SPB / Fabric Connect Solutions

Fabric Extend with VSP4000 and ONA

Engineering

> Fabric Extend (SPBoIP) using VSP4000 and ONA1101GT, plus Senetas Encryptors

(Avaya Lab test)

Avaya Networking

Document Date: September 2015

Document Number: NN48500-652

Document Version: Version 1

© 2015 Avaya Inc.
All Rights Reserved.

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site:
http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:
http:// www.avaya.com/support.

Abstract

This guide details testing conducted to validate customer deployments using Avaya's SPB Fabric Connect network virtualization technology over an IP network. IP networks could be an enterprise wide IP infrastructure where SPB fabric "islands" need to be interconnected into a single fabric area. Additionally, IP networks are commonplace in the wide area (WAN) where IP-VPN based services are used for inter-office corporate communications, for example; between a headquarters site and several remote branch sites. In both cases, the SPB fabric can be 'Extended' over an IP network on selected Avaya VSP switching platforms.

This guide documents testing performed to validate tunneling SPB services over an IP infrastructure, whether in an IP WAN or across an enterprise IP network. The products focused in this testing were VSP4000 series switches with the Open Networking Adapter (ONA) 1101GT device.

Acronym Key

Throughout this guide the following acronyms will be used:

Acronym	Term
SPBm	Shortest Path Bridging (MAC)
SPBoIP	Shortest Path Bridging over Internet Protocol
ISIS	Intermediate System to Intermediate System
NNI	Network to Network Interface
UNI	User to Network Interface
BCB	Backbone Core Bridge
BEB	Backbone Edge Bridge
CFM	Connectivity and Fault Management
GRT	Global Routing Table
ISID	Individual Service IDentifier
VSN	Virtual Service Network
VRF	Virtual Route Forwarding
VSP	Virtual Services Platform
ONA	Open Networking Adapter
WAN	Wide Area Network
VLAN	Virtual Local Area Network
C-VLAN	Customer Virtual Local Area Network (VLAN to ISID mapping)

Revision Control

No	Date	Version	Revised By	Remarks
1	September 2015	1.0	Data BU Arch/SME's	Initial release of document.

Table of Contents

Figures

Tables

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
VSP7024XL# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
VSP7024XLS# show sys-info

