# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>1</td>
</tr>
<tr>
<td>Objective</td>
<td>1</td>
</tr>
<tr>
<td>Glossary</td>
<td>1</td>
</tr>
<tr>
<td>Network Services Description</td>
<td>3</td>
</tr>
<tr>
<td>Network Architecture Overview</td>
<td>5</td>
</tr>
<tr>
<td>Core</td>
<td>7</td>
</tr>
<tr>
<td>Distribution</td>
<td>7</td>
</tr>
<tr>
<td>Access</td>
<td>8</td>
</tr>
<tr>
<td>Service Design</td>
<td>8</td>
</tr>
<tr>
<td>Redundancy</td>
<td>8</td>
</tr>
<tr>
<td>SPB BCB Design</td>
<td>8</td>
</tr>
<tr>
<td>Base config</td>
<td>8</td>
</tr>
<tr>
<td>SPB Service config</td>
<td>10</td>
</tr>
<tr>
<td>IP config</td>
<td>12</td>
</tr>
<tr>
<td>Special Services</td>
<td>12</td>
</tr>
<tr>
<td>Statistics</td>
<td>12</td>
</tr>
<tr>
<td>VLAN Translation</td>
<td>13</td>
</tr>
<tr>
<td>Troubleshooting and Monitoring</td>
<td>13</td>
</tr>
<tr>
<td>Common Show Commands</td>
<td>13</td>
</tr>
<tr>
<td>Common Troubleshooting Commands (CLI and OmniVista)</td>
<td>14</td>
</tr>
<tr>
<td>Conclusion</td>
<td>15</td>
</tr>
<tr>
<td>More Information</td>
<td>16</td>
</tr>
</tbody>
</table>
INTRODUCTION

Purpose
The purpose of this paper is to explain the use case of Shortest Path Bridging (SPB) (IEEE 802.1aq) outside of the data center in the WAN or MAN, the detailed design and implementation requirements including Alcatel-Lucent Operating System (AOS) for OmniSwitch® configuration examples, and the benefits of using SPB as a WAN/MAN protocol.

Objective
A key objective in the deployment of SPB technology across any metro backbone is to provide a consistent enabling foundation to support current and emerging needs of the network. A consistent approach to architecture and design allows for the deployment of new capabilities on a system-wide basis, with confidence that every node in the system is able to implement them. In addition, future growth or additions to the network can be accommodated in a seamless and non-disruptive manner. This document outlines our recommended methods for deploying SPB in a MAN.

Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AOS</td>
<td>Alcatel-Lucent Operating System</td>
</tr>
<tr>
<td>BCB</td>
<td>Backbone Core Bridge</td>
</tr>
<tr>
<td>BEB</td>
<td>Backbone Edge Bridge</td>
</tr>
<tr>
<td>BFD</td>
<td>Bi-directional Forwarding Detection</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BSR</td>
<td>Bootstrap Router</td>
</tr>
<tr>
<td>BVLAN</td>
<td>Backbone VLAN</td>
</tr>
<tr>
<td>CE</td>
<td>Customer Edge</td>
</tr>
<tr>
<td>CVLAN</td>
<td>Customer VLAN</td>
</tr>
<tr>
<td>DC</td>
<td>Data Center</td>
</tr>
<tr>
<td>ECMP</td>
<td>Equal Cost Multi Path</td>
</tr>
<tr>
<td>ECT</td>
<td>Equal Cost Tree</td>
</tr>
<tr>
<td>FDB</td>
<td>Forwarding Database</td>
</tr>
<tr>
<td>GRT</td>
<td>Global Routing Table</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>ISID</td>
<td>Instance Service Identifier</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPVPN Lite</td>
<td>Internet Protocol Virtual Private Network Lite</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System to Intermediate System</td>
</tr>
<tr>
<td>L3VPN</td>
<td>Layer Three Virtual Private Network</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LINKAGG</td>
<td>Link Aggregation</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NNI</td>
<td>Network to Network Interface</td>
</tr>
<tr>
<td>O&amp;M</td>
<td>Operations and Maintenance</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations Administration and Maintenance</td>
</tr>
<tr>
<td>OOB</td>
<td>Out Of Band</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>PBB</td>
<td>Provider Backbone Bridging</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>PIM Sparse Mode</td>
</tr>
<tr>
<td>PIM-SSM</td>
<td>PIM Source Specific Multicast</td>
</tr>
<tr>
<td>POP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>QinQ</td>
<td>IEEE 802.1ad Q in Q</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RP</td>
<td>Rendezvous Point</td>
</tr>
<tr>
<td>SAA</td>
<td>Service Assurance Agent</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Port</td>
</tr>
<tr>
<td>SDP</td>
<td>Service Distribution Point</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SPBM</td>
<td>Shortest Path Bridging MAC</td>
</tr>
<tr>
<td>SPF</td>
<td>Shortest Path First</td>
</tr>
</tbody>
</table>
Modern MAN/WAN network designs are typically connected using either private fiber or carrier service offerings. The difference between a MAN and a WAN can typically be defined by ownership of the interconnections or monthly recurring charged (MRC) leases of the interconnections. A WAN typically has MRCs like Metro-E services from a carrier and a MAN is usually leased or dark fiber and can loosely be defined as a large extended campus. These terms are used interchangeably but have the same meaning throughout this document. These networks typically require high availability and are critical assets to service the business functions in almost every industry vertical. The physical medium is usually Ethernet and there are two common and one less common multipath options used to interconnect WAN and MAN networks. Layer three routing such as open shortest path first (OSPF) or border gateway protocol (BGP), layer two SPB, and multiprotocol label switching (MPLS). MPLS is an expensive and complex offering that is typically relegated to carriers. Enterprises can use carrier MPLS offerings to connect or extend a layer 3 or layer 2 network between locations. For the purposes of this paper we will focus on non-MPLS as our recommended enterprise WAN/MAN protocol option. Regardless of which protocol is chosen (OSPF/BGP/SPB), the OmniSwitch 10K, 6900, and 6860 products support both traditional routing and SPB design architectures, either natively or in parallel. Why choose one protocol over another? Although, both OSPF and SPB accomplish similar goals, SPB has added benefits such as simplicity, resiliency, and security.

OSPF design is a protocol that many customer IT personnel understand and can manage, so there is low O&M overhead cost, minimal training required, and all vendors support it. The disadvantage is that area summarization and complex access control lists (ACLs) need to be applied to segment data for multi-tenant requirements. Multi-tenant environments examples could be different departments (student, staff), compliancy (PCI), or cloud (multiple customers on shared infrastructure). OSPF is a sub-second
failover protocol on smaller networks, but is multi-second in typically sized networks. In today’s demanding voice and video environments, sub-second convergence is becoming a requirement. Layer 2 extensions over routed interfaces are needed for applications if layer 2 transport is required for use cases such as VMware vSphere® vMotion technology, which is a sprawled legacy VLAN due to applications that cannot route, or just due to legacy design requirements. The layer 2 extensions are typically done using VLAN tagging or QinQ tagging on top of the routing interfaces.

The downside is that redundancy in the architecture has to rely on the spanning tree protocol (STP), and layer 2 extensions still require STP to provide redundancy, which is not recommended on a WAN/MAN network. In an OSPF design, each switch is a layer 3 router with equal cost multi-path (ECMP) routes to each destination. Segmentation of those routes needs to be done with ACLs or firewalls as shown in the following figure:

Figure 2: Example segmentation with OSPF

SPB is a new o learn, but it is based on Ethernet provider backbone bridging (PBB) in its data plane, and IP intermediate system to intermediate system (IS-IS) for its control plane. Both of these technologies make up a single protocol (IEEE 802.1aq) and therefore the learning curve is minimal. Additionally, Alcatel-Lucent Enterprise Intelligent-Fabric technology makes the interconnection of new switches plug-and-play in the same way that STP is plug-and-play today.

