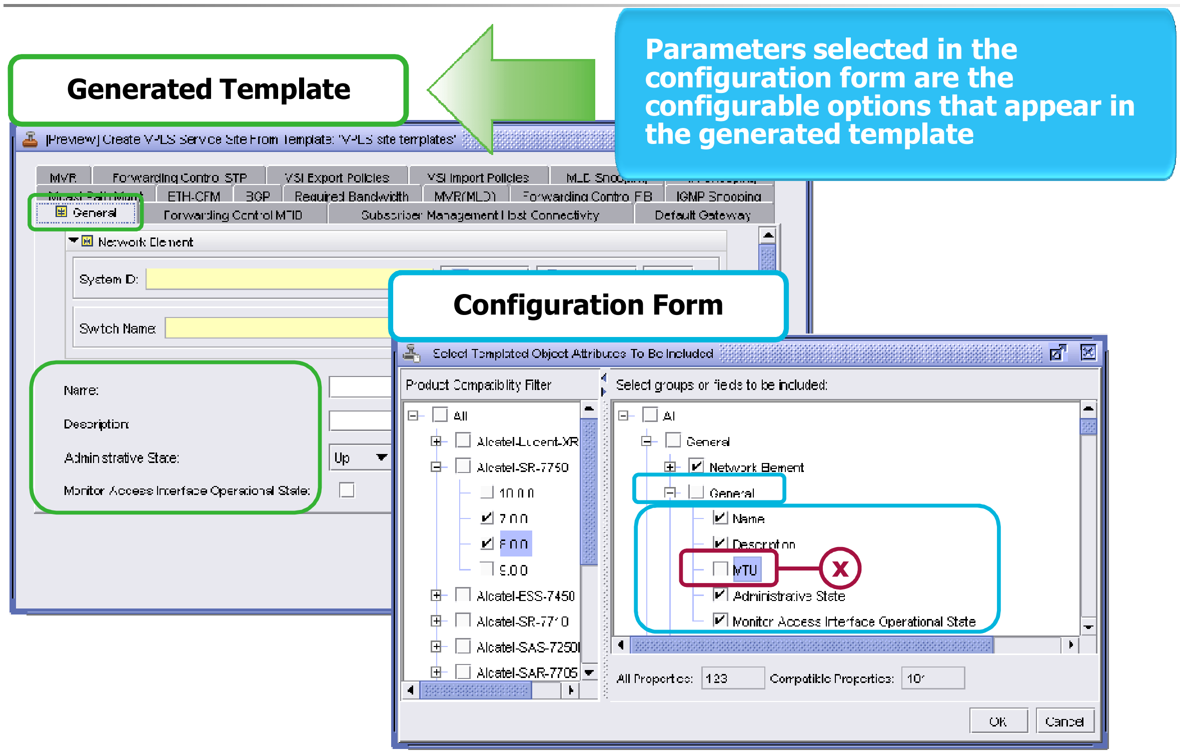


Alcatel·Lucent UNIVERSITY

The Parameter Selection Form allows users to specify the node release types and versions that are specific to the template. The generated template supports the configuration of parameters that are supported on all node release types and versions that are associated with the template. Any parameters excluded from the template but supported on the node can be configured using the object properties form.

The right pane allows users to manually specify which parameters are included in the template. The left pane allows you to specify the node types and releases that are compatible with the template. If a parameter is not available on one of the selected node releases, the parameter is excluded from the parameter selection list.

1.6 Custom node-specific configuration parameters [cont.]



Alcatel·Lucent UNIVERSITY

1.7 XML API template script format

Script example for creation template

```
<xmlapiRequest xmlns="xmlapi_1.0">
<generic.GenericObject.configureChildInstance xmlns="xmlapi_1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<deployer>immediate</deployer>
<distinguishedName>$parent.getObjectFullName()</distinguishedName>
<childConfigInfo>
## insert the child configuration information here
</childConfigInfo>
</generic.GenericObject.configureChildInstance>
</xmlapiRequest>
```

Script example for modification template

```
<xmlapiRequest xmlns="xmlapi_1.0">
<generic.GenericObject.configureInstance xmlns="xmlapi_1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<distinguishedName>$this.getObjectFullName()</distinguishedName>
<configInfo>
## insert the child configuration information here
</configInfo>
</generic.GenericObject.configureInstance>
</xmlapiRequest>
```


There are two types of templates: creation templates and modification templates. A creation template is used to create new objects, a modification template is used to modify an existing object.