Operation Mode:          Switch
MAC Address:             3C-B1-5B-FE-EC-00
Reset Count:             46
Last Reset Type:         Software Download
Power Supply 1:          AC-DC-12V-450W-F2B
Power Supply 2:          Unavailable
Power Status :           1- OK  2- Not Present
Autotopology:            Enabled
Pluggable Port 1:        1000BASE-T
Pluggable Port 2:        None
Pluggable Port ...       None
Base Unit Selection:     Non-base unit using front-panel switch
sysDescr:                Virtual Services Platform 7024XL
                         HW:01       FW:10.3.0.2  SW:v10.3.0.010
                         Mfg Date:20110610    HW Dev:none
```

1. Overview

Avaya's Shortest Path Bridging (SPB) Fabric Connect function is widely supported on most Avaya switching products providing opportunity to architect a SPB fabric core with a range of features and scaling to suite campus and Data Centre fabric based solutions.

This expansion of SPB solutions now includes extending fabric over IP networks, hence the term "Fabric Extend" which is part of Avaya's SDN-Fx architecture. Fabric Extend is targeted at supporting SPB over the WAN with Layer 3 based IP-VPN services, but can also serve to support the connection of SPB/Fabric "islands" located in parts of a large IP routed enterprise network.

This guide illustrates Avaya's SPB Fabric Connect solution being "Extended" over an IP Core/WAN infrastructure using the VSP4000 switching platform in conjunction with Avaya's ONA to provide IP tunneling of SPB and virtualized services over an IP cloud.

Due to the nature of SPBoIP / Fabric Extend, where SPB solutions will also traverse a service-provider public WAN infrastructure, the latter section of this guide also includes testing with Senetas Ethernet encryption devices to encrypt traffic over the IP Core / WAN.

2. Test setup

2.1 Network design

The high level design of the test environment consisted of two main sites, Site 1 and Site 2, separated by an IP Core/WAN. Each site contained two VSP4450GSX-PWR+ switches with SPB enabled to provide virtualized services within each site, with the intention of extending the SPB fabric across the IP Core/WAN to link the two sites into a single SPB entity for all virtualized services.

With VSP4450 switches (any VSP4000 series switch), the Open Network Adapter (ONA 1101GT) is required to perform IP tunneling of SPB control plane and data plane services using a VXLAN header to encapsulate SPB (Mac in Mac) traffic.

Below is a high level view of the physical test environment setup to test SPBoIP, aka; Fabric Extend:

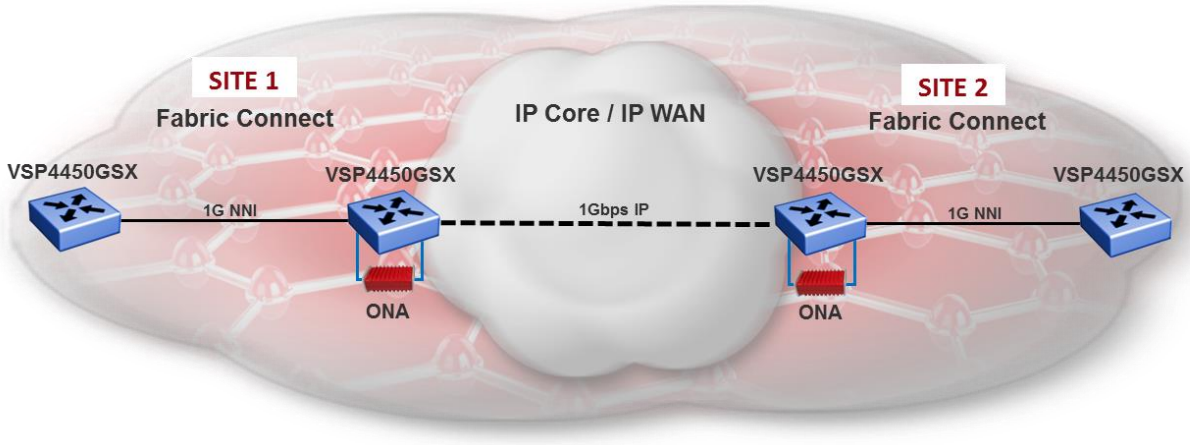


Figure 2.1 – High level SPB over IP test setup

2.2 VSP4000 Switch setup

All VSP4450GSX's were running a pre-beta build of VSP OS version 5.0 (int 643) and were each installed with Premier + MACsec licenses.

All switch interconnects were uniformly set to 1Gbps speeds on all NNI links and IP WAN links with VSP4450 PoE ports also running at 1Gbps for ONA communications and powering the ONA. VSP4450 W1 and W2 nodes were initially connected directly back to back before an additional VSP4800 switch was added to simulate IP routing in the core / WAN with different IP subnets on the WAN edge switches.

Site 1 VSP4450 switch names were configured as VSP4K-A1 (Access) and VSP4K-W1 (WAN), while Site 2 switch names were VSP4K-A2 (Access) and VSP4K-W2 (WAN).

Figure 2.2 shows the port configuration of the test environment:

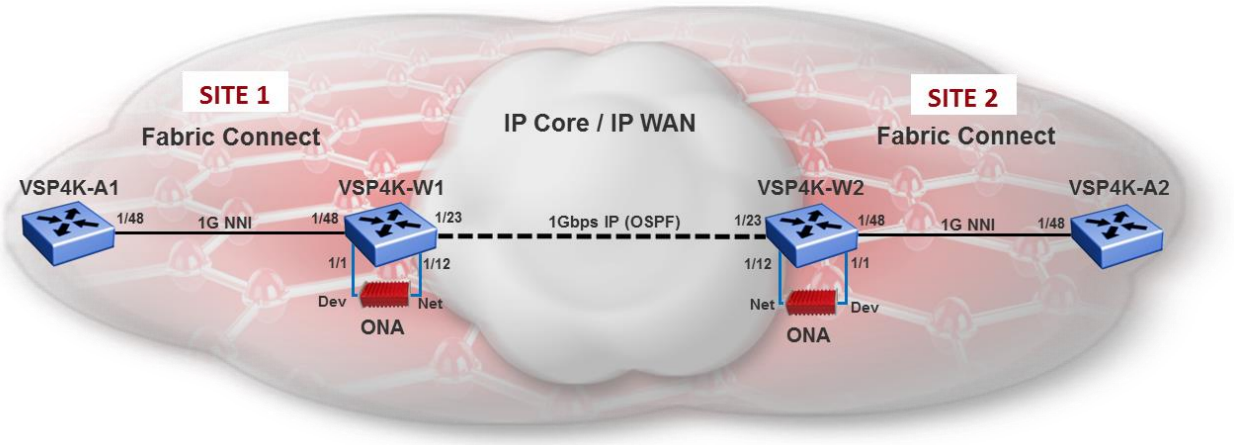


Figure 2.2 – SPB over IP test setup with port detail

2.3 ONA1101GT setup

Two ONA1101GT's were used with two VSP4450's to validate both SPBoIP plus IP fragmentation and reassembly functions for the test solution. The default MTU size of 1950 bytes (set on VSP4000's) was initially used before subsequent tests were performed with the MTU size reduced to 1200 bytes.

Each ONA1101GT was configured for SPBoIP mode where the management IP address, mask, and IP gateway addresses were programmed into the ONA. A special boot sequence process is required to manually set this basic information in the ONA. This is achieved by connecting a PC/laptop to the Device side Ethernet port on the ONA, then holding down the mode switch (behind the ONA pinhole) while powering the ONA via PoE on the Network side Ethernet port, or external DC adapter. The PC will automatically receive an IP address and a browser on the PC can be pointed to IP address 192.168.100.1 to connect to the ONA. The update static configuration option is selected to enter the Operational Mode (1 = SPBoIP), the Management IP Address, the Management IP Subnet Mask and the Default Gateway IP Address. When complete, click on the Save button bar and unplug all

Ethernet connections – which will power down the ONA. The ONA is now ready for SPBoIP operation with a VSP4000 series switch.

Note: The ONA can also receive an IP address assigned via DHCP if this process is chosen. The acquired IP address will then be relayed to the VSP4000 by LLDP. This process provides a full "hands off" method for configuring and attaching the ONA to the VSP4000 switch.

The ONA Management IP has local significance to the GRT for local connection and management of the ONA. The ONA uses LLDP to announce its IP management address to the VSP4000 switch. A IP based webservices session is then established between the ONA and the VSP4000 switch. This is required to program the VXLAN header with the tunnel IP source address for the ONA to add the source IP encapsulation for SPB traffic passing through the ONA. MTU size configuration on the VSP4000 is also programmed on the ONA when used with the SPBoIP solution.

Figure 2.3 – ONA 1101GT device

3. Fabric Extend testing

3.1 Test 1

3.1.1 Physical and Logical Architecture

Test 1 was performed to validate a basic single VXLAN tunnel between two VSP4450 switches, VSP4K-W1 and VSP4K-W2, and an ONA for each switch. In this configuration, each switch used the GRT (Global Router) for ONA management and a VRF “SPBoIP” for the tunnel source IP address. VRF “SPBoIP” also contained an IP gateway interface attached to VLAN 1505 simply used locally on each side of the WAN to connect VSP4K-W1 and VSP4K-W2 back-to-back within a single IP subnet. OSPF was enabled on these interfaces to simulate a routed WAN link between the sites.

IP address schemes used in this test are to assist in providing clearer separation of different functional components and networks. In reality for example, the ONA management VLAN and IP addresses could all be the same network as they are locally contained: IE: 192.168.1.1 for the VLAN gateway and 192.168.1.2 for the ONA management IP address. This would provide a single common address to connect to any ONA from the local VSP switch.

Below are physical and logical illustrations of the Test 1 setup. When SPB was running successfully over the IP core with adjacencies formed between VSP4K-W1 and VSP4K-W2, a single Layer 2 VSN was configured to test communications between two edge PC’s.

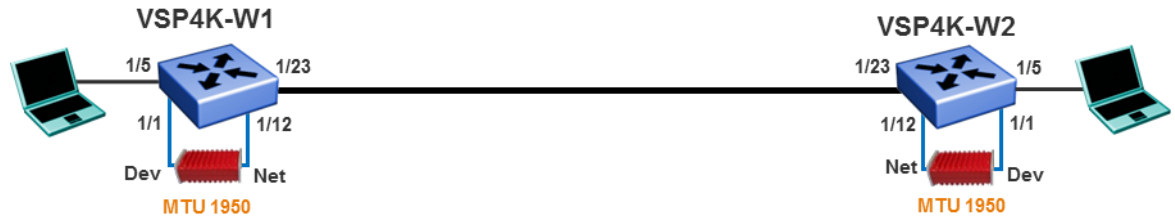


Figure 3.1 – Test 1 Physical Architecture

Figure 3.2 – Test 1 Logical Architecture

3.1.2 VSP4K and ONA SPBoIP detail

Figure 3.3 below details the configuration used to setup the SPB over IP solution between two VSP4450 switches. Each ONA is powered through its Network side port by PoE on each VSP4450, while the device side provides connectivity to and through the ONA to perform VXLAN encapsulation.

The ONA performs VXLAN encapsulation of MAC in MAC traffic egressing port 1/1. The VXLAN tunnel source IP address is defined in the VSP4000 switch configuration and pushed to the ONA – along with the MTU size configuration, which was left at default for Test 1. The VRF "SPBoIP" loopback address 15 is used to define the VXLAN source address on the ONA and provides a VRF linkage or extension to the ONA for transporting SPB over the IP tunnel (as shown by the dotted blue line in figure 3.3).

Note that encapsulated MAC in MAC SPB traffic is egressing the ONA Network port back into the VSP4000 switch on port 1/12 for native IP routing over an IP WAN or IP Core network. OSPF is enabled to perform dynamic routing over the IP WAN subnet as shown in figure 3.3. On port 1/12, the management session between the VSP4000 control plane and the ONA is also exchanged. The VSP4000 automatically ensures that the ONA management traffic is classified into the GRT.

The ONA has a management IP subnet defined for service configuration and management access from the VSP4000 via VLAN 1050 (refer to red line in figure 3.3). This IP subnet is self-contained between the ONA and local VSP4K switch and is not advertised to outside IP networks.

The VSP4000 GRT with loopback address 30 exists for the purpose of supporting IP Shortcuts on the switch if IP service termination over the SPB fabric is required on the local switch.

Finally, logical ISIS interfaces exists on the VSP4000 to support Point-to-Point tunnels originating at the VSP4000. These ISIS tunnels originate at port 1/1 on the VSP4000 and are encapsulated into VXLAN tunnels at the ONA. Below is a detailed view of the configuration used in all testing.

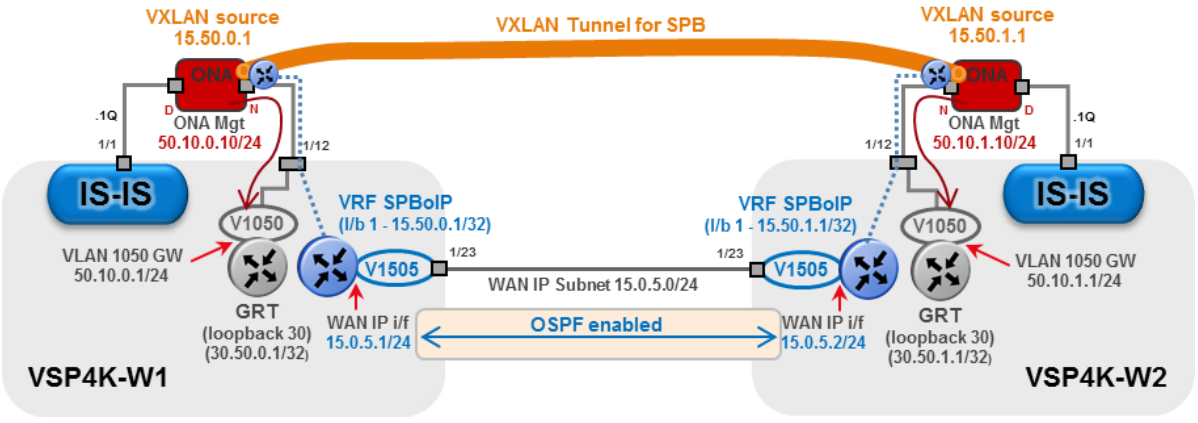


Figure 3.3 – Test 1 Architecture Configuration Detail

Each logical ISIS interface will have its own tunnel. The tunnels are point-to-multipoint from an IP perspective but not from the logical ISIS interface perspective.

NOTE: loopback 30 on the GRT for each VSP4000 is actually not a required configuration.

3.1.3 VSP4K and ONA SPBoIP functional view

Figure 3.4 illustrates the high level functional view of the component and relationships for SPB over IP operation on a VSP4000 platform with the ONA1101GT. This view further clarifies use of the ISIS logical interface in relation to the data plane for mapping ISIS NNI functions to VXLAN tunnels. Also note the relationship of Fabric Attach (LLDP) and ONA management element functions in the model.

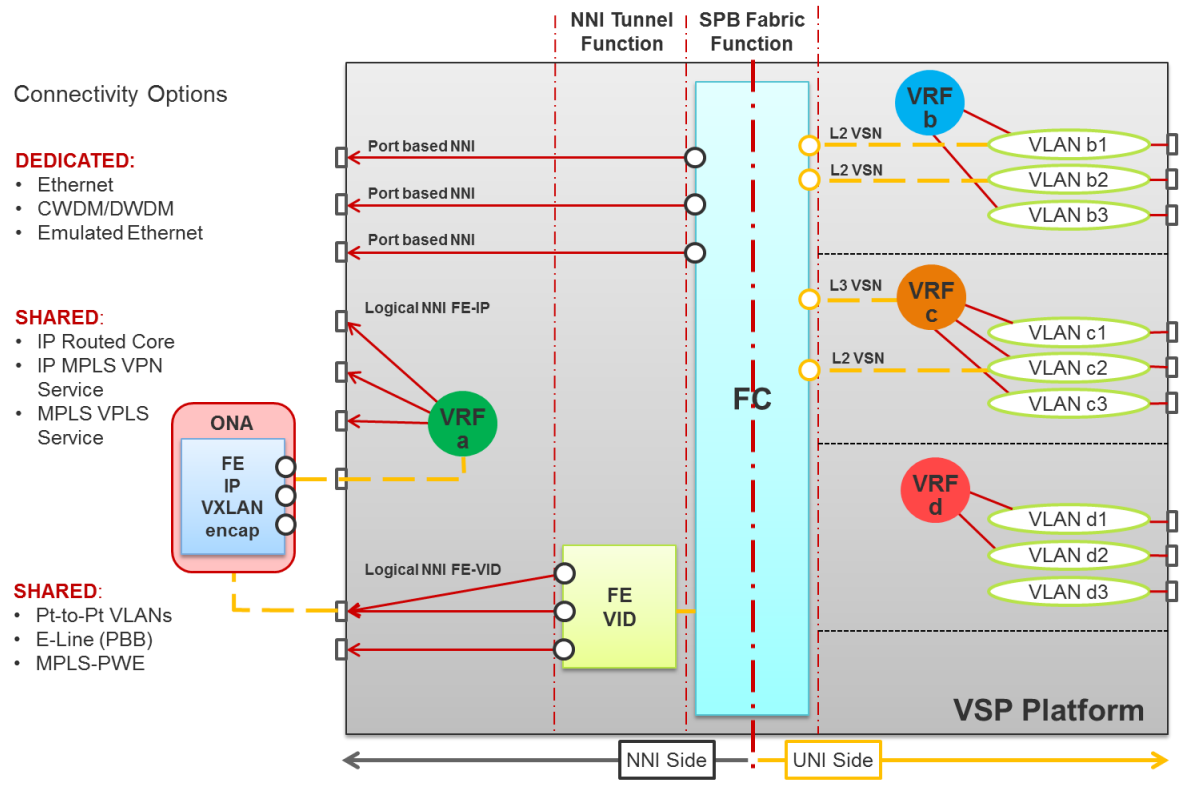


Figure 3.4 – VSP4K and ONA SPBoIP functional components view

Figure 3.4 illustrates how the UNI and NNI side functional blocks operate together in a VSP platform.

UNI Side:

- Ports are assigned to VLANs
- VLANs are assigned to VRF
- VLANs can be attached to the FC (SPB) block by assigning an ISID -> L2 VSN
- VRFs can be attached to the FC block by assigning ISIDs -> L3 VSN
-

NNI Side, NNI functions are:

- Port based NNI, dedicated for physical or emulated Ethernet pipes
- FE IP with VXLAN encapsulated shared IP NNIs for IP routed and IP MPLS cores, as well as VPLS cores.
- FE VID shared VLAN NNIs for point-to-point or point-to-multipoint VID tunnels.

3.2 Test 2

3.2.1 Physical and Logical Architecture

Test 2 builds on test one with the addition of two VSP4450's "VSP4K-A1" and "VSP4K-A2" at the network extremities to expand SPB, plus a core VSP4850 "VSP4K-C1" adding a core IP routing node in the center of the test network.

The additional SPB nodes and core IP routing switch causes very little change to the configurations of nodes VSP4K-W1 and VSP4K-W2. The IP WAN ports and IP addresses change on one side as the connection is no longer back to back and contained in a single IP subnet. Then an additional NNI port is configured on each switch to add connectivity to the SPB access nodes A1 & A2.

Below are physical and logical illustrations of the Test 2 setup. When SPB was running successfully over the IP core with adjacencies formed between VSP4K-W1, VSP4K-W2, VSP4K-A1 and VSP4K-A2, a single end to end Layer 2 VSN was configured to test communications between two edge PC's.

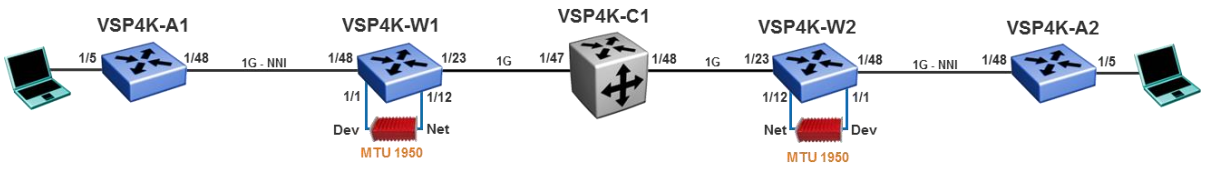


Figure 3.5 – Test 2 Physical Architecture

Figure 3.6 – Test 2 Logical Architecture

3.2.2 VSP4K and ONA SPBoIP detail

Figure 3.7 details the new configuration used for Test 2 setup of SPB over IP solution. The IP tunnel still exists between nodes VSP4K-W1 and VSP4K-W2, but now with an additional IP hop across VSP4K-C1. It is important to note that SPB has no awareness of the underlying IP network in the core of this environment and all SPB nodes communicate within a single SPB area. The simulated IP WAN /Core is simply carrying SPB traffic over the layer 3 routed network in the middle of the test environment. Further, any IP network domains configured with SPB using IP Shortcuts (GRT) or via VRFs are completely separate entities to the IP network in the WAN or campus core of an enterprise.

Although the testing illustrates a single SPBoIP tunnel, multiple tunnels can exist at any tunnel source point enabling the configuration of part-mesh or full-mesh topologies over an IP infrastructure.

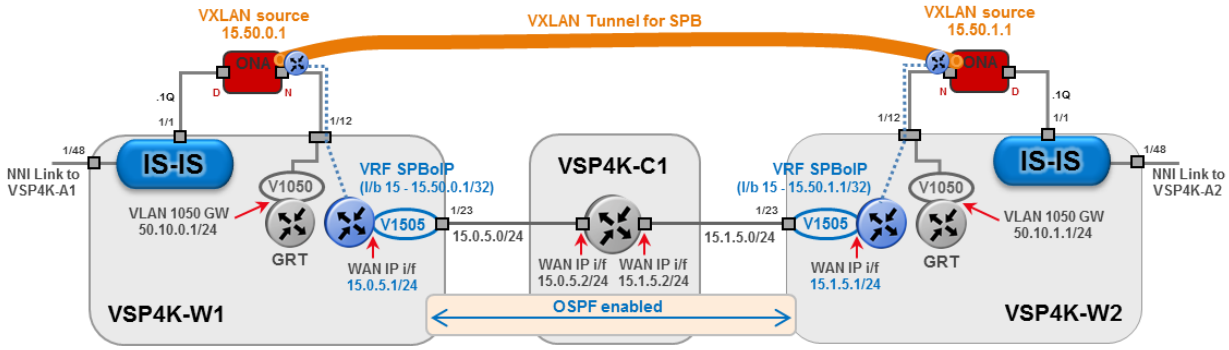


Figure 3.7 – Test 2 Architecture Configuration Detail

3.3 Test 3

3.3.1 Senetas Encryptors with SPBoIP

Test 3 adds two Senetas CN4010 tabletop 1Gbps Ethernet encryptors into the environment used in Test 2; “CN4010-E1” and “CN4010-E2”, refer to figure 3.7. The encryptors are positioned inline on the NNI connection in between “VSP4K-A1” and “VSP4K-W1” switches at Site 1, and in between “VSP4K-A2” and “VSP4K-W2” at Site 2. Senetas Encryptors contain a non-encrypted side “Local” port and an encrypted side “Network” port. At each site the Network port faces the VSP4K-W1 / VSP4K-W2 switch creating an “encrypted tunnel association” between those points (Senetas term). Although only two sites are shown in the test, multiple sites connected in a hub and spoke topology are supported requiring one encryptor at each site. IE: a third site with W3 and A3 switches, and E3 encryptor could exist connecting back to the site W1, E1, A1 devices.