The benefits of SPB include the following:

- You can use SPB for layer 3 and layer 2 multi-path transport without the use of STP
- Standards-based IEEE 802.1aq – no lock-in (proprietary) technology, fully interoperable and ratified in IETF and IEEE
- Resiliency - sub-second failover
- Optimal network bandwidth utilization
- Simple to deploy and manage
- Plug-and-play using Alcatel-Lucent Enterprise’s standards-based Intelligent-Fabric
- Scalability – SPB scales to millions of “services”
- Evolved from carrier – MPLS-like functionality (VPLS service-oriented approach) without the cost and complexity
• Secure separation – multi-tenancy, compliancy, and so on
• No constraints on network topology – make use of the fiber plant (mesh, ring, hub and spoke)
• Interoperable with carrier offerings (MPLS, OAM)
• Removes the limitations and concerns of “stretching” layer 2 services through the core or WAN

SPB is essentially the combination of two very mature and well understood protocols. SPB was derived from IS-IS for its control plane functionality and PBB (MAC in MAC encapsulation) for its dataplane functions. Instance service identifiers (ISIDs) or services are exchanged between SPB nodes to build a better “bridged” network. The term “bridged” is used loosely because the flexibility of SPB is that the protocol is running a layer 3 routing protocol (IS-IS) to exchange adjacency awareness and all sites have visibility to all other sites. Within that, the concept of services bundled within ISIDs can be extended across this fabric to provide layer 2 or layer 3 connectivity in a point-to-point or multi-point design. If you wish to perform IP routing at each location, use a virtual route forwarder (VRF) and put the local routes into SPB. Do not run OSPF unless you want to run it on top of SPB to interoperate with legacy routers from other vendors. If you need a layer 2 extension from one site to another, simply provision a switch port in DC1 and a switch port in DC2 in the same ISID. There is no need to configure the switches in the middle. For example, if you need to connect a VMware server in DC1 and allow that same VLAN in DC2, the two ports at each end can be provisioned (automatically or manually) and there is no need to configure VLANs on the core or any intermediate switches. SPB performs that function using MAC-in-MAC encapsulation (PBB).

Figure 3: Example segmentation with SPB

Whether you choose traditional routing or SPB, the OmniSwitch product selection remain the same. A mix of both technologies can run in parallel if required to assist with migrations. As with any new technology, it is important to understand the benefits that
can be expected from its use. It is critical to weigh these benefits against the cost in order to arrive at a realistic value proposition. Understanding the value also sets the proper expectations upfront, and is a key factor in how and where the technology is deployed. Several benefits are described here as proof points for the use of Shortest Path Bridging which, along with best practice design recommendations, provides you with the data you need to design a next-generation Intelligent Fabric with Alcatel-Lucent Enterprise.

**NETWORK ARCHITECTURE OVERVIEW**

Metro and wide-area networks can be plumbed together using hub and spoke, rings, or mesh architectures. There is no limitation or requirement if using SPB. SPB can accommodate any type of design no matter what kind of physical fiber plant or carrier layout you have. In a typical environment, there are usually two data centers and more than one branch, campus, or remote facility that requires connectivity to those DCs. Regardless of how many layers of switching there are, there is at least a core/distribution and access layer for a two-tiered design. Larger networks may require a separate core and distribution or a three-tiered design. For the purposes of this paper we explain a three-tiered design, but two layer designs are quite common and their configurations can be deduced based on the following information.

*Figure 4: Sample three-tiered design*
In an SPB design, the core typically does not route. Its purpose is to switch MAC-in-MAC frames between distribution nodes. This core node is called a backbone core bridge (BCB). There can be one or many BCBs but the customer CVLAN MAC addresses are never learned in the layer 2 forwarding database (FDB) of a BCB. The BCB switches frames based on the outer MAC header. The concept of a backbone VLAN (BVLAN) is used. In an SPB network the OmniSwitch is a layer 2 fabric for the BVLAN networks and the FDB maps each node’s BVLAN reachability information to a backbone MAC (BMAC). The BVLAN ID to BMAC mapping is the VLAN the BCB uses to make its forwarding decisions. Alcatel-Lucent OmniSwitches support up to 16 BVLANs. Each BVLAN is mapped to an equal cost tree (ECT). ECTs are the calculated shortest path from source to destination nodes. A BCB does not have to be SPB aware; any modern switch that supports jumbo frames and MAC-in-MAC encapsulation can function as a BCB.