Modification templates are secondary templates that can be bound to the creation templates. Multiple modification templates can be bound to multiple creation templates.

1.8 Workflow to manage XML API templates

1. Convert service templates created with the 5620 SAM, Release 5.0 or earlier, to XML API service templates. If required, you can delete old templates.
2. Create XML API service or tunnel templates.
3. Create an XML API site template for service templates, if required.
4. Create XML API templates for child network objects.
5. Bind an XML API site template to an XML API service template, if required.
6. Bind children network object XML API templates to XML API site templates.
7. Apply XML API tunnel templates to Auto tunnels, if required.

***DELETE

Alcatel·Lucent UNIVERSITY

Knowledge Verification – Template creation

The Parameter Selection Form allows users to specify the node release types and versions that are specific to the template.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

This page is left blank intentionally

End of module
Service and Tunnel Templates

Section 7
Service classification and Forwarding

Module 1
QoS Policy

TOS36042_V3.0-SG-English-Ed1 Module 7.1 Edition 1

5620 SAM
Services Operations and Provisioning
TOS36042_V3.0-SG Edition 1

Alcatel·Lucent
UNIVERSITY

This page is left blank intentionally

Document History			
Edition	Date	Author	Remarks
1.0	2012-10-12	MCGRATH, John	TOS36042_V1.0 – SAM 10.0 R1
1.1	2012-11-16	MCGRATH, John	TOS36042_V1.1 – SAM 10.0 R5
2.0	2013-04-10	MCGRATH, John	TOS36042_V2.0 First edition – SAM 11.0 R1
2.1	2013-08-16	MCGRATH, John	TOS36042_V2.0 Second edition – SAM 11.0 R1 (update)
3.0	2014-04-03	MCGRATH, John	TOS36042_V3.0 First edition – SAM 12.0 R1

Module objectives

Upon completion of this module, you should be able to explain:

- Quality of Service definition
- Requirement for Quality of Service
- Alcatel-Lucent QoS model