This test environment was conducted to validate data encryption over a Layer 3 WAN solution incorporating Avaya’s SPB Fabric Connect technology. The test successfully validated the operational function of encryption over a Layer 3 network with SPBoIP. Although the test was performed over a single IP tunnel, this solution can be used as a valid reference model for point to multipoint and multipoint to multipoint solutions in the WAN. The same is also true for Campus IP networks where point-to-point, part-mesh up to full mesh SPB interconnections may exist.

Note that Senetas encryptors require a layer 2 domain for key management traffic which would normally be sent in band via the encrypted side “Network” port. Over a Layer 3 WAN such as this the encryptor’s Out of Band (OOB) key management feature was enabled using the CN4010’s Ethernet management port. OOB key management forces all encryptor key management traffic to be sent over the management port as noted by the additional third link extending out of each CN4010 encryptor into a separate port on each VSP4450 WAN switch.

All SPB based data traffic egressing the encryptor Network port is encrypted before being encapsulated with a VXLAN header by the ONA, and then routed over the WAN via the SPBoIP VRF. On the opposite side, the reverse process occurs where the routed IP packets have the VXLAN header stripped off by the ONA (the destination tunnel IP address) before ingressing the far end encryptor Network port, then being decrypted and egressing the Local port in the clear.

Note: Because the Senetas Ethernet encryptors are located in between two SPB switching nodes, the IS-IS control plane function must remain unencrypted in order for SPB node adjacencies to form across the encryptor. For this reason an encryption “Bypass” rule must be configured on the Senetas

encryptors to allow IS-IS control plane traffic to reach the node on the Network port side of the encryptor. The manually configured bypass rule allows all traffic using the IS-IS “well known MAC address” 09:00:2b:00:00:05 to pass through unencrypted.

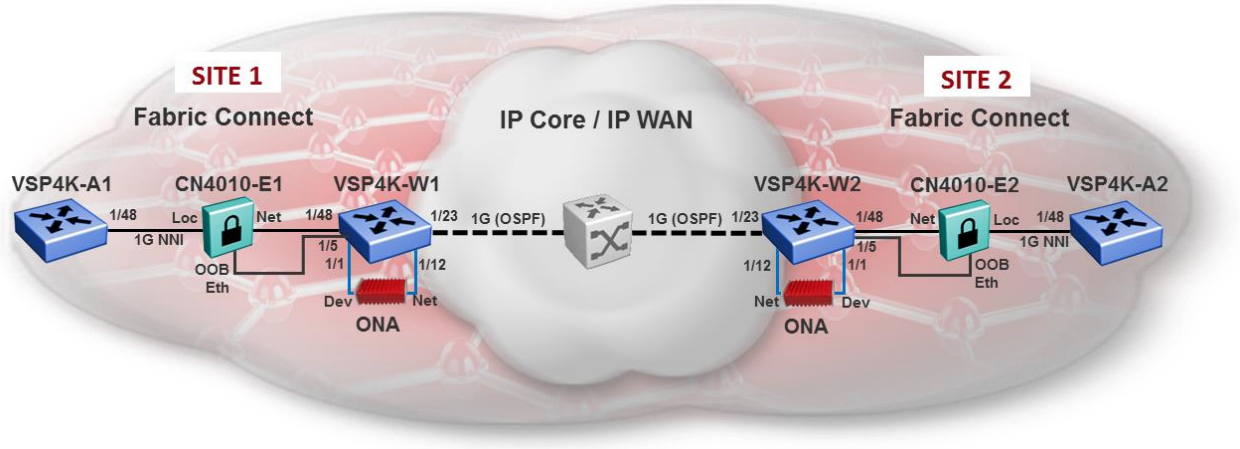


Figure 3.8 – Test 3 Architecture Configuration Detail

NOTE: IS-IS MD5 hash keys can be used to prevent rogue SPB nodes from attaching to the network and forming IS-IS neighbor adjacencies, and potentially participate in service termination. While not used in this testing, it is important to note that this feature provides additional protection to the SPB fabric, given that an encryption bypass rule was used to allow IS-IS control plane traffic across the encryption boundary/zone.

3.3.1.1 Senetas CN 4010 Encryptors

Senetas CN4010 Ethernet encryptors are cost effective compact tabletop line rate encryptors capable of operating from 10Mbps up to 1Gbps. Senetas encryptors have a non-blocking architecture that delivers wire speed throughput with ultra-low latency. All Senetas encryptors are also government certified to FIPS 140-2 and Common Criteria standards.

The Senetas CN4010’s used in this testing were set to 1Gbps and performed both transparently and flawlessly in conjunction with SPB and in the test architecture illustrated in this section, enabling a uniquely flexible and high performance solution for SPB carrying encrypted virtualized network services over a customer Wide Area Network.

Figure 3.9 – Senetas CN4010 Ethernet Encryptor (front / rear)

3.3.2 Physical and Logical Architecture

Test 3 adds two Senetas CN4010 encryptors in between VSP4450 W1 and A1 nodes, plus, VSP4450 W2 and A2 nodes as per figure 3.10 below. The CN4010 out of band Ethernet ports were used specifically for encryption key management. This function requires a L2 domain for group key exchange and synchronization. To support this, a Layer 2 VSN with C-VLAN mapping was created on nodes VSP4K-W1 and VSP4K-W2 with port 1/5 dedicated for connecting the CN4010 OOB Ethernet port to this service.

Figure 3.10 illustrates the test environment with encryptors added to perform data encryption over the SPBoIP WAN connection. With a SPBoIP Fabric Extend solution, encryption must be performed prior to MAC in MAC frames being encapsulated in a VXLAN header before being routed over the WAN. It can be seen that the "inside" Key Mgmt and Switch Mgmt L2 VSNs within the encryption boundary are denoted with a "1298xxxx" prefix compared to the "outside" Switch Mgmt L2 VSN "1299xxxx". These domains are separated due to the location of the Senetas encryptors.

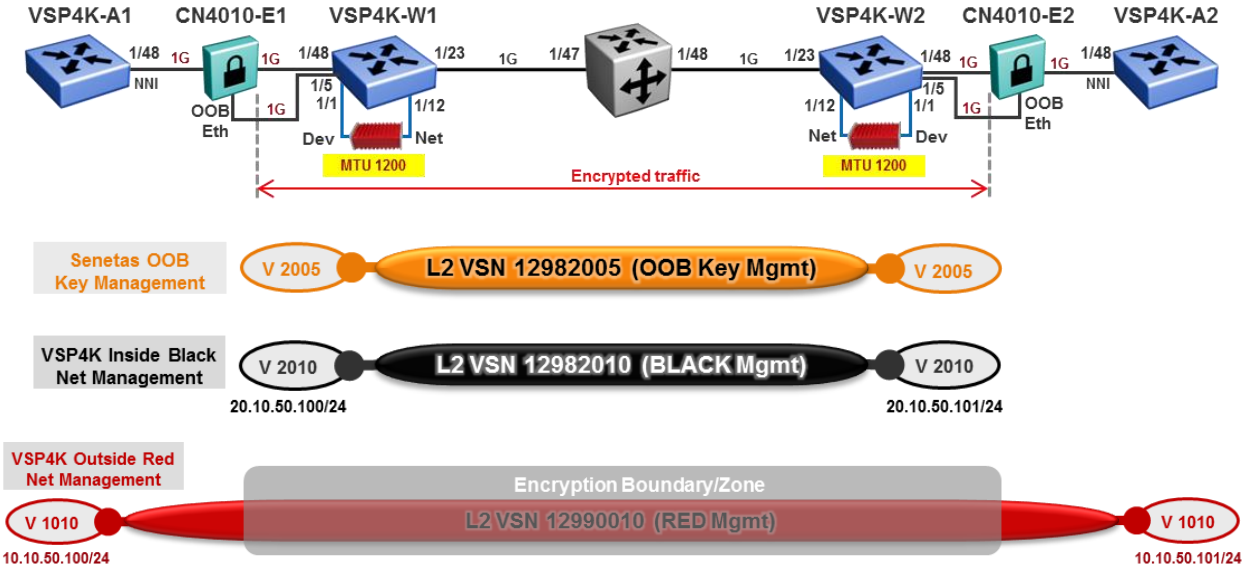


Figure 3.10 – Test 3 Physical and Logical Management Architecture with Encryption

In addition to this, the MTU sizes were also reduced to 1200 bytes. In previous tests, the typical maximum frame size over the IP WAN/core was 1594 bytes.

3.3.2.1 Switch Management

Figure 3.10 illustrates the dedicated Layer 2 Virtual Service Network used for Senetas encryptor key management between all encryptor OOB Ethernet management ports. This VSN only exists on the inside of the encryptor boundary – all SPB nodes on the Network side of Senetas encryption devices.

As a result of connecting encryption devices in between SPB nodes, a level of communication separation is created between the encryption boundary/zone and outside the encryption boundary. As per Figure 3.10, there is a "Black" management VSN domain for VSP4000 switches located in-between the encryptors inside the encryption boundary/zone. A "Red" management VSN domain was created for VSP4000 switches on the outside of the encryption boundary. Any additional SPB nodes outside the encryption boundary will also be part of the "Red" management VSN domain.

Figure 3.11 provides a more simplistic view to illustrate the data plane separation due to encryption between SPB nodes. A single SPB control plane is still maintained across the entire SPB area.

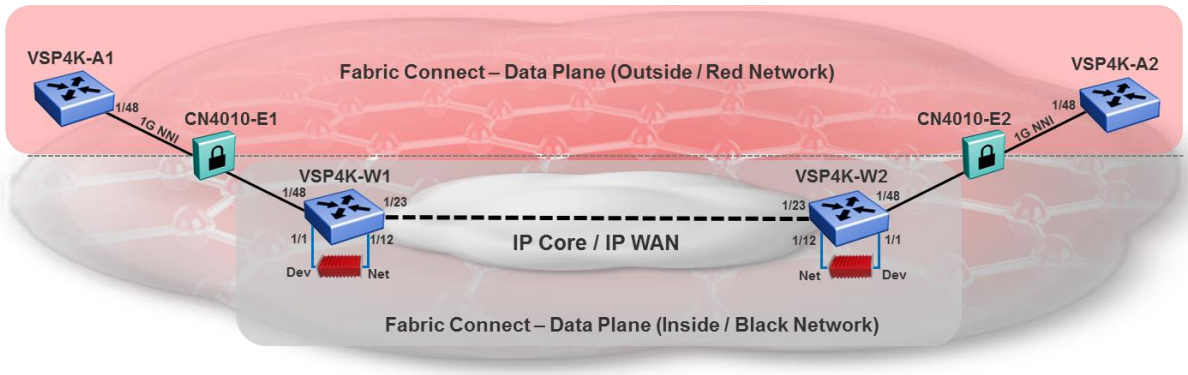


Figure 3.11 – Split Fabric Connect Data Plane view

3.3.2.1.1 Recommendation for Management with Encryption

Avaya recommends that in environments requiring government certified encryption that separate switch management domains be used for the non-encrypted boundary versus the encrypted boundary.

For customers requiring a single management domain, a government certified firewall could be used to “bridge” the two management domains to provide management capability across both domains as a single entity if required. Be aware that GRT IP addresses and loopback IP addresses could potentially overlap if the boundaries are bridged, and additional routing rules would likely be required to facilitate a single domain in this manner.

Additionally in the near future (EoY 2015), Senetas encryptors will support a new feature in which individual security associations can be created based on SPB I-SIDs. This capability means the Layer 2 VSN /I-SID created to support inside Black Management domain could be in bypass mode to allow it to be extended to areas outside the encryption boundary. However, while this provides additional convenience, it will be recommended to maintain separation of management domains to protect against exposure of non-encrypted management addresses within the encryption boundary where a public infrastructure will likely exist.

3.3.2.2 Global Routing Tables

Figure 3.12 illustrates the result to the GRT on VSP4000 switches within the encryption boundary compared to VSP4000 switches outside the encryption boundary, providing separation of the GRT functions between the two groups of switches. All IP interfaces were being redistributed across the inside and outside GRT.

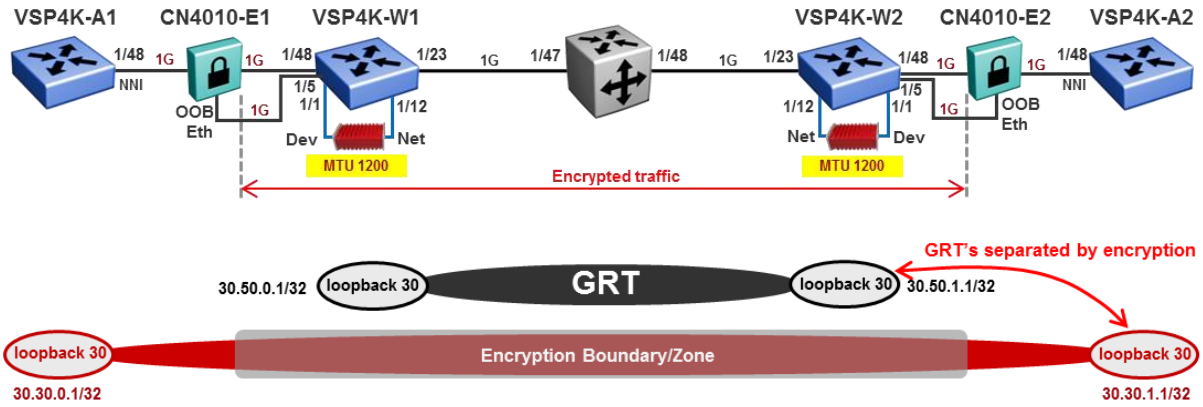


Figure 3.12 – Test 3 GRT IP Shortcuts (loopbacks)

3.3.2.3 Virtualized Network Services

Figure 3.13 illustrates end to end virtualized services over the SPB network for multiple tenants, users or applications. The pre-existing Layer 2 VSN I-SID 12990020 from Test 2 was still place after Senetas encryptors were added, and remained operational.

A Layer 3 VSN 13990010 was then created and linked to VRF Green which contained both a loopback address (for internal VRF route testing) and a VLAN with IP subnet for local users. Note: if the same L3 VSN was also created on nodes W1 and W2, hosts within the encryption boundary will not be able to communicate with hosts outside the encryption boundary.

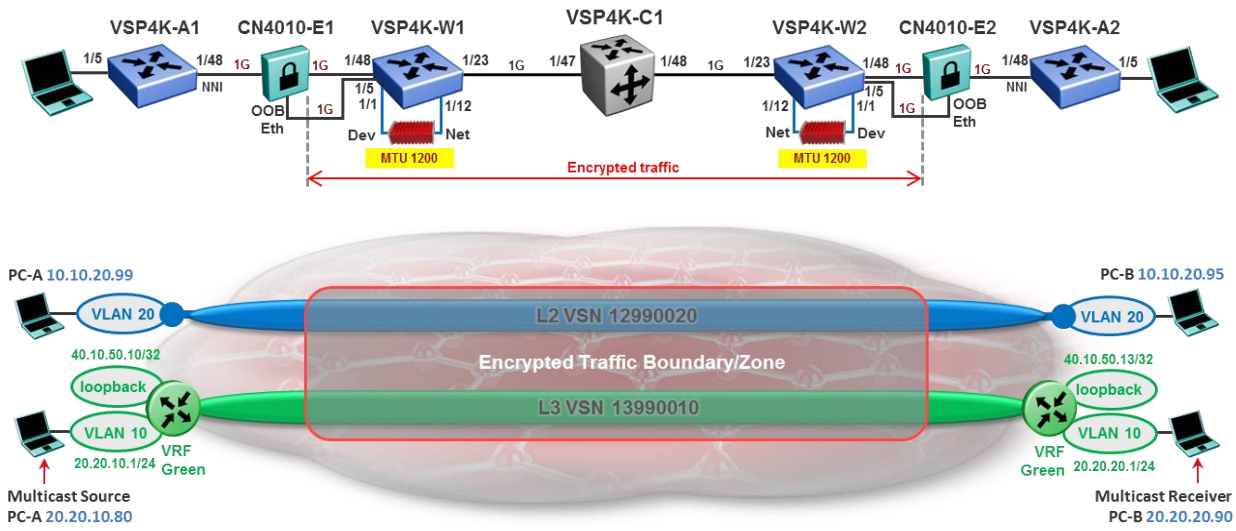


Figure 3.13 – End to End Virtualized Services (VSNs)

3.3.2.4 Testing communications over VSNs

Several tests were conducted over the Layer 2 and Layer 3 VSNs configured across the two end point BEB nodes in the test environment to validate operation and functionality.

Layer 2 VSN 12990020 consisted of VLAN 20 mapped locally at each end VSP4K node (VSP4K-A1 and VSP4K-A2) of the test network. Two laptop PCs, PC-A and PC-B, were configured within the same IP subnet for communications across the VSN and was successfully tested with ICMP Ping and MS Windows file sharing.

Layer 3 VSN 13990010 consisted of VLAN 10 mapped locally at each end VSP4K node (VSP4K-A1 and VSP4K-A2) to VRF Green with IP gateway addresses as per Figure 3.13 of the test network. A loopback address was also configured on each end VSP4K switch for VRF Green to test route re-distribution and in-band network connectivity in the VRF.

VRF Green was enabled with Multicast virtualization over SPB to test dynamic multicast services over the test environment. PC-A was configured with IP address 20.20.10.80 running MC Hammer sending IP Multicast packets on multicast group address 234.5.6.7. This group creates dynamic data I-SID 16150002. PC-B with IP address 20.20.20.90 was a Multicast receiver listening to multicast address 234.5.6.7.

CLI show command outputs of this multicast test can be seen in section 5.1.5 of this document. What will also be seen is PC-B (20.20.20.90) sending IP Multicast packets on 239.255.255.250 creating a dynamic multicast data I-SID 16000001. This is Microsoft Windows advertisements (on by default).

3.3.2.5 Packet Fragmentation and Reassembly

With the support of IP / VXLAN encapsulation of MAC-in-MAC frames in a SPBoIP solution, the maximum standard packet size will reach 1594 bytes. However, many IP-VPN WAN service providers may not support frames over 1550 bytes (approximately). Therefore, fragmentation of IP packets will be required to ensure packet transmitted fall within the maximum frame size limit.

When IP packet fragmentation and reassembly is a requirement in IP networks that cannot support at least 1594 bytes for SPBoIP solutions, the ONA must be used and terminate every end point of the IP tunnel (IE: the ONA must be bookended for fragmentation and reassembly to work). This also means a VSP4000 switch is required in order to support an ONA1101GT device performing this function.

3.3.2.6 Connectivity and Fault Management (CFM)

In Test 3, CFM was enabled on all VSP4000 switches and continuity testing was performed across the test environment using Layer 2 traceroute and Layer 2 tracetree. An important thing to note that with the Senetas Encryptors located in between VSP4K-A1 - VSP4K-W1 and VSP4K-A2 - VSP4K-W2 nodes is that CFM tests produce results consistent with the “Encryption Boundary/Zones” as described in Section 3.3.2.2 and illustrated in Figure 3.12.

Because the Senetas encryptors were configured to “bypass” (not encrypt) IS-IS control plane traffic, all SPB nodes in the test network were visible to each other. However, the encryption boundary prevents full CFM operation between the outside zone and inside zone. Performing Layer 2 traceroute and Layer 2 tracetree commands on VSP4K-A1 or A2 nodes results in only revealing the nodes in a path outside the encryption boundary. Nodes inside the encryption zone will not be seen as the data path is encrypted in that area of the network.

4. Device Configurations

4.1 VSP Switch Configurations

4.1.1 Switch software releases

All VSP series switches were loaded with the latest runtime and diagnostic images at the time of testing. The software release versions are:

- VSP4450's – release 5.0.0.0 int643
- VSP4850 (C1) – release 4.2.1 (GA)

4.1.2 SPB Node list

VSP4000 Nodes	System ID	Nick-name
VSP4K-W1	c050.0000.0001	c.00.01
VSP4K-W2	c050.0001.0001	c.01.01
VSP4K-A1	a030.0000.0001	a.01.03
VSP4K-A2	a030.0001.0001	a.01.04

Table 4.1 – VSP4000 SPB Node Information

- SPB Manual Area: **61.0200**
- SPB Backbone VLAN IDs: **4051** (primary) and **4052**.

NOTE: System ID's are automatically generated during SPB configuration, and is the recommended approach for customer SPB installations. For the purposes of testing in this document, system ID's were manually defined and configured.

4.1.3 VSP4K-W1 Configuration

Below is the configuration detail for VSP4450GSX switch VSP4K-W1. These are a summary of the unique/non-default configuration commands used in the Test 3 network environment.

Configuration Commands (summary):