Distribution

In a larger network, more port density at a point of presence (POP) can be needed if the physical plant cannot accommodate a centralized two-tier design. Distribution nodes can be a BCB, a backbone edge bridge (BEB), or both. From the point of view of the ISID flow, any node can be a core or edge bridge. For example, if an ISID service was terminated on a distribution node for the purposes of routing (most common), there is a physical cable extension from an SPB port where the ISID terminates to the VRF port where the router interfaces exists. These router interfaces can be imported/exported into the SPB control plane or global routing table (GRT) for reachability information. This method is called L3VPN. VPN Lite is when routing protocols can ride on top of SPB (similar to the way OSPF rides on top of a broadcast medium like a VLAN). L3VPN is what you get when you import/export router interfaces in the GRT and VPN Lite is what you get when router interfaces ride on top of SPB. These two methods, L3VPN and VPN Lite are both supported in OmniSwitch product lines.
Access
Access switches or BEBs are where the ISIDs terminate. The port on which an ISID terminates is called a service access port (SAP). Access switches can also be routers and use the same routing VPN services as described in the previous Distribution paragraph, but access switches that are layer 2 in design are more common. The OmniSwitch 6860 is the only SPB-capable access switch and is also layer 3-capable (OSPF, BGP, ISIS). OmniSwitch 6450 is a layer 2 access switch but is not SPB-capable, so the ISID needs to terminate on the nearest SPB neighbor switch upstream of the 6450s. Access switches are where the customer VLAN (CVLAN) traffic enters the network. This is where VLANs map into the SPB fabric.

Service design
Depending on the goals of the network, service mapping or VLAN to ISID design is done in one of two ways; manually or dynamically. To create a manual SAP choose the CVLAN(s), associated port(s), and map that to an ISID, which is mapped to a BVLAN/ECT. If the same ISID is created on one or more switches, that CVLAN traffic is tunneled through SPB and those customer nodes are connected to each other as if they were on the same LAN. Dynamic ISID creation can be done using policy-based decisions when gaining access (VLAN ID, IP, MAC) and have those decisions mapped to a particular ISID/BVLAN/ECT combination. For a MAN/WAN environment, routed interfaces use the physical cable extension at the access router to extend IP interface reachability information from a remote site to the DC.

Redundancy
Redundancy is done using SPB, by having more than one link in between two or more adjacent nodes (for example, triangle) or using link aggregation (LINKAGG) between two adjacent nodes. Using LINKAGG instead of separate links in between two adjacent nodes means that SPB calculates the shortest path that can be manipulated based on path costs. Node-to-node convergence times are sub-second when failing from one path to an alternate path.

SPB BCB DESIGN
In this sample design, we assume one DC, four distribution POPs, and four remote sites similar to those shown in Figure 4. Traffic flow is typically from remote to DC, but remote to remote traffic is allowed. Most traffic is routed, but some applications require layer 2 connections. Unicast and multicast traffic is used in the MAN.

Base config
```bash
! spb bvlan 4000-4015 admin-state enable
mac-learning vlan 4000-4015 disable
!
! ***a good best practice unless running ‘ships in the night’ is to
disable native vlan on nni links
!
vlan 999 admin-state disable
vlan 999 name “BIT-BUCKET”
vlan 999 members port 1/1 untagged
vlan 999 members linkagg 1 untagged
```
SPB supports two methods for replicating and forwarding broadcast, unknown unicast, and multicast traffic: head-end replication and tandem replication. In head-end replication, the accessing head-end switch makes a copy of each packet for each BEB where the ISID exists. In tandem replication mode, a multicast distribution tree is used and the functionality is similar to protocol independent multicast (PIM) trees where a fork in the tree sends a copy of the packet to each ISID. Whichever mode is used on a BVLAN, all nodes must have the same base config or unexpected behavior can result. The tandem or head-end selection is done in the next section (service manager). If tandem mode is used the base configuration, BVLAN has a choice to change the multicast mode:

```
!  spb isis bvlan bvlan_id tandem-multicast-mode {sgmode | gmode}
```
**SPB Service config**

If the core is a pure BCB, there is no SAP configuration other than management if required.