Alcatel·Lucent UNIVERSITY

This page is left blank intentionally

Table of Contents

This page is left blank intentionally

1 Quality of Service definition

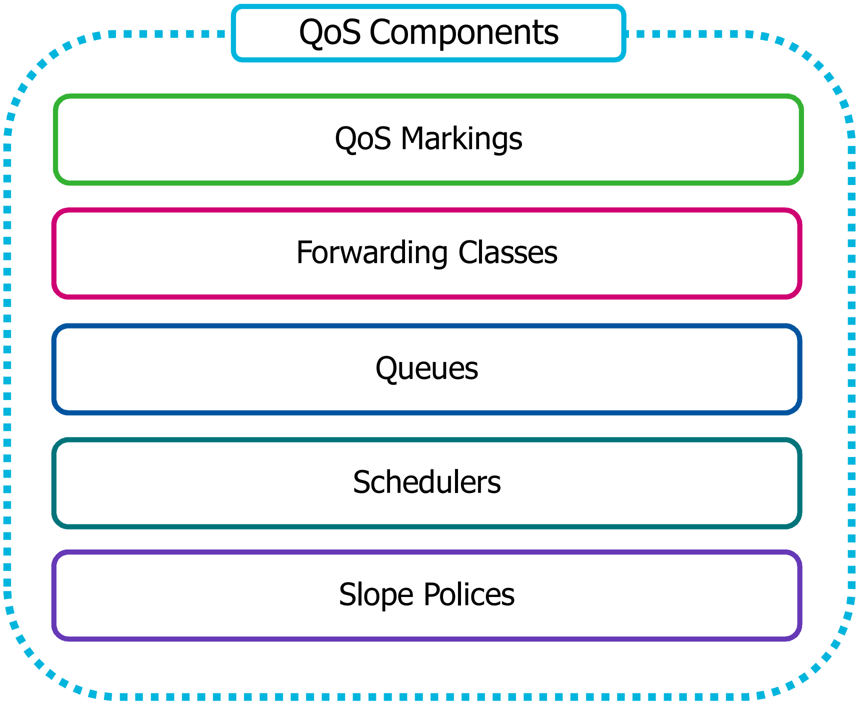
1.1 The Quality of Service concept

QoS provides the ability to rate limit across multiple queues from one or more access interfaces for a customer, and to differentiate service levels for different types of traffic. For higher priority traffic such as VoIP or video, you can specify reserved bandwidth. Lower priority applications, such as data traffic, may not have reserved bandwidth but can burst to use all the available bandwidth.

QoS characteristics

- Uses a combination of hardware and software to provide consistent delivery of traffic across a network
- Distinguishes between different types of traffic in order to allocate resources
  - QoS gives differential treatment to different types of traffic
- Helps to use existing bandwidth more efficiently
- Provides a way to deliver Service Level Agreements (SLA)
- QoS techniques optimize:
  - Bandwidth
  - Delay
  - Jitter
  - Packet loss

1.2 Main components of QoS



The main elements of QoS are:

- QoS markings
  Customer traffic may be marked with QoS markings, such as DSCP, EXP, and dot1p, that are mapped to forwarding classes. All forwarding classes support profile marking of packets as in-profile or out-of-profile. In-profile packets have a high enqueuing priority. Out-of-profile packets have a low enqueuing priority. Profile marking of packets can occur at two points: when packets are classified into forwarding classes at access ingress and when packets are classified at service egress. Profile marking is only done on the internal header and not in an actual encapsulation.

- Forwarding classes
  Provide network elements with a method to weigh the relative importance of packets, only in relation to other forwarding classes. A forwarding class is also referred to as a Class of Service.

- Queues
  Location for buffering packets that are to be forwarded before they are scheduled.

- Schedulers
  Hardware scheduling (or single-tier scheduling) exists by default on a device and consists of a high-priority and a low-priority scheduler.
  Scheduler policies (or multi-tier scheduling) provide a more complex, hierarchical structure of virtual schedulers that override the default hardware behavior for more flexible scheduling capabilities.

- Slope policies
  Define the WRED slope characteristics of hardware buffer space that is used by the ingress and egress queues

Knowledge Verification – QoS Components

What components of QoS provides network elements with a method to weigh the relative importance of packets, in relation to other forwarding classes?

a. Queues.
b. Forwarding classes.
c. Slope polices.
d. Schedulers.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

2 The requirement for Quality of Service

2.1 The requirement for Quality of Service

Drivers for QoS

In order for traffic to be useful at the receiver end, some **requirements** need to be satisfied (e.g. delay, transmission rate or loss ratio)

Different traffic flows may have different requirements:
- They need to receive differentiated treatment
- Separate buffering and forwarding decisions

Requirements are related to the traffic characteristics, aka traffic **profile** (e.g. expected arrival rate or maximum burst size)

Packets that arrive within the expected profile receive agreed service level; packets out of profile may expect to be dropped or delayed

Quality of Service (QoS): guaranteeing that traffic requirements will be satisfied as long as the traffic remains within the established profile