```
boot config flags ftpd
boot config flags sshd
boot config flags telnetd
boot config flags tftpd
spbm
spbm ethertype 0x8100
auto-recover-delay 900
prompt "VSP4KW1"
password password-history 3
ssh
web-server enable
```

```
ip vrf spboip vrfid 1
router vrf spboip
ip ospf
exit
interface GigabitEthernet 1/1
encapsulation dot1q
exit
interface GigabitEthernet 1/48
encapsulation dot1q
exit

router isis
spbm 1
spbm 1 nick-name c.00.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
exit

vlan members remove 1 1/1-1/50 portmember
vlan create 1050 name "To_ONA_N" type port-mstprstp 0
vlan members 1050 1/12 portmember
interface Vlan 1050
ip address 50.10.0.1 255.255.255.0 1
exit
vlan create 1505 name "SPBoIPWAN" type port-mstprstp 0
vlan members 1505 1/23 portmember
interface Vlan 1505
vrf spboip
ip address 15.0.5.1 255.255.255.0 2
ip ospf enable
exit
vlan create 2005 name "Senetas OOB Key Mgmt" type port-mstprstp 0
vlan members 2005 1/5,1/7 portmember
vlan i-sid 2005 12982005
vlan create 2010 name "BLACK-Mgmt" type port-mstprstp 0
vlan i-sid 2010 12982010
interface Vlan 2010
ip address 20.10.50.100 255.255.255.0 0
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 1/1
default-vlan-id 0
no shutdown
fa
exit
interface GigabitEthernet 1/5
no shutdown
spanning-tree mstp edge-port true
exit
interface GigabitEthernet 1/7
no shutdown
spanning-tree mstp edge-port true
exit
interface GigabitEthernet 1/12
no shutdown
no spanning-tree mstp force-port-state enable
exit
```

```
interface GigabitEthernet 1/23
no shutdown
exit

interface GigabitEthernet 1/48
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable
exit

interface loopback 30
ip address 30 30.50.0.1/255.255.255.255
exit
interface loopback 15
ip address 15 15.50.0.1/255.255.255.255 vrf spboip
ip ospf 15 vrf spboip
exit

router isis
sys-name "VSP4kW1"
ip-source-address 30.50.0.1
ip-tunnel-source-address 15.50.0.1 port 1/1 mtu 1200 vrf spboip
is-type l1
system-id c050.0000.0001
manual-area 61.0200
exit
router isis enable

logical-intf isis 1 dest-ip 15.50.1.1 name To_VSP4KW2
isis
isis spbm 1
isis enable
exit

cfm spbm enable
router ospf
exit

router vrf spboip
ip ospf admin-state
exit
```

4.1.4 VSP4K-W2 Configuration

Below is the configuration detail for VSP4450GSX switch VSP4K-W2. These are a summary of the unique/non-default configuration commands used in the Test 3 network environment.

Configuration Commands (summary):

```
boot config flags ftpd
boot config flags sshd
boot config flags telnetd
boot config flags tftpd
```

