# Table of Contents

Preface ............................................................................................................................................... 1  
Introduction ........................................................................................................................................ 1  
Campus LAN Design .......................................................................................................................... 2  
  Traditional vs Avaya Fabric Connect Campus LAN Design ............................................................... 3  
  Traditional Campus LAN Design ....................................................................................................... 3  
  Campus LAN Design with Avaya Fabric Connect ............................................................................. 4  
Core Layer Design Details .................................................................................................................... 6  
  Core Layer Components .................................................................................................................... 6  
  Packet Forwarding ............................................................................................................................ 6  
  Core-to-Aggregation Layer Connectivity ......................................................................................... 7  
Aggregation Layer Design Details ........................................................................................................ 7  
  Aggregation Layer Components ...................................................................................................... 7  
  IP Unicast Routing ........................................................................................................................... 9  
  IP Multicast Routing ...................................................................................................................... 9  
  Aggregation-to-Access-Layer Connectivity ...................................................................................... 10  
Access Layer Design Details .............................................................................................................. 12  
  Access Layer Components .............................................................................................................. 12  
  Services ...................................................................................................................................... 12  
  Security/Resiliency Features .......................................................................................................... 13  
  Deploying Core Layer Avaya VSP 8000 Series Switch Pair .......................................................... 14  
Campus LAN Core Layer Deployment .............................................................................................. 14  
  Deploying Aggregation Layer Switch Pair ....................................................................................... 20  
Campus LAN Aggregation Layer Deployment .................................................................................. 20  
Campus Access Layer Deployment ...................................................................................................... 33  
  Deploying Access Layer ERS Switch .............................................................................................. 33  
Validated Hardware and Software ...................................................................................................... 40  
New in this version ............................................................................................................................ 41  
Glossary ........................................................................................................................................... 42
Preface

Document Conventions

Tips

Notes contain additional information.

Cautions contain important information about preventing data loss or equipment damage.

Text

Bold text indicates either a value to be entered or a user interface element.

This design uses 4051 and 4052 for the backbone VLANs

Blue text in a procedure indicates a configuration variable that you need to substitute with a value appropriate for your network. That value will differ from the value shown in the procedure.

\texttt{b0ad.aa42.b884}

or

Right-click \texttt{example.org}, and click \texttt{New Host}.

Highlighted text indicates emphasis.

Port1/32 1 \texttt{UP} 7d 06:26:22 127 22 d4ea.0ece.3465

Configuration Variables

For command-line input (CLI), you need to substitute example configuration values (such as IP addresses and MAC addresses) with values appropriate for your network.

Depending on the number of devices you are configuring, you will perform some procedures multiple times. Those procedures begin with a “Configuration variables” table. In the below example, you would first perform the procedure on box 8201, substituting values appropriate for your network. Then you would repeat the procedure on box 8202, substituting values for the second device in your network.

\textit{Configuration variables}

<table>
<thead>
<tr>
<th>Value</th>
<th>8201</th>
<th>8202</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPBM instance</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>SPBM nick-name</td>
<td>1.82.01</td>
<td>1.82.02</td>
</tr>
<tr>
<td>Backbone VLANs</td>
<td>4051,4052</td>
<td>4051,4052</td>
</tr>
<tr>
<td>ISIS area</td>
<td>49.0010</td>
<td>49.0010</td>
</tr>
</tbody>
</table>
Diagrams

- Red lines denote a shortest path bridging (SPB) link.
- Black lines denote a non-SPB link.

You can also view a glossary of the icons used in this guide.

Feedback

Please send us your comments and suggestions.
Introduction

The Campus LAN Reference Design discusses the design and deployment of a wired local area network (LAN) in organizations occupying one or more buildings in close proximity. This guide discusses the choices available when designing a campus LAN using Avaya Fabric Connect and how to decide between them. This guide also explains how to deploy the LAN switches, enabling communication between devices connected to the network anywhere in the campus.