Alcatel·Lucent UNIVERSITY

The concept of Quality of Service

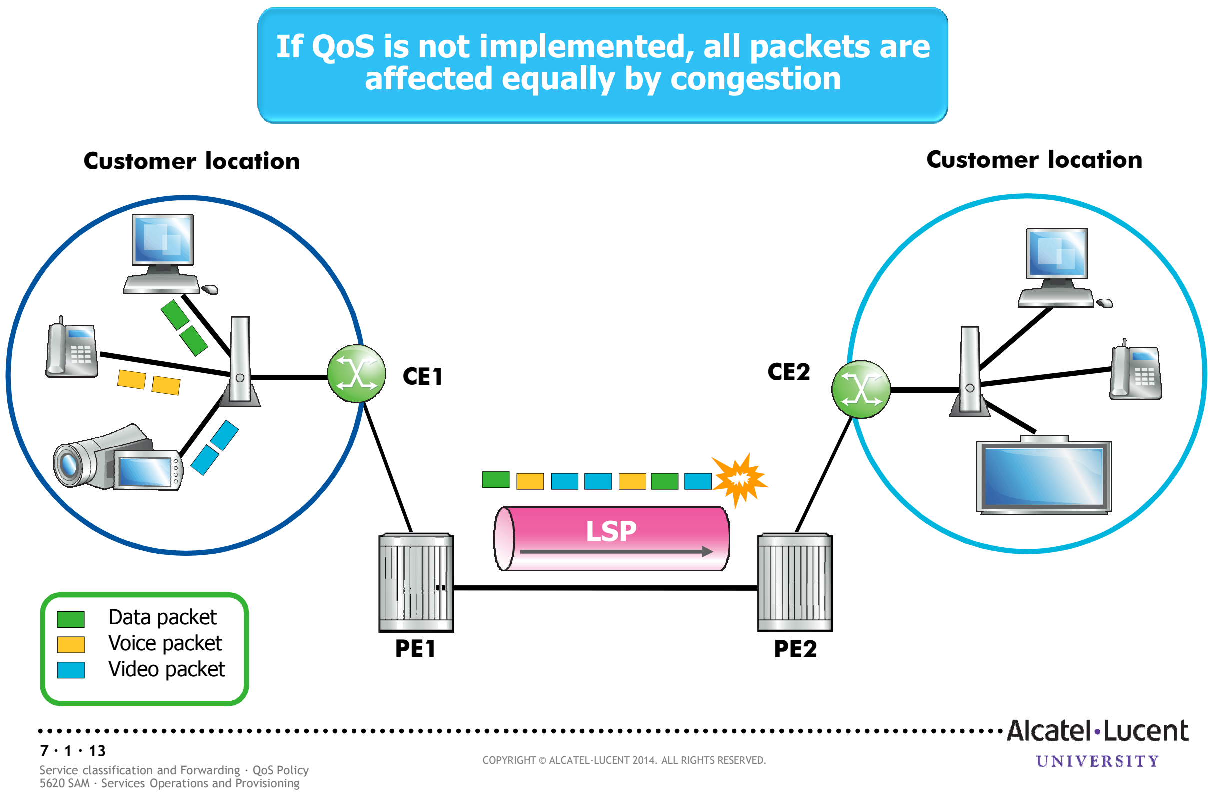
In order for the traffic carried by a network to be useful when it is received at the far end, some requirements need to be satisfied. These requirements may be in terms of the maximum delay or delay variations that individual packets can experience, in terms of the average or peak rate with which packets will flow through the network, or in terms of the maximum percentage of packet losses that can be tolerated by the specific application at hand.

Those requirements are closely related to the traffic characteristics (aka traffic profile), such as the expected average rate with which packets will be generated or the maximum burst size that will be observed.

Different traffic flows may have different requirements. For that reason, flows need to receive a differentiated treatment when it comes to buffering and forwarding packets. For instance, packets that have time constraints need to be forwarded before packets that have no such constraints. In addition to that, packets that arrive within the expected profile need to be serviced in such a way that its constraints are satisfied, while packets that arrive out of profile may expect to be dropped or delayed beyond the limits as the network does not have the responsibility to guarantee for them a certain level of service.

Quality of Service (QoS) has to do with guaranteeing that the requirements needed by traffic (in terms of delay, delay variations, throughput and losses) will be satisfied as packets travel inside the network provided that the traffic itself is maintained within the established profile.