```
spbm
spbm ethertype 0x8100
auto-recover-delay 900

prompt "VSP4KW2"
password password-history 3
ssh
web-server enable

ip vrf spboip vrfid 1
router vrf spboip
ip ospf
exit

interface GigabitEthernet 1/1
encapsulation dot1q
exit
interface GigabitEthernet 1/48
encapsulation dot1q
exit

router isis
spbm 1
spbm 1 nick-name c.01.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
exit

vlan members remove 1 1/1-1/50 portmember
vlan create 2 name "SPBMGT002" type port-mstprstp 0
interface Vlan 2
ip address 10.1.42.1 255.255.255.0 0
exit
vlan create 1050 name "To_ONA_N" type port-mstprstp 0
vlan members 1050 1/12 portmember
interface Vlan 1050
ip address 50.10.1.1 255.255.255.0 1
exit
vlan create 1515 name "SPBoIPWAN" type port-mstprstp 0
vlan members 1515 1/23 portmember
interface Vlan 1515
vrf spboip
ip address 15.1.5.1 255.255.255.0 2
ip ospf enable
exit
vlan create 2005 name "Senetas OOB Key Mgmt" type port-mstprstp 0
vlan members 2005 1/5,1/7 portmember
vlan i-sid 2005 12982005
vlan create 2010 name "BLACK-Mgmt" type port-mstprstp 0
vlan i-sid 2010 12982010
interface Vlan 2010
ip address 20.10.50.101 255.255.255.0 3
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 1/1
default-vlan-id 0
```

```
no shutdown
fa
exit
interface GigabitEthernet 1/5
no shutdown
spanning-tree mstp edge-port true
exit
interface GigabitEthernet 1/7
no shutdown
spanning-tree mstp edge-port true
exit
interface GigabitEthernet 1/12
no shutdown
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 1/23
no shutdown
exit
interface GigabitEthernet 1/48
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable
exit

interface loopback 30
ip address 30 30.50.1.1/255.255.255.255
exit
interface loopback 15
ip address 15 15.50.1.1/255.255.255.255 vrf spboip
ip ospf 15 vrf spboip
exit

router isis
sys-name "VSP4KW2"
ip-source-address 30.50.1.1
ip-tunnel-source-address 15.50.1.1 port 1/1 mtu 1200 vrf spboip
is-type l1
system-id c050.0000.0001
manual-area 61.0200
exit
router isis enable

logical-intf isis 1 dest-ip 15.50.1.1 name To_VSP4KW1
isis
isis spbm 1
isis enable
exit

cfm spbm enable
router ospf
exit

router vrf spboip
ip ospf admin-state
exit
```

4.1.5 VSP4K-A1 Configuration

Below is the configuration detail for VSP4450GSX switch VSP4K-A1. These are a summary of the unique/non-default configuration commands used in the Test 3 network environment.

Configuration Commands (summary):

```
boot config flags telnetd

spbm
spbm ethertype 0x8100

prompt "VSP4KA1"
password password-history 3
web-server enable

ip vrf green vrfid 10

interface GigabitEthernet 1/36-1/50
encapsulation dot1q
exit

router isis
spbm 1
spbm 1 nick-name a.00.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 multicast fwd-cache-timeout 60
spbm 1 ip enable
exit

vlan members remove 1 1/1-1/50 portmember
vlan create 10 name "VRF-Green" type port-mstprstp 0
vlan members 10 1/11-1/12 portmember
interface Vlan 10
vrf green
ip address 20.20.10.1 255.255.255.0 2
exit
vlan create 20 name "SPBVSN0020" type port-mstprstp 0
vlan members 20 1/1-1/10 portmember
vlan i-sid 20 12990020
interface Vlan 20
ip address 10.10.20.100 255.255.255.0 1
exit
vlan create 1010 name "RED Mgmt" type port-mstprstp 0
vlan i-sid 1010 12991010
interface Vlan 1010
ip address 10.10.50.100 255.255.255.0 0
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 1/1-1/36
no shutdown
exit
interface GigabitEthernet 1/37-1/50
default-vlan-id 0
no shutdown
```

```
isis
isis spbm 1
isis enable
no spanning-tree mstp  force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable
exit

interface loopback 30
ip address 30 30.30.0.1/255.255.255.255
exit

interface loopback 40
ip address 40 40.10.50.10/255.255.255.255 vrf green
exit

router isis
sys-name "VSP4KA1"
ip-source-address 30.30.0.1
is-type l1
system-id a030.0000.0001
manual-area 61.0200
exit
router isis enable

cfm spbm enable

router vrf green
ipvpn
i-sid 13990010
mvpn enable
ipvpn enable
exit

router vrf green
isis redistribute direct
isis redistribute direct metric 1
isis redistribute direct enable
exit

isis apply redistribute direct vrf green
```

4.1.6 VSP4K-A2 Configuration

Below is the configuration detail for VSP4450GSX switch VSP4K-A2. These are a summary of the unique/non-default configuration commands used in the Test 3 network environment.

Configuration Commands (summary):

```
boot config flags telnetd

spbm
spbm ethertype 0x8100

prompt "VSP4KA2"
password password-history 3
web-server enable

ip vrf green vrfid 10

interface GigabitEthernet 1/36-1/50
encapsulation dot1q
exit

router isis
spbm 1
spbm 1 nick-name a.01.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 multicast fwd-cache-timeout 60
spbm 1 ip enable
exit

vlan members remove 1 1/1-1/50 portmember
vlan create 10 name "VRF-Green" type port-mstprstp 0
vlan members 10 1/11-1/12 portmember
interface Vlan 10
vrf green
ip address 20.20.20.1 255.255.255.0 1
exit
vlan create 20 name "SPBVSN0020" type port-mstprstp 0
vlan members 20 1/1-1/10 portmember
vlan i-sid 20 12990020
vlan create 1010 name "RED-Mgmt" type port-mstprstp 0
vlan i-sid 1010 12991010
interface Vlan 1010
ip address 10.10.50.101 255.255.255.0 0
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 1/1-1/36
no shutdown
exit
interface GigabitEthernet 1/37-1/50
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
```

```
no spanning-tree mstp  force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable
exit

interface loopback 30
ip address 30 30.30.1.1/255.255.255.255
exit

interface loopback 40
ip address 40 40.10.50.13/255.255.255.255 vrf green
exit

router isis
sys-name "VSP4KA2"
ip-source-address 30.30.1.1
is-type l1
system-id a030.0001.0001
manual-area 61.0200
exit
router isis enable

cfm spbm enable

router vrf green
ipvpn
i-sid 13990010
mvpn enable
ipvpn enable
exit

router vrf green
isis redistribute direct
isis redistribute direct metric 1
isis redistribute direct enable
exit