The information included in this guide is based on common customer requirements and provides a tested starting point for engineers to begin designing and deploying an Avaya network. This guide does not document every possible way to design and deploy a network but instead presents the tested and recommended options that will meet the majority of customer needs.
The Campus LAN enables communication between devices in one or more buildings in close proximity. It also provides communication to devices not in the campus through interconnections to the Data Center, MAN/WAN, and Internet.

Standard applications (web browsing and email), communication applications (unified communications, video conferencing) and other networking services (Wireless LANs, video surveillance, digital signage) all rely on the Campus LAN to function. All of these applications require a reliable Campus LAN; some require additional services from the Campus LAN, such as priority service through the network, power over Ethernet, and security functions that provide different groups of users and devices unique levels of network access.

Campus network design is based off of a hierarchical three layer model. Each layer has a distinct function in the design.

- **Core Layer**—Provides connectivity between aggregation layer switches
- **Aggregation Layer**—Provides connectivity between access layer switches
- **Access Layer**—Provides connectivity to the end user devices at the edge of the network, phones, PCs, as well as network devices such as access points, digital signage, and surveillance cameras

When there is more than one instance of a layer (that is, when there are two locations on a campus where an aggregation layer is required to connect access layers), each instance is called a block.

When designing a campus LAN, there are two major topologies that you can implement: three-tier and two-tier.

In the three tier architecture, access switches terminate into an aggregation layer. The aggregation layer network then terminates into the core.

In the two-tier architecture, which includes only the access and aggregation layers, the aggregation is the central point of the network. This is alternately called a collapsed core topology.

![Traditional three-tier network design](image-url)
Traditional vs Avaya Fabric Connect Campus LAN Design

Traditional Campus LAN Design

In a traditional campus network design, three-tier designs are the common recommendation. Cabling plant restrictions between layers is one reason; other common reasons include fault isolation and scalability.

The core layer provides fault isolation by separating the Layer 2 services running at each aggregation layer. The fault isolation is necessary because spanning tree propagates Layer 2 failures and configuration errors within the Layer 2 domain. The core layer separates the Layer 2 services in the aggregation layer by running Layer 3 services only.

Layer 3 services running in the traditional campus core layer include:

- The Layer 3 interior gateway protocol (IGP), such as Open Shortest Path First (OSPF).
- Multicast services, such as protocol-independent multicast (PIM).
- Virtualization services, such as multi-protocol label switching (MPLS).

Because only Layer 3 services are running in the core layer, VLANs must be contained within a single aggregation block.

**Figure 2  VLANs within an aggregation block**

If spanning tree is active on links between aggregation switches, VLANs should not span access layer wiring closets connected to the same aggregation block.

**Figure 3  VLANs within an access layer wiring closet**
In the traditional network design, all traffic between aggregation layer blocks will cross the core layer, so correctly sizing the switches and ensuring the maximum amount of resiliency is imperative. Typically, the highest capacity modular switch available is the one recommended.

To provide the maximum amount of resiliency, each Layer 3 service needs to be tuned to provide fast failure recovery. OSPF, PIM, and MSDP timers need to be adjusted.

However, when the physical layout of the network doesn’t require a three-tier network design and the core layer is needed primarily for fault isolation, a number of issues arise:

- Expensive core switches are underutilized, and they are often located right next to aggregation switches.

- Physical cabling plant has to be reworked to support the required star topology. Few campus networks have a centralized building to which all other buildings have a connection.

- If more bandwidth is needed between buildings, all of the links from aggregation to core to aggregation need to be upgraded.