2.2 Congested networks and QoS

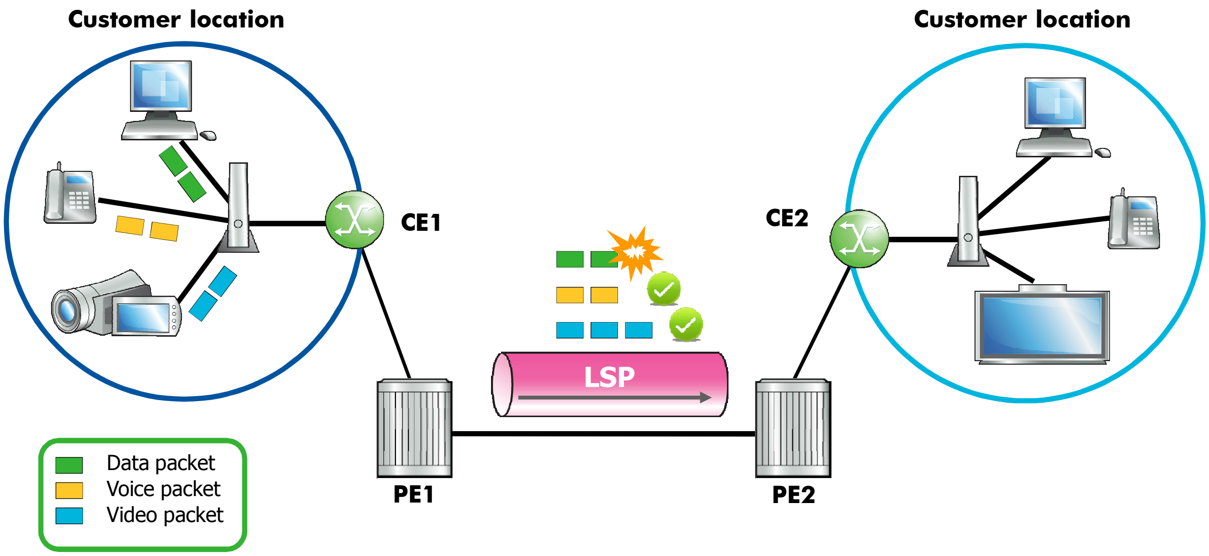


If we have a network with very high bandwidth and little traffic, there is no need to implement QoS since all packets will be serviced with practically no delay. This may require a great infrastructure investment, however, since the network needs to be over-provisioned in terms of hardware.

When traffic needs are closer to the network capacity, which provides a better balance between cost and profit, congestion may start to appear. If all packets are treated equally, congestion will affect all types of traffic the same. This is not optimum since, while data traffic (such as e-mail or web downloads) can afford retransmissions without affecting the perceived level of service, voice and video traffic (being real-time applications) are much more sensitive to packet delays, delay variations and losses.

2.3 Congested networks and QoS

If QoS is implemented, packets are treated differently, depending on needs. Only low-class packets are affected by congestion.



Alcatel·Lucent UNIVERSITY

In a well-planned QoS-aware network, we can have a controlled balance between traffic needs and network capacity in such a way that delay-sensitive applications will have enough resources guaranteed for the service to have a high quality, and non-delay-sensitive applications that may not have too many resources allocated to them, but which may benefit from the resources that are allocated to other traffic streams but not utilized at a given point in time.

This way, if congestion occurs, delay-sensitive applications will not be affected, and it will be low-class traffic flows which will notice a degradation in the service they are receiving.

Knowledge Verification – Traffic Congestion

A user can still experience a delay in traffic delivery for networks that implement QoS.

a. True.
b. False.

Alcatel·Lucent
UNIVERSITY

Choose the correct answer for the knowledge verification question above.