isis apply redistribute direct vrf green
```

4.2 Senetas Encryptor Configurations

4.2.1 CN4010 Encryptor general information

Both CN4010 encryptors were licensed to operate at 1Gbps (line rate) and were configured with the following basic parameter settings:

- GA Encryptors activated and certified from CM7 Certificate Authority.
- VLAN encryption mode.
- Group auto-discovery enabled.
- Key management over the front panel management port.
- Bypass Reserved Multicast enabled.
- 09:00:2b:00:00:05 manually added to bypass MAC table (to bypass IS-IS traffic between VSP4K-A1 to VSP4K-W1, and VSP4K-A2 to VSP4K-W2).

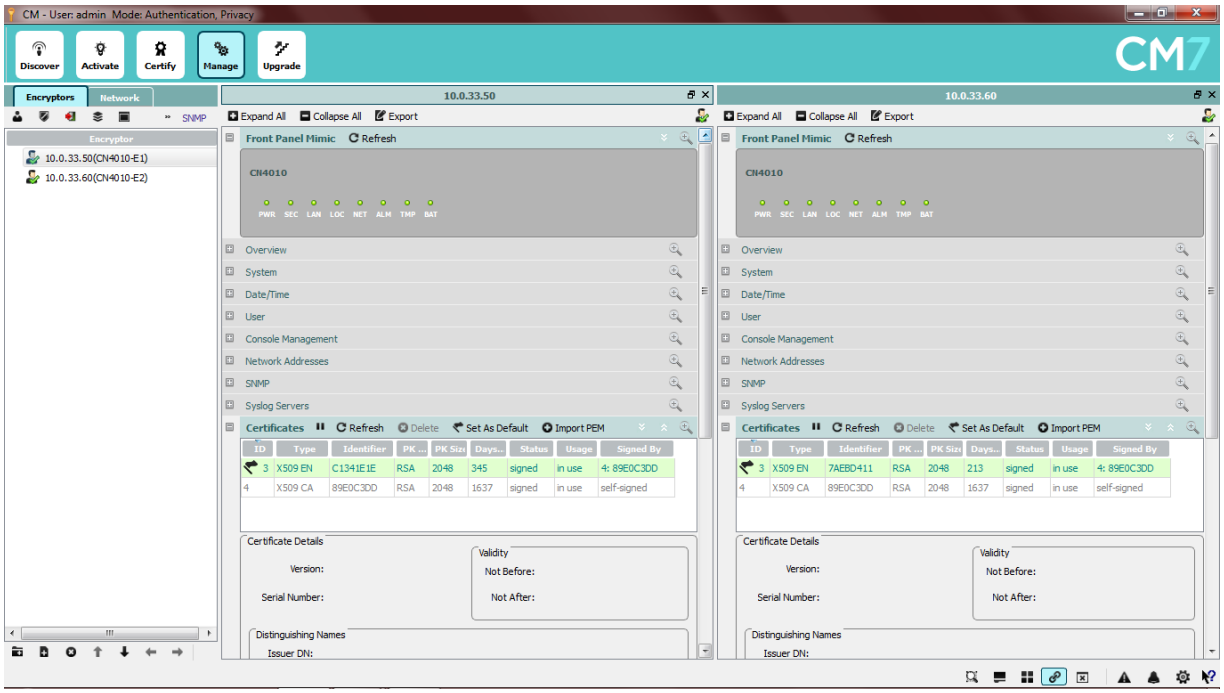
4.2.2 CN4010 Configuration

Below is the configuration detail for both CN4010 encryptors used in the Test 3 network environment. Although Senetas encryptors support a Command Line Interface via console, the following section details CN4010 configuration screens from the GUI based encryptor configuration tool CM7.

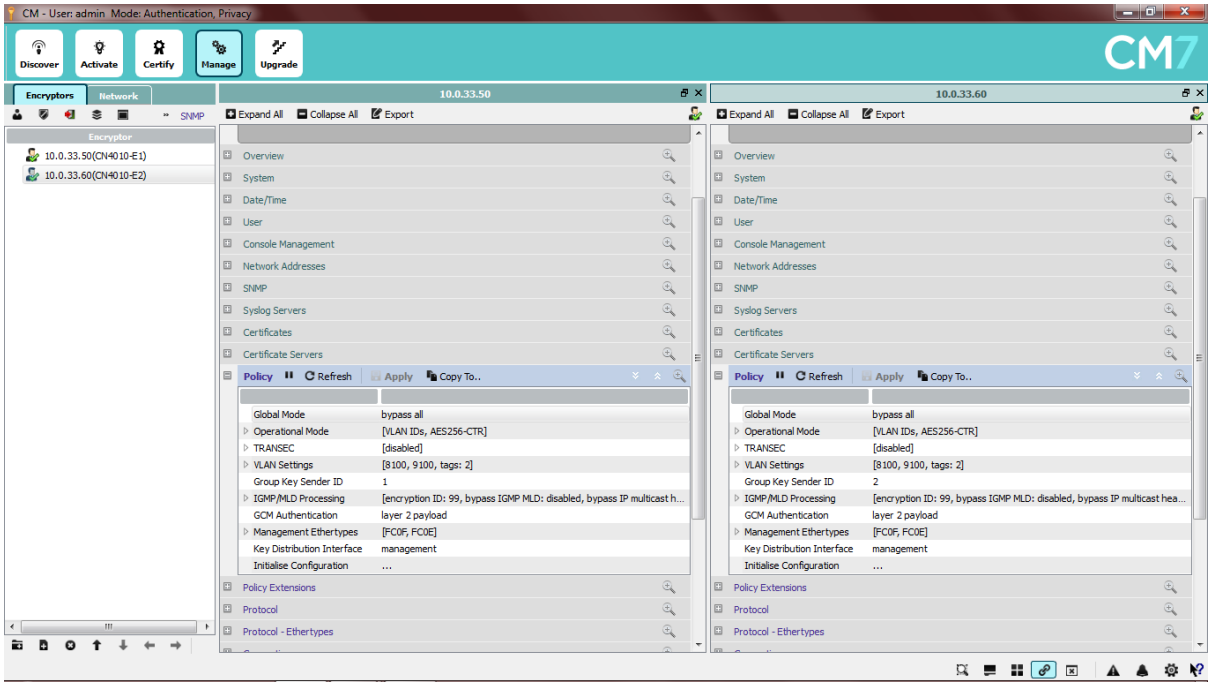
Encryptor management IP addresses:

- CN4010-E1 – management IP address 10.0.33.50
- CN4010-E2 – management IP address 10.0.33.60

Certificate Configuration (both encryptors – linked view)

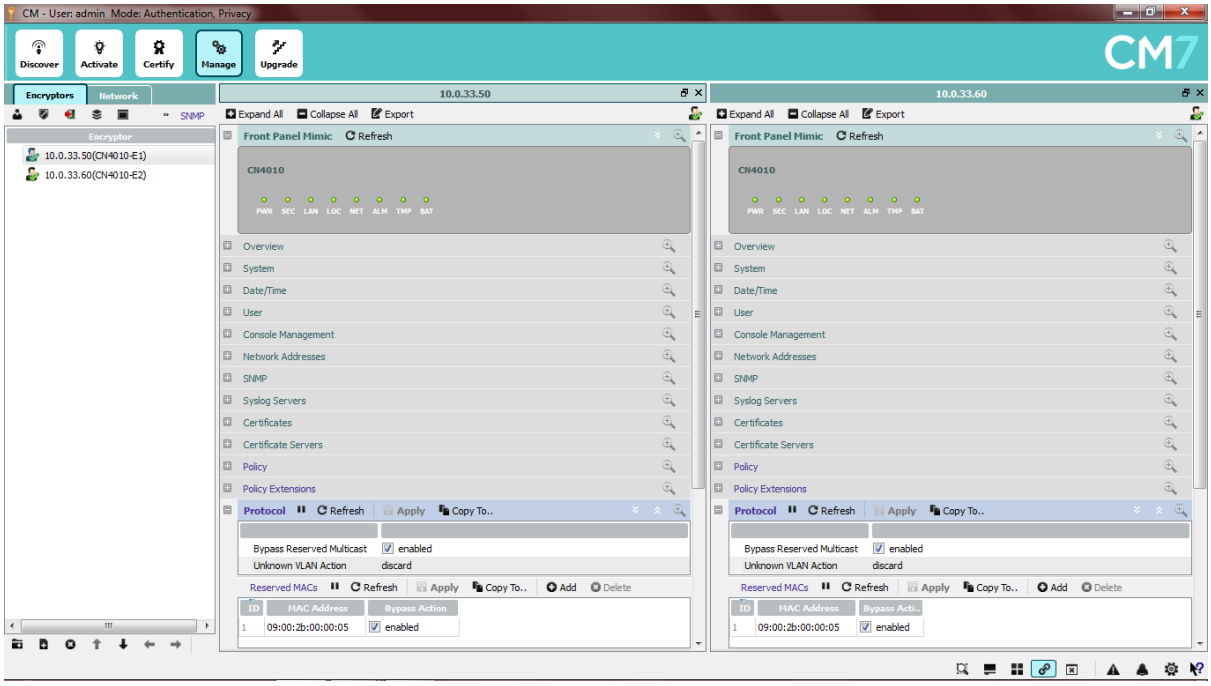


Encryption Mode Configuration (both encryptors – linked view)



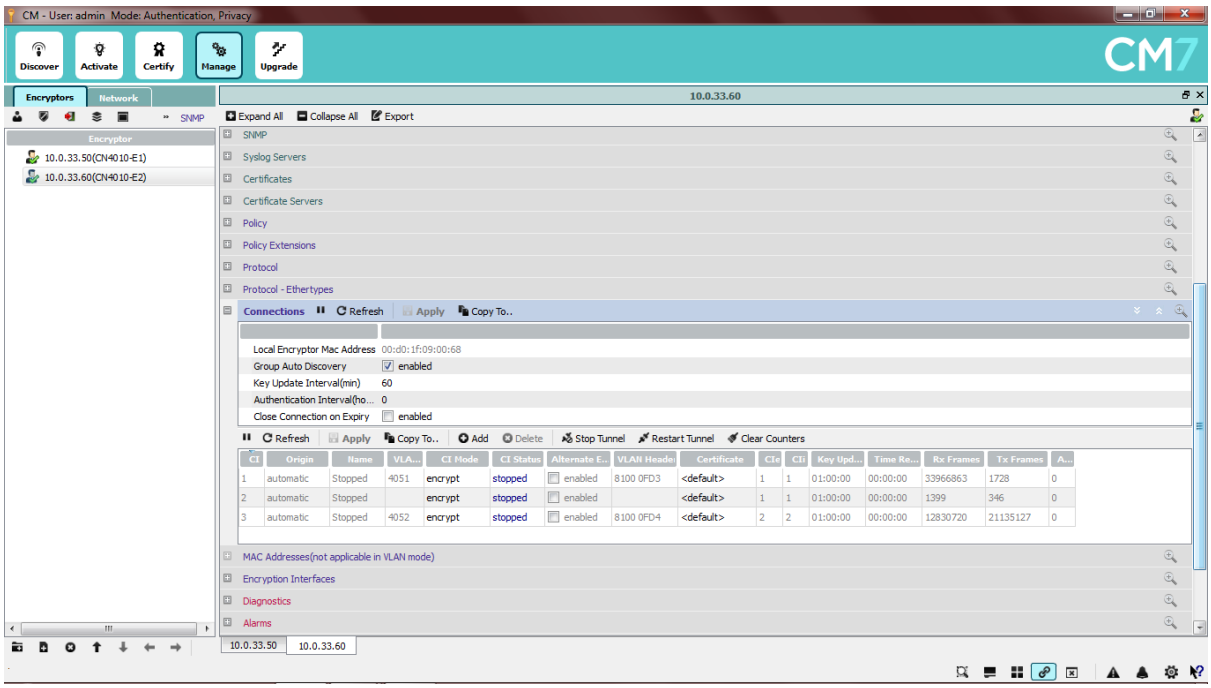
* Note encryption mode set to VLAN mode (VLAN ID's) with AES256-CTR and Key Distribution Interface set to management (the OOB Ethernet management interface) in Policy screen.

Encryption Bypass Configuration (both encryptors – linked view)



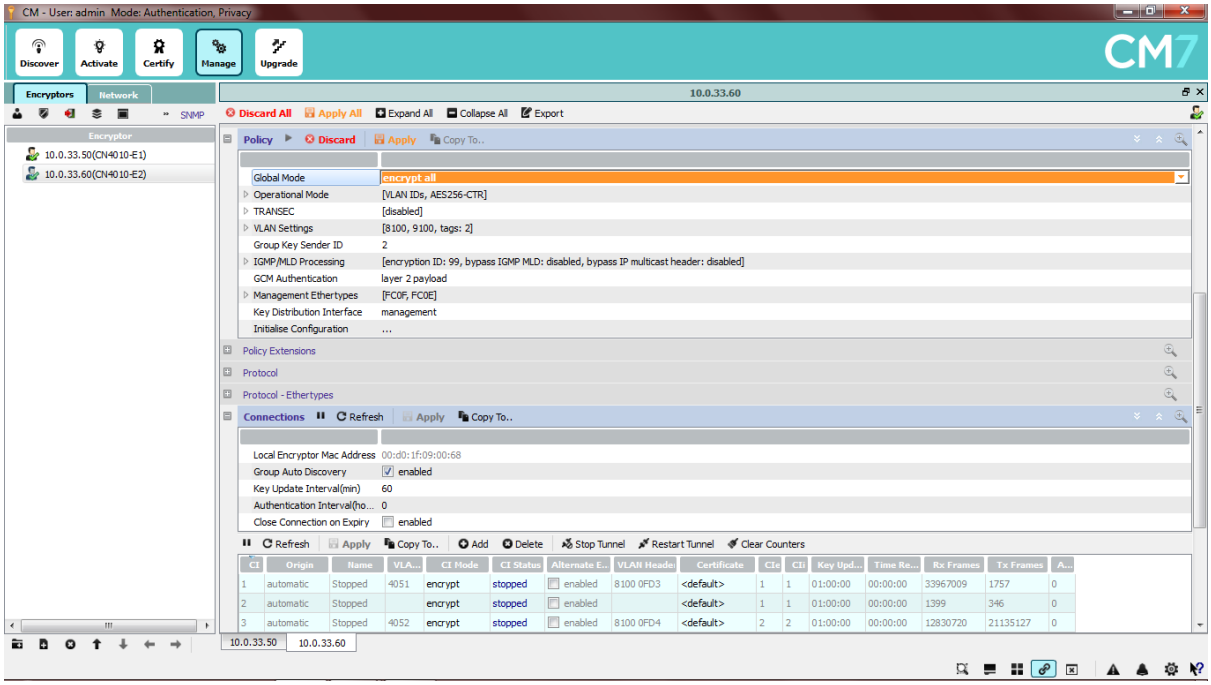
* Note "Bypass Action" in Protocol screen for MAC address 09:00:2b:00:00:05 (IS-IS well known MAC). This is manually entered to enable IS-IS control plane traffic to pass unencrypted between nodes on either side of CN4010 encryptors.

Connection Configuration and tunnel status view with Encryption off (CN4010-E2 view)



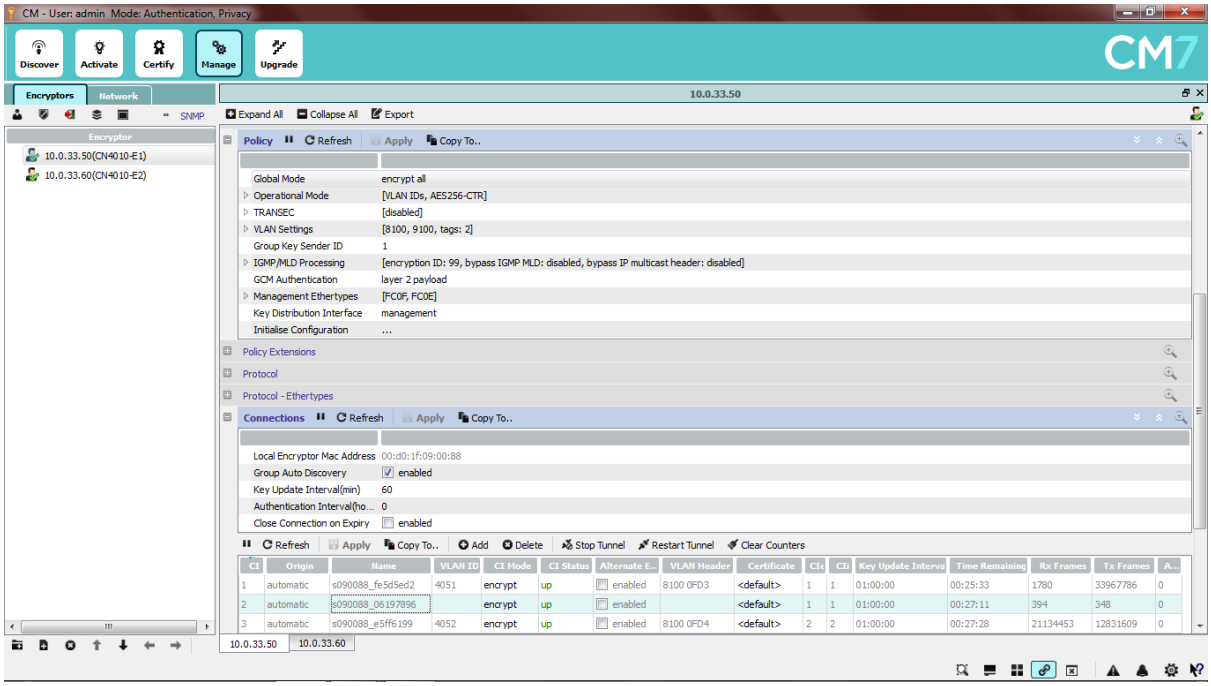
* Note in “Connections” configuration that VLAN 4051 and 4052 (SPB BVIDs) are configured for encryption. The middle row seen above is a default entry for untagged traffic and is not required.

Enabling Encryption from Policy screen and tunnel view (CN4010-E2 view)



* To start encrypting traffic, select “encrypt all” in Policy configuration and apply. Encrypted tunnels will restart and re-negotiate with all peer encryptors.

Encryption enabled with tunnel view and tunnel status up (CN4010-E1 view)



* Once encryption tunnels for VLANs 4051 and 4052 have successfully started with peer encryptors and the tunnel master / slave relationship is setup, Traffic within the designated VLANs will be encrypted and be forwarded out of the CN4010 Network port.

5. Network and Service Operations

This section contains a number of CLI show command outputs to illustrate the SPB network topology from a topology and operational perspective captured during Test 3.

It is important to note that whether Senetas encryptors have data encryption enabled or disabled that all IS-IS and SPB control plane information will be visible because IS-IS control plane traffic is not being encrypted between A1 – W1 nodes, and A2 – W2 nodes. This applies to control plane information only, which is being bypassed through the encryptors.

5.1.1 IS-IS information and node tables

ISIS Link State Database (LSDB) Information