**Campus LAN Design with Avaya Fabric Connect**

This design uses Avaya Fabric Connect in order to provide benefits over traditional campus LAN design. Fabric Connect, built upon shortest path bridging (SPB), was originally built as a replacement for older STPs, removing many of the shortcomings of existing protocols. Fabric Connect can support multiple paths between points in the network where legacy STP blocked redundant paths. Fabric Connect reduces the complexity of Ethernet networks while improving their ability to scale, from 4000 VLANs to 16 million Layer 2 instances. Support for mesh or partial mesh topologies allows for equal cost load-balancing across the network, and every link is active.

Fabric Connect extends the functionality of SPB to include full Layer 3 routing functionality as well as enhanced IP multicast services. With a single protocol, Fabric Connect replaces:

- STP.

- The Layer 3 interior gateway protocol (IGP), such as Open Shortest Path First (OSPF).

- Multicast services, such as Protocol-Independent Multicast (PIM).

- Layer 2 and Layer 3 virtualization services, such as MPLS.

Because it uses a link state routing protocol, Fabric Connect has several benefits over STP:

- The control plane has a global view of the network, providing loop avoidance while allowing all links to be active.

- Link-state routing recovers very quickly from failure by detecting the break and recovering around it.

- The link state protocol calculates the unicast and multicast trees simultaneously, making all traffic on the network recover quickly instead of having to wait for unicast to recover before multicast can begin to recover from a failure.

Fabric Connect allows you to use more flexible network topologies. A network design can follow the physical layout of the network or the existing fibre-optic plant. If more bandwidth is needed between buildings, you can add more or higher-speed links between those two points in the network. Ring, partial mesh, full mesh, and star topologies are all supported. No core layer switches are required, but you can use them if the physical plant and network size justify it.
With Fabric Connect, you can extend Layer 2 anywhere in the network. The aggregation layer does not have to be a Layer 2/Layer 3 boundary for network stability, as it would be in a traditional campus network. In this design, VLAN numbering is only locally significant within the aggregation block. Therefore, Layer 2 networks that connect across multiple aggregation blocks do not require the same VLAN number in each block.

Fabric Connect creates symmetrical shortest paths between all participating switches in the Fabric Connect network. Fabric Connect uses a pair of backbone VLANs to transport traffic across the network and load-balance across equal cost paths. When a Fabric Connect switch receives a frame, it encapsulates it in a mac-in-mac header and transports it across the network.

If the frame came into the switch on a VLAN connected to a Layer 2 virtual service network (L2VSN), Fabric Connect finds the switch on the network with the destination MAC address and sends the frame to that switch, where it is de-encapsulated and forwarded to the VLAN with the destination system.

If the frame enters the Fabric Connect switch on an interface connected to a routed interface, it looks up the destination address in its route table and forwards the frame to the switch connected to the destination subnet. This subnet can be in the global route table or inside a virtual routing and forwarding (VRF) instance using a Layer 3 virtual service network (L3VSN).
Core Layer Design Details

Core Layer Components

This design uses two or more Avaya Virtual Services Platform (VSP) 8400 switches in the core layer. The VSP 8404 is a flexible compact form-factor Ethernet switch that features 4 “mini-module” slots on the front face, supporting a variety of hot-swappable 8400 Series Ethernet Switch Modules (ESM). The ESMs most often used in the core include:

- **8408QQ**—8-interface 40BASE-QSFP+ Ethernet Switch Module (Note: Interfaces 7 & 8 are reserved for future use). This is our primary recommendation for organizations with 10 Gbps connections between core blocks and high bandwidth aggregation blocks together over 40Gbps.

- **8424XS**—24-interface 10BASE-SFP+ Ethernet Switch Module (also supports selected 1000BASE-SFP).

Primarily, 8408QQ modules are used in core switches in order to connect to core blocks and high bandwidth aggregation blocks together over 40Gbps.

For aggregation blocks with lower bandwidth requirements, connect them to the core with 10 Gbps connections. The 40 Gbps interfaces on the 8408QQ can be channelized, which allows the interface to operate as four separate 10 Gbps interfaces. Breakout cables allow for direct connection between QSFP+ and SFP+ interfaces as well as from QSFP+ to fiber plant connections when the remote switch is not within 5 meters. In addition, the 8424XS module provides 10Gbps connections natively without breakout cables, as well as supporting 1 Gbps connections.