3 Alcatel-Lucent QoS model

3.1 QoS and Alcatel-Lucent service routers

Service differentiation

- Uses differentiated service model (Diff-Serv)

Aggregation and forwarding classes

- Large number of individual micro-flows are aggregated into forwarding classes (8)
- Mapping of traffic to forwarding classes (FC) is based on multi-field classification rules

Resource allocation

- IOM resources are allocated on a per-FC basis
- Performance of FC flows is provided through shaping, queuing, scheduling, and aggregate bandwidth reservation

Traffic policing and shaping

- Available at service ingress and egress
- Policing prevents excessive traffic from congesting the network and assuring that classified traffic conforms to SLAs
- Shaping improves bandwidth utilization minimizes packets loss at downstream policing points

QoS is an integral part of the Alcatel-Lucent service router family of products. QoS techniques, applied to both incoming and outgoing traffic, support multiple customers and multiple services for each physical interface. Alcatel-Lucent service routers have extensive and flexible capabilities for classifying, policing, shaping, and marking traffic.

QoS techniques classify traffic into forwarding classes, also known as classes of service or types of service. A forwarding class provides network elements with a method to weigh the relative importance of one packet over another. Traffic assigned to forwarding classes is placed into queues and the contents of the queues are output in a controlled manner using schedulers. The packet's forwarding class—along with the in-profile and out-of-profile state—determines how the packet is queued and handled as it passes through each service router.

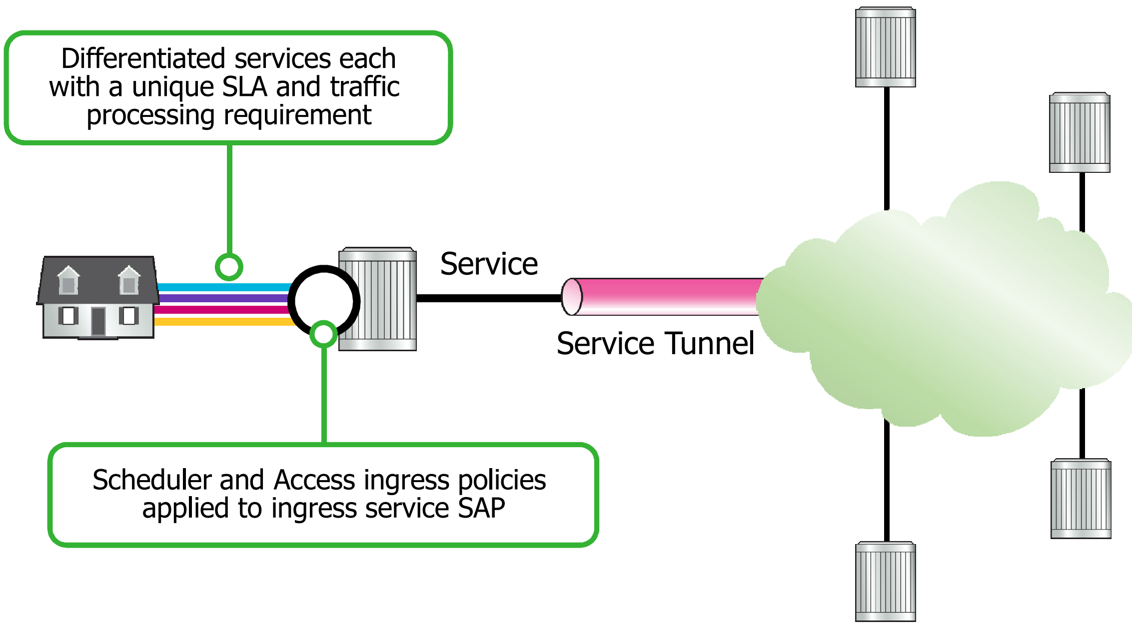
3.2 Traffic Classification - Internal Forwarding Classes

FC ID	FC Name	FC Designation	Default Class Type	Definition
7	Network Control	NC	High Priority	Intended for network control traffic.
6	High-1	H1		Intended for network control traffic or delay/jitter sensitive traffic.
5	Expedited	EF		Intended for delay/jitter sensitive traffic.
4	High-2	H2		
3	Low-1	L1	Assured	Intended for assured traffic. Also the default priority for network management traffic.
2	Assured	AF		Intended for assured traffic.
1	Low-2	L2	Best Effort	Intended for best effort traffic.
0	Best Effort	BE		

The 5620 SAM supports the configuration of eight forwarding classes and class-based queuing or policing on the managed devices. Each forwarding class is only important in relation to other forwarding classes. A forwarding class provides NEs with a method to determine the relative importance of one packet over another packet in a different forwarding class.