```
#show isis lsdb

================================================================================
                                ISIS LSDB
================================================================================
LSP ID                          LEVEL     LIFETIME  SEQNUM     CHKSUM    HOST-NAME
--------------------------------------------------------------------------------
a030.0000.0001.00-00            1         380       0xcd       0x1075    VSP4KA1
a030.0000.0001.00-01            1         380       0xc4       0x490c    VSP4KA1
a030.0000.0001.00-05            1         674       0x5        0x220     VSP4KA1
a030.0001.0001.00-00            1         481       0x13       0xc34c    VSP4KA2
a030.0001.0001.00-01            1         481       0xe        0x25e1    VSP4KA2
a030.0001.0001.00-04            1         677       0x7        0x3fe1    VSP4KA2
c050.0000.0001.00-00            1         345       0xd1       0x9cf4    VSP4kW1
c050.0000.0001.00-01            1         345       0xc8       0xe1e1    VSP4kW1
c050.0001.0001.00-00            1         1181      0x13       0xf04c    VSP4kW2
c050.0001.0001.00-01            1         1181      0x11       0x5a1c    VSP4kW2

--------------------------------------------------------------------------------
Level-1 : 10 out of 18 Total Num of LSP Entries
Level-2 : 0 out of 0 Total Num of LSP Entries
--------------------------------------------------------------------------------
```

SPB Node Nick-names

```
#show isis spbm nick-name

================================================================================
                            ISIS SPBM NICK-NAME
================================================================================
LSP ID                          LIFETIME NICK-NAME HOST-NAME
--------------------------------------------------------------------------------
a030.0000.0001.00-00            701       a.00.01  VSP4KA1
a030.0001.0001.00-00            802       a.01.01  VSP4KA2
c050.0000.0001.00-00            665       c.00.01  VSP4kW1
c050.0001.0001.00-00            602       c.01.01  VSP4kW2

--------------------------------------------------------------------------------
 Total Number of Entries: 4
--------------------------------------------------------------------------------
```

5.1.2 SPB tables and information (encryption disabled)

Node VSP4K-A1 - SPB Unicast Forwarding Information Base Information

```
VSP4KA1:1#show isis spbm unicast-fib

================================================================================
                            SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION         BVLAN     SYSID             HOST-NAME       OUTGOING        COST
ADDRESS                                                         INTERFACE
--------------------------------------------------------------------------------
a0:30:00:00:00:01   4051      a030.0000.0001    VSP4KA1         cpp             0
a2:00:01:ff:ff:ff   4051      a030.0000.0001    VSP4KA1         cpp             0
a0:30:00:00:00:01   4052      a030.0000.0001    VSP4KA1         cpp             0
a2:00:01:ff:ff:ff   4052      a030.0000.0001    VSP4KA1         cpp             0
a0:30:00:01:00:01   4051      a030.0001.0001    VSP4KA2         1/48            20020
a2:01:01:ff:ff:ff   4051      a030.0001.0001    VSP4KA2         1/48            20020
a0:30:00:01:00:01   4052      a030.0001.0001    VSP4KA2         1/48            20020
a2:01:01:ff:ff:ff   4052      a030.0001.0001    VSP4KA2         1/48            20020
c0:50:00:00:00:01   4051      c050.0000.0001    VSP4kW1         1/48            10
c2:00:01:ff:ff:ff   4051      c050.0000.0001    VSP4kW1         1/48            10
c0:50:00:00:00:01   4052      c050.0000.0001    VSP4kW1         1/48            10
c2:00:01:ff:ff:ff   4052      c050.0000.0001    VSP4kW1         1/48            10
c0:50:00:01:00:01   4051      c050.0001.0001    VSP4kW2         1/48            20010
c2:01:01:ff:ff:ff   4051      c050.0001.0001    VSP4kW2         1/48            20010
c0:50:00:01:00:01   4052      c050.0001.0001    VSP4kW2         1/48            20010
c2:01:01:ff:ff:ff   4052      c050.0001.0001    VSP4kW2         1/48            20010

--------------------------------------------------------------------------------
 Total number of SPBM UNICAST FIB entries 16
--------------------------------------------------------------------------------
```

Node VSP4K-A1 - SPB Multicast Forwarding Information Base Information

```
VSP4KA1:1#show isis spbm multicast-fib

================================================================================================
                                  SPBM MULTICAST FIB ENTRY INFO
================================================================================================
MCAST DA            ISID      BVLAN SYSID           HOST-NAME      OUTGOING-INTERFACES   INCOMING
                                                                                         INTERFACE
------------------------------------------------------------------------------------------------
a3:00:01:c6:36:44   12990020  4052  a030.0000.0001  VSP4KA1        1/1,1/3,1/48          cpp
a3:00:01:c6:3a:22   12991010  4052  a030.0000.0001  VSP4KA1        1/48                  cpp
a3:01:01:c6:36:44   12990020  4052  a030.0001.0001  VSP4KA2        1/1,1/3               1/48
a3:01:01:c6:3a:22   12991010  4052  a030.0001.0001  VSP4KA2                              1/48

------------------------------------------------------------------------------------------------
 Total number of SPBM MULTICAST FIB entries 4
------------------------------------------------------------------------------------------------
```

Node VSP4K-W1 - SPB Unicast Forwarding Information Base Information

```
VSP4KW1:1#show isis spbm unicast-fib

================================================================================
                            SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION         BVLAN     SYSID             HOST-NAME       OUTGOING        COST
ADDRESS                                                         INTERFACE
--------------------------------------------------------------------------------
a0:30:00:00:00:01   4051      a030.0000.0001    VSP4KA1         1/48            10
a2:00:01:ff:ff:ff   4051      a030.0000.0001    VSP4KA1         1/48            10
a0:30:00:00:00:01   4052      a030.0000.0001    VSP4KA1         1/48            10
a2:00:01:ff:ff:ff   4052      a030.0000.0001    VSP4KA1         1/48            10
a0:30:00:01:00:01   4051      a030.0001.0001    VSP4KA2         To_VSP4KW2      20010
a2:01:01:ff:ff:ff   4051      a030.0001.0001    VSP4KA2         To_VSP4KW2      20010
a0:30:00:01:00:01   4052      a030.0001.0001    VSP4KA2         To_VSP4KW2      20010
a2:01:01:ff:ff:ff   4052      a030.0001.0001    VSP4KA2         To_VSP4KW2      20010
c0:50:00:00:00:01   4051      c050.0000.0001    VSP4kW1         cpp             0
c2:00:01:ff:ff:ff   4051      c050.0000.0001    VSP4kW1         cpp             0
c0:50:00:00:00:01   4052      c050.0000.0001    VSP4kW1         cpp             0
c2:00:01:ff:ff:ff   4052      c050.0000.0001    VSP4kW1         cpp             0
c0:50:00:01:00:01   4051      c050.0001.0001    VSP4kW2         To_VSP4KW2      20000
c2:01:01:ff:ff:ff   4051      c050.0001.0001    VSP4kW2         To_VSP4KW2      20000
c0:50:00:01:00:01   4052      c050.0001.0001    VSP4kW2         To_VSP4KW2      20000
c2:01:01:ff:ff:ff   4052      c050.0001.0001    VSP4kW2         To_VSP4KW2      20000
--------------------------------------------------------------------------------
Total number of SPBM UNICAST FIB entries 16
--------------------------------------------------------------------------------
```

Node VSP4K-W1 - SPB Multicast Forwarding Information Base Information

```
VSP4KW1:1#show isis spbm multicast-fib

================================================================================================
                                  SPBM MULTICAST FIB ENTRY INFO
================================================================================================
MCAST DA            ISID      BVLAN SYSID           HOST-NAME    OUTGOING-INTERFACES   INCOMING
                                                                                       INTERFACE
------------------------------------------------------------------------------------------------
a3:00:01:c6:36:44   12990020  4052  a030.0000.0001  VSP4KA1      To_VSP4KW2            1/48
a3:00:01:c6:3a:22   12991010  4052  a030.0000.0001  VSP4KA1      To_VSP4KW2            1/48
a3:01:01:c6:36:44   12990020  4052  a030.0001.0001  VSP4KA2      1/48                  To_VSP4KW2
a3:01:01:c6:3a:22   12991010  4052  a030.0001.0001  VSP4KA2      1/48                  To_VSP4KW2
c3:00:01:c6:16:f5   12982005  4051  c050.0000.0001  VSP4kW1      1/5,To_VSP4KW2        cpp
c3:00:01:c6:16:fa   12982010  4052  c050.0000.0001  VSP4kW1      To_VSP4KW2            cpp
c3:01:01:c6:16:f5   12982005  4051  c050.0001.0001  VSP4kW2      1/5                   To_VSP4KW2
c3:01:01:c6:16:fa   12982010  4052  c050.0001.0001  VSP4kW2      -                     To_VSP4KW2
------------------------------------------------------------------------------------------------
Total number of SPBM MULTICAST FIB entries 8
------------------------------------------------------------------------------------------------
```

Node VSP4K-A1 - SPB Unicast Tree for B-VLAN 4051 (same output for 4052)

```
VSP4KW1:1#show isis spbm unicast-tree 4051

Node:a030.0001.0001 (VSP4KA2) -> Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001
(VSP4kW1) -> ROOT
Node:c050.0000.0001 (VSP4kW1) -> ROOT
Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001 (VSP4kW1) -> ROOT
```

Node VSP4K-A1 - SPB Service ID's (I-SIDs)

```
VSP4KA1:1#show isis spbm i-sid all

================================================================================
                                SPBM ISID INFO
================================================================================
ISID      SOURCE NAME   VLAN   SYSID                TYPE         HOST_NAME
--------------------------------------------------------------------------------
12990020  a.00.01       4052   a030.0000.0001       config       VSP4KA1
12991010  a.00.01       4052   a030.0000.0001       config       VSP4KA1
12990020  a.01.01       4052   a030.0001.0001       discover     VSP4KA2
12991010  a.01.01       4052   a030.0001.0001       discover     VSP4KA2

--------------------------------------------------------------------------------
 Total number of SPBM ISID entries configured: 2
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries discovered: 2
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries: 4
--------------------------------------------------------------------------------
```

Node VSP4K-W1 - SPB Service ID's (I-SIDs)

```
VSP4KW1:1#show isis spbm i-sid all

================================================================================
                                SPBM ISID INFO
================================================================================
ISID      SOURCE NAME   VLAN   SYSID                TYPE         HOST_NAME
--------------------------------------------------------------------------------
12990020  a.00.01       4052   a030.0000.0001       discover     VSP4KA1
12991010  a.00.01       4052   a030.0000.0001       discover     VSP4KA1
12990020  a.01.01       4052   a030.0001.0001       discover     VSP4KA2
12991010  a.01.01       4052   a030.0001.0001       discover     VSP4KA2
12982005  c.00.01       4051   c050.0000.0001       config       VSP4kW1
12982010  c.00.01       4052   c050.0000.0001       config       VSP4kW1
12982005  c.01.01       4051   c050.0001.0001       discover     VSP4kW2
12982010  c.01.01       4052   c050.0001.0001       discover     VSP4kW2

--------------------------------------------------------------------------------
 Total number of SPBM ISID entries configured: 2
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries discovered: 6
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries: 8
--------------------------------------------------------------------------------
```

Note in above table that I-SIDs with a path through node VSP4K-W1 are visible in addition to I-SIDs terminating on the node.

5.1.3 IP information

The following CLI outputs show the various IP address views from ISIS LSDB and from a general IP routing view from the GRT and VRFs.

Node VSP4KA1 – ISIS LSDB for IP Unicast

```
VSP4KA1:1#show isis lsdb ip-unicast

================================================================================
                        ISIS IP-UNICAST-ROUTE SUMMARY
================================================================================
                            PREFIX          METRIC    TLV   LSP   HOST
I-SID     ADDRESS           LENGTH  METRIC  TYPE      TYPE  FRAG  NAME
--------------------------------------------------------------------------------
-         30.30.0.1         32      1       Internal  135   0x2   VSP4KA1
13990010  40.10.50.10       32      1       Internal  184   0x3   VSP4KA1
-         30.30.1.1         32      1       Internal  135   0x2   VSP4KA2
-         10.10.100.0       24      1       Internal  135   0x2   VSP4KA2
-         10.10.50.0        24      1       Internal  135   0x2   VSP4KA2
13990010  40.10.50.13       32      1       Internal  184   0x3   VSP4KA2
-         30.50.0.1         32      1       Internal  135   0x2   VSP4kW1
-         30.50.1.1         32      1       Internal  135   0x2   VSP4kW2
--------------------------------------------------------------------------------
8 out of 8 Total Num of Entries
```

Node VSP4KA1 – IP Route Table for GRT