Figure 6 shows a simplified view of the 40 Gbps links between core and aggregation blocks.

![Figure 6 40 Gbps link between core blocks](image)

Packet Forwarding

Because Fabric Connect switches forward packets based only on the packets outer mac-in-mac header, Fabric Connect switches support multiple services on a single configuration. IP, Layer 2 Ethernet, multicast, and segmented networks are examples of the services a Fabric Connect network supports.

Core switches run Fabric Connect only. While all network services are forwarded in the core, in this design, the network services are deployed in the aggregation layer only and the core does not need to be configured for them. Adding, deleting, and changing services does not required changes to the core configuration.
Core-to-Aggregation Layer Connectivity

All links from the core layer run Fabric Connect. This includes links between core switches as well as links between core and aggregation layers. Only one adjacency is supported between two switches running Fabric Connect, so if more bandwidth is required than a single physical link can support, an MLT must be used.

We recommend, for increased resiliency, that all aggregation switches have two equal-cost paths to the core.

Aggregation Layer Design Details

Aggregation Layer Components

This design uses a pair of Avaya Virtual Services Platform (VSP) 8000, 7200, or 4000 series switches at each aggregation layer block. The VSP 8000, 7200 and 4000 series switches run a common software image and the configuration is the same except for interface numbering.

VSP 8000 Series

The VSP 8000 Series is a family of high-performance / high density switches. There are two VSP 8000 series to choose from: a fixed form factor or modular switches.

The VSP 8284XSQ is an 84-interface Ethernet Switch, supporting eighty 10 gigabit Ethernet interfaces & four 40 gigabit Ethernet interfaces. The highlights of the VSP 8284XSQ are:

- Fixed compact form-factor platform simplifies deployment & operation
- Very high-density 10 gigabit plus 40 gigabit uplinks

The VSP 8404, a flexible compact form-factor Ethernet Switch that features 4 “mini-module” slots on the front face, supporting a variety of hot-swappable 8400 Series ESMs. The ESMs most often used in the aggregation include:

- 8418XSQ—16-interface 10GBASE-SFP+ and 2-interface 40GBASE-QSFP+ Combo Ethernet Switch Module (SFP+ also supports selected 1000BASE-SFP).
- 8424XS—24-interface 10GBASE-SFP+ Ethernet Switch Module (also supports selected 1000BASE-SFP).
- 8408QQ—8-interface 40GBASE-QSFP+ Ethernet Switch Module (Note: Interfaces 7 & 8 are reserved for future use).

VSP 7200 Series

The Avaya VSP 7200 is fixed form-factor 10 gigabit/40 gigabit switch optimal for medium-sized aggregation layers. There are two versions of the VSP 7200 in the aggregation layer; thus this design recommends the VSP 7254XSQ.

The VSP 7254XSQ has forty eight 10 gigabit Ethernet SFP+ ports and six 40 gigabit Ethernet QSFP+ ports. It supports high-availability AC or DC power (1+1), field-replaceable fan trays, and both back-to-front and front-to-back airflow.
VSP 4000 Series

The VSP 4000 delivers fully featured fabric capabilities in a low cost 1 gigabit/10 gigabit platform optimized for small aggregation layers. Although there are four versions of the VSP 4000 series, in the aggregation layer, this design recommends the VSP4450.

The VSP 4450GSX-PWR+ has thirty-six 100/1000 Mbps SFP interfaces, twelve 10/100/1000Base-T interfaces with PoE+, and two interfaces of 1/10 gigabit SFP+

Determining the Number of Aggregation Blocks Required in an MDF

When determining the platform to use in an aggregation block, it is important to consider not only the physical connectivity but also the scalability of the platform’s Layer 2 and Layer 3 entries. It is possible, especially in organizations with dense wireless environments, to reach the limits of the platforms entry scalability while only using a small number of interfaces.