Queues are created for a specific forwarding class to determine how the queue output is scheduled into the switch fabric and the type of parameters that the queue accepts. The forwarding class of the packet, and the in-profile and out-of-profile states, determine how the packet is queued and handled at each hop along its path to a destination egress point. Forwarding classes may also be associated with policers instead of queues. Eight forwarding classes are supported.

3.3 QoS and the 5620 SAM



You can use 5620 SAM to configure and enforce traffic rate limiting, based on the priority of the traffic entering the ingress SAP of a service. This configuration limits bandwidth, to ensure that SLAs are met and higher priority traffic is processed first.

Knowledge Verification – QoS Components

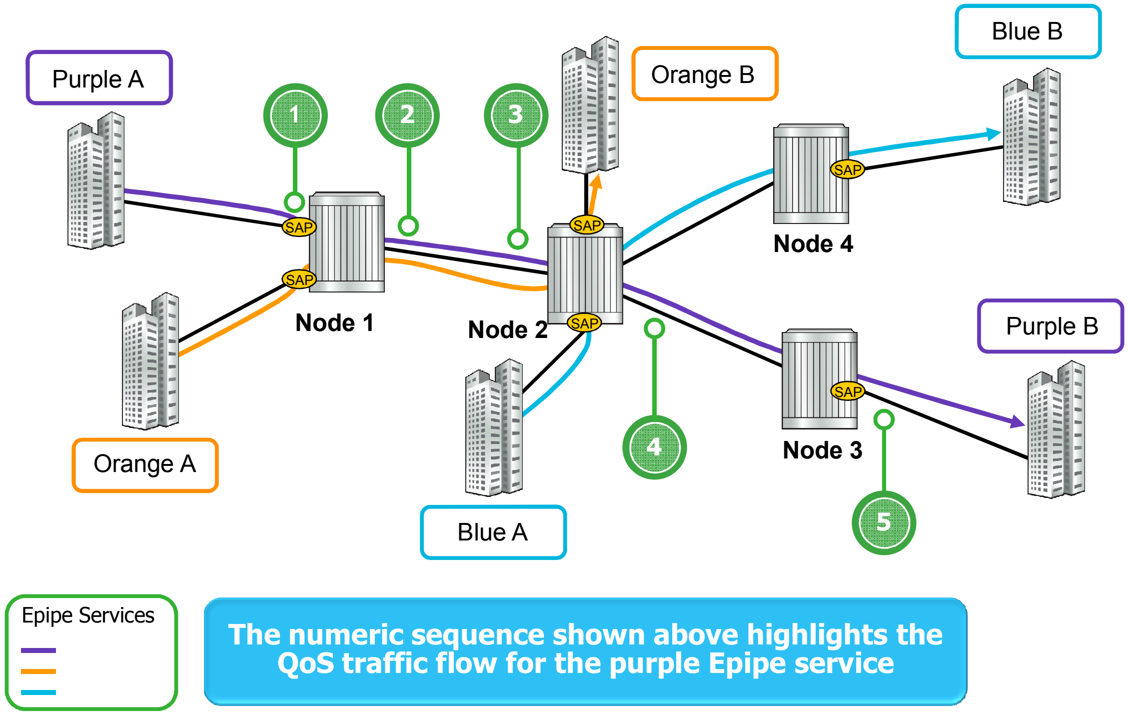
The forwarding class is the single method used to determine how the packet is queued and handled at each hop along its path to a destination egress point.

a. True.
b. False.

Alcatel·Lucent UNIVERSITY

Choose the correct answer for the knowledge verification question above.