**IP config**

If the core is a pure BCB, there is no IP configuration other than management. Management of an SPB node can be done in one of three ways.

1. Out of band (OOB): Pure out-of-band using EMP ports (not available on some models)
2. In-band using STP approach as an overlay. This option requires a loopback cable at only one node in the fabric but requires the management VLAN to run STP.
3. In-band using SPB. This option requires a loopback cable on each node for management.

Option 3 is the recommended method. A logical IP config using L3VPN looks like this:

```plaintext
vlan 100 members port 1/1 tagged
vlan 3000 members port 1/1 tagged
ip interface "MGMT" address x.x.x.x/24 vlan 100
ip interface "L3vpn1" address y.y.y.y/24 vlan 3000
ip export all-routes
ip import isid 4001 all-routes
spb ipvpn bind vrf default isid 4001 gateway y.y.y.y all-routes
service access port 1/2
service spb 4001 isid 4001 bvlan 4001 admin-state enable
service spb 4001 sap port 1/2:3000 admin-state enable
```

**SPB BEB DESIGN**

Any node can be a BEB. If an ISID is terminated on a SAP on any SPB node, by definition it is considered a BEB. A BEB can also be considered a BCB for any transit ISID where no termination exists.

**Base config**

Same as BCB.

**SPB service config**

A similar setup to IP config of the BCB section is needed for layer 3 services. A single ISID is mapped to all nodes with a loopback cable where the router interfaces are imported/exported into the GRT.

For layer 2 services, there are two methods to configure access ports on SPB. Manual SAPs and dynamic SAPs. Dynamic SAP creation can be done in a few different ways; all methods are described below.

The following sample configuration illustrates the SAP configuration options:

```plaintext
! Manual Method
! ***The example below shows a single ISID with 3 VLAN’s bound to BVLAN 4001
! on port 1/10
```
service access port 1/10
service spb 1000 isid 1000 bvlan 4001 multicast-mode Tandem admin-state enable
service spb 1000 sap port 1/10:10 admin-state enable
service spb 1000 sap port 1/10:20 admin-state enable
service spb 1000 sap port 1/10:30 admin-state enable

! Dynamic Method Option 1
! ***The example below is for 1 vlan per isid : dynamic isid derived from:
! 10,000,000 + (customer domain ID * 10,000) + (outer VLAN tag of the packet)
! all in same BVLAN and tandem
!
unp customer-domain 256 description "customer1"
unp port 1/11 trust-tag enable
unp port 1/11 port-type spb-access
unp port 1/11 classification enable
unp port 1/11 unp-customer-domain 256

! Dynamic Method Option 2
! ***This example is for multiple VLAN’s per ISID or 1:1 but unclassified traffic
! is NOT dropped
! you can create a default spb-profile otherwise it goes into ISID 10000000 BVLAN 4000
!
unp spb-profile customer1 tag-value 100 isid 1001 bvlan 4001
unp spb-profile customer2 tag-value 200 isid 2001 bvlan 4002
unp spb-profile customer3 tag-value 300 isid 3001 bvlan 4003
unp classification vlan-tag 100 spb-profile customer1
unp classification vlan-tag 200 spb-profile customer2
unp classification vlan-tag 300 spb-profile customer3
unp port 1/11 port-type spb-access
unp port 1/11 trust-tag enable
unp port 1/11 classification enable