Table 1  Platform Capacity

<table>
<thead>
<tr>
<th>Capability</th>
<th>VSP 4450</th>
<th>VSP 7200</th>
<th>VSP 8000 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC entries</td>
<td>16,000</td>
<td>112,000</td>
<td>112,000</td>
</tr>
<tr>
<td>ARP entries</td>
<td>6000</td>
<td>32,000</td>
<td>32,000</td>
</tr>
<tr>
<td>RSMLT Interfaces</td>
<td>252</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast Receivers</td>
<td>1000</td>
<td>6000</td>
<td>6000</td>
</tr>
<tr>
<td>Max 1 Gbps Interfaces</td>
<td>48</td>
<td>48</td>
<td>96</td>
</tr>
<tr>
<td>Max 10 Gbps Interfaces</td>
<td>2</td>
<td>72</td>
<td>96</td>
</tr>
<tr>
<td>Max 40 Gbps Interfaces</td>
<td>-</td>
<td>6</td>
<td>24</td>
</tr>
</tbody>
</table>

Design your network so that an aggregation block does not exceed 70 percent of the interface or entry capacity at full utilization. This will allow you room to grow. If one pair of switches cannot support the access layer at this utilization level, add more aggregation blocks until the recommended capacity level is reached. For example, if a large building with many dozens of floors had a physical fiber plant that terminated all wiring closets in a single location, multiple aggregation-layer blocks in that single location would be appropriate.

Figure 7  Aggregation layer block
IP Unicast Routing

IP Shortcuts

For Layer 3 routing on the network, this design uses IP Shortcuts, an Avaya extension to SPB. IP Shortcuts allow you to route IP traffic across the network by using the global routing table on the Fabric Connect enabled switches. This functions very similarly to how a traditional network would route using an IGP, but instead of having to provision subnets hop by hop on each link across a network, a Fabric Connect switch needs only a single loopback address for IP Shortcuts to work.

![Figure 8 IP Shortcuts network routing](image)

In Figure 8, all three switches are running Fabric Connect, but only switches with IP subnets that need to be routed across the network need to run IP Shortcuts. In this example, switch 1 and switch 3 have loopback addresses and VLAN interfaces with IP subnets. This is all you need in order to route IP packets between the 10.10.16.0/23 and 10.10.18.0/23 subnets. If you added a VLAN and subnet to switch 2, you need only to add a loopback and enable IP Shortcuts for the new subnet to reach the existing subnets on the network.

RSMLT Layer 2 Edge

RSMLT Layer 2 Edge provides default gateway redundancy to access layer subnets. Each switch in the aggregation block is configured with a unique IP addresses for each VLAN. Each switch in the aggregation block is configured with the peer switch information as is able to forward on behalf of itself as well as its peer. This makes very efficient use of bandwidth and resources and also ensures seamless failover and recovery in the event of a failure.

IP Multicast Routing

Traditional networks that support multicast rely on PIM with a central rendezvous point (RP). Multicast traffic starts on a shared tree and routing is often sub-optimal. In Figure 9, the multicast stream from the sender goes to the RP and then down the shared tree to the receiver, taking three hops across the network instead of just one. After the receiver gets the flow over the shared tree, the network should learn the shortest path and route the flow in a more optimal way, but the solution is complicated and can be difficult to troubleshoot.
At the aggregation layer, this design uses Avaya Fabric Connect’s SPB multicast feature to provide multicast services to and from the rest of the network. SPB multicast doesn’t rely on a central router, there is no RP, and the network doesn’t run PIM. When a Fabric Connect enabled switch receives a multicast stream from a sender, it announces the stream to all other Fabric Connect–enabled switches and builds a special SPB multicast service identifier. When a receiver requests the stream, the traffic is sent via the shortest path in the network over the multicast service identifier that was created, as shown below.