3.4 QoS Traffic Flow Example



Alcatel·Lucent UNIVERSITY

1. Orange and purple traffic enters Node 1 through separate service access points (SAP). Each SAP classifies its traffic into one or more forwarding classes based on multi-field classification rules. Classified packets are placed into queues based on the SAP they entered on and their forwarding class. Purple traffic is queued separately from orange traffic. Classification rules and queue parameters are defined in **SAP-ingress QoS policies**.

2. The forwarding class and profile status (in/out) of the purple and orange traffic is translated into tunnel header QoS markings (Exp, DSCP, or dot1q bits). Translation is defined in a **network QoS policy**. All traffic, purple and orange, belonging to the same FC is queued together at the network egress of Node 1. The parameters for network queues, which are different from SAP-ingress queues, are defined by a **network-queue policy**. Queued packets are serviced by virtual output queue (VoQ) schedulers and sent towards the appropriate network port.

3. Purple and orange traffic arrives on the same network interface. The traffic is classified into forwarding classes based on tunnel header markings. The tunnel header to forwarding class translation is defined in a **network QoS policy**. All network ingress traffic on an MDA uses a common buffer pool to create the forwarding class queues. Purple and orange traffic belonging to the same FC is placed into the same queue. Blue traffic, arriving on a SAP, is queued separately from the purple and orange traffic. The queued packets are serviced by a VoQ scheduler and sent towards the switching fabric.

4. Because purple packets are coming from a network ingress on Node 2, they are remarked only if the remark flag in the associated **network QoS policy** is enabled. The purple packets egress port is different from the orange and blue egress ports, so they are queued independently according to their FCs.

5. A **SAP-egress QoS policy** defines queuing and packet marking based on FCs. Packets are queued according to their SAP and forwarding class. The queued packets are serviced by an egress VoQ scheduler and sent towards an egress port for delivery to customers. Traffic arriving at the ingress of Node 3 is processed in the same manner as traffic arriving at the network ingress of Node 2.

3.5 Workflow to configure a rate limiting policy on a SAP

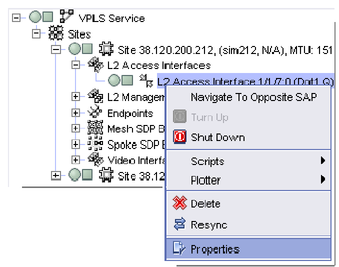
1. Create an Ingress Group Queue Template — Queues (optional CIR/PIR, MBS)

2. Create an Access Ingress QoS Policy — Forwarding CoS to queues
Queue (CIR/PIR and MBS)

Not part of this lab exercise

3. Initiate application of policy to ingress SAP — Manage→Service→Services
Properties

4. Select L2 Access Interface associated with the service



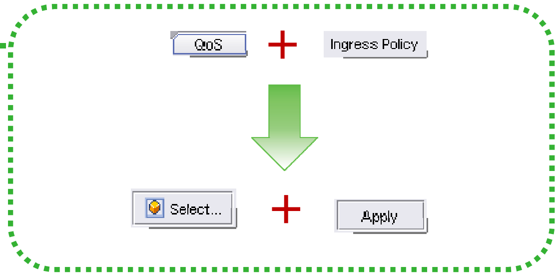
Alcatel·Lucent UNIVERSITY

Note

This model introduces the Quality of Service concept. The intent of the module is to show to potential to apply rate-limiting policies to the services created using the 5620 SAM. Please contact your Alcatel-Lucent support representative for more information on QoS and the associated policy training that is specific to the topic.

3.5 Workflow to configure a rate limiting policy on a SAP [cont.]

5 Apply the Access Ingress policy to the SAP



Note

This model introduces the Quality of Service concept. The intent of the module is to show to potential to apply rate-limiting policies to the services created using the 5620 SAM. Please contact your Alcatel-Lucent support representative for more information on QoS and the associated policy training that is specific to the topic.

This page is left blank intentionally

End of module
QoS Policy

Congratulations
You have finished the training

Your feedback is appreciated!
Please feel free to Email your comments to:

training.feedback@alcatel-lucent.com

Please include the training reference in your email (see cover page)

Thank you!

Alcatel·Lucent