! Dynamic Method Option 3
! ***This example is config for multiple vlan per isid or 1:1 but unclassified 1 traffic IS dropped
! It sends unclassified traffic to default profile that is using an admin-down ISID (9999)
!
unp spb-profile default tag-value 0 isid 9999 bvlan 4015
unp spb-profile customer1 tag-value 100 isid 1001 bvlan 4001
unp spb-profile customer2 tag-value 200 isid 2001 bvlan 4002
unp spb-profile customer3 tag-value 300 isid 3001 bvlan 4003
unp classification vlan-tag 100 spb-profile customer1
unp classification vlan-tag 200 spb-profile customer2
unp classification vlan-tag 300 spb-profile customer3
unp port 1/11 port-type spb-access
unp port 1/11 classification enable
unp port 1/11 trust-tag enable
unp port 1/11 default-spb-profile default

! service spb 999 isid 9999 bvlan 4015 admin-state disable

The simplicity of SPB allows you to create a SAP on any two (or more) ports in the Intelligent-Fabric, as well as to create a private L2 link between those ports. Any BCB switches in the path do not need to be configured other than the base configuration to accommodate the connection.

**IP config**

The IP config is similar to section three in BCB section. Additional router interfaces can be added but only a single L3VPN ISID is required. If multicast routing is required, simply add PIM interfaces as normal to the IP interfaces. L3 SPB multicast on the OmniSwitch works the same way as standard multicast PIM. The only difference is the control plane PIM interface reachability information uses the SPB L3 type length value fields (TLV) to exchange state information, but data plane traffic traverses the ISID as normal L2 traffic.