```
VSP4KA1:1#show ip route

================================================================================================
                                  IP Route - GlobalRouter
================================================================================================
                                                 NH                    INTER
DST             MASK             NEXT            VRF/ISID         COST FACE    PROT AGE TYPE PRF
------------------------------------------------------------------------------------------------
10.10.20.0      255.255.255.0    10.10.20.100    -                1    20      LOC  0   DB   0
10.10.50.0      255.255.255.0    10.10.50.100    -                1    1010    LOC  0   DB   0
10.10.100.0     255.255.255.0    VSP4KA2         GlobalRouter     20020 4051   ISIS 0   IBS  7
30.30.0.1       255.255.255.255 30.30.0.1        -                1    0       LOC  0   DB   0
30.30.1.1       255.255.255.255 VSP4KA2          GlobalRouter     20020 4051   ISIS 0   IBS  7
30.50.0.1       255.255.255.255 VSP4kW1          GlobalRouter     10    4051   ISIS 0   IBS  7
30.50.1.1       255.255.255.255 VSP4kW2          GlobalRouter     20010 4051   ISIS 0   IBS  7

7 out of 7 Total Num of Route Entries, 7 Total Num of Dest Networks displayed.
------------------------------------------------------------------------------------------------
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW, F=Replaced by FTN, V=IPVPN Route, S=SPBM Route
PROTOCOL Legend:
v=Inter-VRF route redistributed
```

5.1.4 CFM Layer 2 Connectivity information

The following CLI outputs show the various results of Layer 2 ping and Layer 2 traceroute commands from nodes VSP4K-A1 and VSP4K-W1, with no encryption and then with encryption enabled.

5.1.4.1 CFM outputs with no encryption

The outputs below are examples of basic connectivity and reachability with no encryption. Both Senetas encryptors are in “bypass” mode for all traffic and are transparent to the network.

Node VSP4KA1 – Layer 2 Ping (from node A1 to node A2, three hops away)

```
VSP4KA1:1#l2 ping ip 30.30.1.1

 Please wait for l2ping to complete or press any key to abort

L2 PING  Statistics : IP 30.30.1.1, paths found 1, paths attempted 1
================================================================================
                                          TX    RX    PERCENT  ROUND TRIP TIME
VLAN NEXT HOP                             PKTS  PKTS  LOSS     MIN/MAX/AVE (us)
================================================================================
4051 VSP4KA2           (a0:30:00:01:00:01)  1     1       0.00%  2838/2838/2838.00
```

Node VSP4KA1 – Layer 2 Ping (similar to last command, using router node name)

```
VSP4KA1:1#l2 ping vlan 4052 routernodename VSP4KA2

 Please wait for l2ping to complete or press any key to abort

----a0:30:00:01:00:01       L2 PING Statistics----  0(64) bytes of data
1 packets transmitted, 1 packets received,   0.00% packet loss
  round-trip (us)    min/max/ave/stdv =  2590/2590/2590.00/ 0.00
```

Node VSP4KA1 – Layer 2 Traceroute

```
VSP4KA1:1#l2 traceroute vlan 4052 routernodename VSP4KA2

 Please wait for l2traceroute to complete or press any key to abort

l2traceroute to VSP4KA2  (a0:30:00:01:00:01),  vlan 4052
0    VSP4KA1             (a0:30:00:00:00:01)
1    VSP4kW1             (c0:50:00:00:00:01)
2    VSP4kW2             (c0:50:00:01:00:01)
3    VSP4KA2             (a0:30:00:01:00:01)
```

Node VSP4KA1 – SPBM Unicast Tree for B-VLAN 4052

```
VSP4KA1:1#show isis spbm unicast-tree 4052

Node:a030.0001.0001 (VSP4KA2) -> Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001
(VSP4kW1) -> ROOT
Node:c050.0000.0001 (VSP4kW1) -> ROOT
Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001 (VSP4kW1) -> ROOT
```

Node VSP4KA1 – Layer 2 Tracetree on B-VLAN 4052 for ISID 12990020

```
VSP4KA1:1#l2 tracetree 4052 12990020 routernodename VSP4KA1

 Please wait for l2tracetree to complete or press any key to abort

l2tracetree to a3:00:01:c6:36:44, vlan 4052 i-sid 12990020 nickname a.00.01 hops 64
1   VSP4KA1          a0:30:00:00:00:01 -> VSP4kW1          c0:50:00:00:00:01
2   VSP4kW1          c0:50:00:00:00:01 -> VSP4kW2          c0:50:00:01:00:01
3   VSP4kW2          c0:50:00:01:00:01 -> VSP4KA2          a0:30:00:01:00:01
```

5.1.4.2 CFM outputs with Encryption enabled

As expected, when data encryption is enabled between the A1 – W1 and A2 –W2 nodes, the data path is only contiguous between nodes that are outside the encryption boundary or between the inner nodes within the encryption boundary.

Node VSP4KA1 – SPBM Unicast Tree for B-VLAN 4052

```
VSP4KA1:1#show isis spbm unicast-tree 4052

Node:a030.0001.0001 (VSP4KA2) -> Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001
(VSP4kW1) -> ROOT
Node:c050.0000.0001 (VSP4kW1) -> ROOT
Node:c050.0001.0001 (VSP4kW2) -> Node:c050.0000.0001 (VSP4kW1) -> ROOT
```

Node VSP4KA1 – Layer 2 Tracetree on B-VLAN 4052 for ISID 12990020

```
VSP4KA1:1#l2 tracetree 4052 12990020 routernodename VSP4KA1

 Please wait for l2tracetree to complete or press any key to abort

l2tracetree to a3:00:01:c6:36:44, vlan 4052 i-sid 12990020 nickname a.00.01 hops 64
1   VSP4KA1           a0:30:00:00:00:01 -> VSP4KA2           a0:30:00:01:00:01
```

Note tracetree output across network now that encryption is enabled. Nodes VSP4KW1 and VSP4KW2 are inside the encryption boundary and therefore are not seen by the layer 2 traceroute continuity test.

Node VSP4KA1 – Layer 2 Traceroute on B-VLAN 4052 to node VSP4KA2

```
VSP4KA1:1#l2 traceroute vlan 4052 routernodename VSP4KA2

 Please wait for l2traceroute to complete or press any key to abort

l2traceroute to VSP4KA2  (a0:30:00:01:00:01),  vlan 4052
0    VSP4KA1             (a0:30:00:00:00:01)
1    VSP4KA2             (a0:30:00:01:00:01)
```

Likewise for the layer 2 tracetree output across network now that encryption is enabled. Nodes VSP4KW1 and VSP4KW2 are inside the encryption boundary and are not seen by the layer 2 traceroute test. The output only shows nodes outside the encryption boundary.

Node VSP4KA1 – Layer 2 Ping on B-VLAN 4052 to node VSP4KA2

```
VSP4KA1:1# l2 ping vlan 4052 routernodename VSP4KA2

 Please wait for l2ping to complete or press any key to abort

----a0:30:00:01:00:01       L2 PING Statistics----  0(64) bytes of data
1 packets transmitted, 1 packets received,   0.00% packet loss
  round-trip (us)    min/max/ave/stdv =  2192/2192/2192.00/ 0.00
```

*Pinging end to end is still ok to test reachability.

Node VSP4KA1 – Layer 2 Ping on B-VLAN 4052 to node VSP4KW1 & VSP4KW2

```
VSP4KA1:1# l2 ping vlan 4052 routernodename VSP4kW1

 Please wait for l2ping to complete or press any key to abort

Error: Lookup Failure for RouterNodeName or SystemIdMac.

VSP4KA1:1# l2 ping vlan 4052 routernodename VSP4kW2

 Please wait for l2ping to complete or press any key to abort

Error: Lookup Failure for RouterNodeName or SystemIdMac.
```

Attempting layer 2 ping of nodes VSP4K-W1 or VSP4K-W2 which are inside the encryption boundary yields the above output as they cannot be seen or resolved.

Attempting a straight “ping” of an IP address on any node inside the encryption boundary from a node outside will also fail. Ping will only succeed to nodes outside the encryption boundary – despite the output of a GRT or VRF `show ip route` command.

5.1.5 Multicast testing information

Operational testing and view of IP multicast running over the Test 3 network environment over Layer 3 VSN 13990010 and VRF Green with dynamic data I-SIDs created by IP multicast virtualization. The outputs contained in this section are with encryption enabled in the network core, but has no relevance or impact to the visibility, operation and performance of multicast running end to end over the test environment.

Node VSP4KA2 – SPB Multicast Summary

```
VSP4KA2:1#show isis spb-mcast-summary

================================================================================
                            SPB Multicast - Summary
================================================================================
SCOPE    SOURCE          GROUP           DATA            LSP  HOST
I-SID    ADDRESS         ADDRESS         I-SID     BVID  FRAG NAME
--------------------------------------------------------------------------------
13990010 20.20.10.80     234.5.6.7       16150002  4052  0x4  VSP4KA1
13990010 20.20.20.90     239.255.255.250 16000001  4051  0x5  VSP4KA2
--------------------------------------------------------------------------------
2 out of 2 Total Num of Entries
```

The Multicast Group Address 239.255.255.250 is being propagated from Microsoft Windows version 7 on Laptop “PC-B” (IP 20.20.20.90) connected directly to node VSP4KA2 in VLAN 10, VRF Green and I-SID 13990010.

Node VSP4KA2 - Multicast info for GRT

```
VSP4KA2:1#show ip igmp interface

================================================================================
                          Igmp Interface - GlobalRouter
================================================================================
       QUERY              OPER            QUERY   WRONG            LASTMEM
IF     INTVL STATUS VERS. VERS QUERIER    MAXRSPT QUERY JOINS ROBUST QUERY MODE
--------------------------------------------------------------------------------
V1010  125    inact  2     2   0.0.0.0    100     0     0     2      10
V4051  125    inact  2     2   0.0.0.0    100     0     0     2      10
V4052  125    inact  2     2   0.0.0.0    100     0     0     2      10

3 out of 3 entries displayed
```

Node VSP4KA2 - Multicast info for VRF Green

```
VSP4KA2:1#show ip igmp interface vrf green

================================================================================
                           Igmp Interface - VRF green
================================================================================
       QUERY              OPER            QUERY   WRONG            LASTMEM
IF     INTVL STATUS VERS. VERS QUERIER    MAXRSPT QUERY JOINS ROBUST QUERY MODE
--------------------------------------------------------------------------------
V10    125    active 2     2   20.20.20.1 100     0     10    2      10    routed-spb

1 out of 1 entries displayed
```

```
VSP4KA2:1#show ip igmp group interface vrf green

================================================================================
                             Igmp Group - VRF green
================================================================================
GRPADDR         INPORT          MEMBER          EXPIRATION TYPE
--------------------------------------------------------------------------------
234.5.6.7       V10-1/11        20.20.20.90     226        Dynamic
239.255.255.250 V10-1/11        20.20.20.90     225        Dynamic

2 out of 2 group Receivers displayed

Total number of unique groups 2
```

```
VSP4KA2:1#show ip igmp sender vrf green

================================================================================
                             Igmp Sender - VRF green
================================================================================
                                                PORT/
GRPADDR         IFINDEX    MEMBER               MLT        STATE
--------------------------------------------------------------------------------
239.255.255.250 Vlan 10    20.20.20.90          1/11       NOTFILTERED

1 out of 1 entries displayed
```

6. Conclusion

In conclusion of the testing, Avaya's SPB Fabric Connect over IP (SPBoIP) performed exactly as designed when using VSP4000 routing switch products with the ONA1101GT. When combined, these products provide both IP/VXLAN tunneling capability in conjunction with IP packet fragmentation and reassembly functions to support a large range of SPB solutions that need to be extended over IP networks, either across a large enterprise network or over a Wide Area Network using IP-VPN services.

In addition to supporting SPB over an IP WAN, Senetas Ethernet encryptors were included in testing to validate a reference architecture and deployment model to provide data protection by encrypting data traffic running over public infrastructure, such as any IP WAN based service. All Senetas Ethernet encryptors are certified to very high levels catering for military, government and financial sectors and are also ideally suitable for regular enterprise networks.

This document is available to use as a reference architecture guide for Avaya & Partner Architects, Network Specialists, Sales Engineers and Sales Representatives.

© 2015 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.