**SPECIAL SERVICES**

**Statistics**

Node-to-node traffic can be monitored using service assurance agent (SAA). This can provide delay, jitter, and latency for WAN nodes communicating across the fabric. The output is provided in nanoseconds.

```plaintext
! saa spb auto-create auto-start
!
! SAMPLE OUTPUT:
!
-> show saa statistics

legend: eth-lb = ethoam-loopback
eth-dmm = ethoam-two-way-delay
- = Daley or jitter value not available

Aggregate Record:
<table>
<thead>
<tr>
<th>Saa Owner</th>
<th>Type</th>
<th>Time of Last-Run</th>
<th>RTT</th>
<th>RTT</th>
<th>RTT</th>
<th>RTT</th>
<th>Jitter</th>
<th>Jitter</th>
<th>Jitter</th>
<th>Jitter</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip-ping</td>
<td>2013-06-19,12:52:52.0</td>
<td>970</td>
<td>1067</td>
<td>1432</td>
<td>-</td>
<td>17</td>
<td>793</td>
<td>455</td>
<td>7</td>
<td>DEFAULT</td>
</tr>
<tr>
<td></td>
<td>ip-ping</td>
<td>2013-06-19,11:00:00.0</td>
<td>192</td>
<td>238</td>
<td>383</td>
<td>200</td>
<td>15</td>
<td>42</td>
<td>181</td>
<td>150</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>eth-dmm</td>
<td>2013-06-19,12:52:52.0</td>
<td>1563</td>
<td>2654</td>
<td>3574</td>
<td>-</td>
<td>15</td>
<td>27</td>
<td>173</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>eth-lb</td>
<td>2013-06-19,12:30:40.0</td>
<td>1245</td>
<td>1537</td>
<td>2166</td>
<td>100</td>
<td>23</td>
<td>42</td>
<td>96</td>
<td>506</td>
<td>6</td>
</tr>
</tbody>
</table>

! ***Statistics should also be enabled on SAP ports in different sections of the CLI. This allows for show commands to provide input and output statistics. Statistics are enabled by default on UNP ports.**
service spb 10 isid 1000010 bvlan 4001 admin-state enable stats enable
service spb 10 sap linkagg 39:10 admin-state enable stats enable

VLAN translation
SPB VLAN translation is processed according to the local SAP configuration (the SAP on which the frames exit) and not according to the configuration of the SAP on which the frames were received. For example, if a frame entering on a SAP port 802.1Q tagged with VID 20 is transported across an SPB fabric and the exit SAP is tagged with VID 20, there is no need for translation. But if the exit VLAN is native or needs to be changed, the SAP can be configured with VID 30 but translation commands need to be entered in different locations in the CLI:

service access linkagg 101 vlan-xlation enable
service spb 10 isid 1000010 bvlan 4001 admin-state enable stats enable
vlan-xlation enable

***UNP vlan-xlation is enabled by default on UNP ports
! but required on classification profiles
unp spb-profile TEST tag-value 1002 isid 1011002 bvlan 4002 vlan-xlation
enable

TROUBLESHOOTING AND MONITORING
A more comprehensive troubleshooting document can be found at https://support.esd.alcatel-lucent.com/pm/download/file/9822 in chapter 21. Below are a few common show and troubleshooting commands:

Common show commands

! Verify the SPB ISIS adjacency is up
show spb isis adjacency
!
! Verify all SPB nodes are reachable
show spb isis nodes
!
! Verify SPB services (ISID) are being advertised
! Local services have *
show spb isis services
!
! Verify service distribution points (SDP) between nodes are up
show service sdp spb
!
! Verify the SAP ports are up
show service spb service_id ports
!
! Verify traffic is entering and exiting the SAP
! Stats must be enabled
show service spb service_id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1 | :outer_qtag.inner_qtag]

Common troubleshooting commands (CLI and OmniVista)

CLI Option:
“How do I find the path a packet takes through my SPB network in case I need to troubleshoot an issue hop-by-hop (bad GBIC, faulty cable, port, link, ECT)?”

OmniSwitches support a layer 2 MAC-traceroute method, and have a MAC-ping command for enhanced troubleshooting.

To use MAC-ping you need to ping the base MAC (BMAC) on the control BVLAN. You can find destination BMACs by typing “show mac-learning” and/or “show system”, get the MAC address of the switch, and use it for the MAC-ping.

Here is a sample use case to trace an SPB path:

- My device (MAC AAA) is reporting slowness to server (MAC SSS)
- Log into OV – locate MAC AAA and MAC SSS
- MAC AAA lives on switch XXX
- Server lives on switch YYY
- There are several switches and multiple paths in between client and server and I am running SPB, which path did the AAA to SSS flow take?
- On switch XXX, type “show MAC-learning”
- You should see the server MAC SSS in the table with output similar to:
- Now you know the path it is taking is using ISID 4001 bound to BVLAN 4001 and its using the SDP 32786
- Now type “show service sdp” and get an output similar to:
  - 32786 00e0.b1e7.0bd3:4001 Up Up SPB
- That MAC is the BMAC of the remote switch at the other end of the SDP
- Now you know my destination node (although you could find this out from OV locater as well)
- Now type “show spb isis spf bvlan 4001 bmac 00e0.b1e7.0bd3”
  - This outputs the path hop-by-hop of the shortest path SPB chose for this flow
  SPB ISIS Path Details:
  Path Hop Name        Path Hop BMAC
  --------------------+-------------------
  XXX                 e8:e7:32:cb:cf:03
  ZZZ                 e8:e7:32:cb:cd:35
  YYY                 e8:e7:32:d5:84:55
  Now we know the path is X→Z→Y
  How do we find out what port each node is living on? For that you need to SSH into each node perform a MAC-learning lookup of each of those BMAC IPs from above to see what port they are learned on each switch
  - VLAN 4001 e8:e7:32:cb:cd:35 bmac bridging 0/21
OmniVista 2500 NMS:
OmniVista® 2500 NMS also has an SPB view in the topology application to show a visual representation of SPB trees. In the topology application, while viewing a regional map, you can display SPB links by clicking on the SPB Links icon at the bottom of the screen. All SPB Links in the network are displayed. To view information about a specific link, place the cursor on the connection you wish to view.

Figure 6: SPB Link Information

CONCLUSION

SPB can be a very powerful protocol to use for network designers. Its origins in the data center have expanded into the WAN and even the campus and can provide flexibility and options that are not available or easy to implement with traditional protocols. This document provides some context for using SPB in the WAN and Metro and some examples of how to configure and troubleshoot it. More details can be found on our website as well as in network configuration and CLI guides.

MORE INFORMATION

http://enterprise.alcatel-lucent.com/
http://enterprise.alcatel-lucent.com/docs/?id=23999
http://enterprise.alcatel-lucent.com/docs/?id=22516