There is no central router to become a choke point. The load from the multicast is distributed across more switches and allows the design to scale easily to thousands of multicast flows. When multiple receivers want to receive the same stream, the network replicates the traffic along the shortest path tree as needed. When multiple senders are present, multicast traffic on the network is load-balanced so that traffic is spread evenly and no one switch or path is overburdened, as shown below.

**Aggregation-to-Access-Layer Connectivity**

Aggregation to access layer connectivity is achieved through 802.1q trunks running between the access and aggregation layers. In this design, the switches in the aggregation layer run split multi-link trunking (SMLT) across virtual interswitch trunks (vIST) in order to support the access layer connections, resiliently, on both switches in the aggregation block.
Split Multi-link Trunking

SMLT allows a multi-link trunk for the access layer switch to be connected across a pair of aggregation switches. To the access switch, the SMLT pair looks like a single switch. This improves availability, allowing network operation to continue in the event of link or switch failures.

Virtual Interswitch Trunking

For SMLT to operate, the two switches across which the trunk is split run vIST. vIST allows the two switches to share addressing, state, and forwarding information. In the event of a failure, the IST pair can detect and recover from the failure rapidly.

vIST does not require a direct physical connection for the IST link. vIST can operate over any SPB path between the switches, meaning an aggregation pair of switches could be in separate buildings on a campus. However, this design recommends that two links, configured as a multi-link trunk, connect the switch pair in the aggregation layer when they are in close proximity. The two 10 GB interfaces in the VSP 8000 series, or 1 GB interfaces in the VSP 4000 series platforms, will provide a resilient and efficient path to transmit information during normal operation.
Access Layer Design Details

Since the access layer is the edge of the network, it has two key roles it must fill. The first role is to provide services to the clients and the second role is to protect the network from attacks and failures that would affect network availability.

Access Layer Components

This design uses the Avaya ERS 5900 or 4850 series switches at each access layer block.

Avaya ERS 5900 is a premium stackable chassis system providing high-performance, convergence-ready, resilient, and more secure Ethernet-switching connectivity. Available in four model variants supporting 10/100/1000 switching and routing, 4 x SFP+ uplinks, and Power-over-Ethernet+, the ERS 5900 is ideally suited for high-end wiring closet and network edge deployments.

Avaya ERS 4850 is a stackable, high-performance Ethernet access-layer switch. The ERS 4850 switch provides 48 10/100/1000BASE-T interfaces, including 2 shared SFP Uplink interfaces, plus 2 additional SFP+ Uplink interfaces. The SFP+ interfaces deliver flexibility in terms of uplink speeds—allowing you to install either 1 gigabit or 10 gigabit SFP+ switches. Two models of ERS 4850 are available; one supports PoE+, and the other does not.

To support wiring closets with more than 48 connected devices, the ERS 5900 and 4850 switches include a resilient stacking architecture. You create a stack of ERS switches by connecting the switches with stacking cables such that every switch has two stacking connections. The maximum number of switches in a stack is 8. A failure in a member of the stack does not adversely affect the operation of the remaining switches in the stack.

Services

Network services provided from the access layer allow clients to easily use unified communications applications, including voice and video. These services also allow an organization to easily include new client facing technologies into their network including 802.11ac wireless.

PoE+

Power over Ethernet (PoE) is a required service in the access layer, because many of the devices that connect to it—such as IP telephones, wireless access points, video surveillance cameras, and digital signage—will require the service in order to operate.

The ability to centrally power these devices from the access layer not only makes the physical installation simpler, but it also provides a central point to provide power resiliency to all of the devices through a UPS.

The access layer switches shown in this guide support the IEEE 802.3at standard, also known as PoE+. PoE+ supports an increased power draw over previous standards, up to 30 watts, which allows for a more diverse set of devices that are able to utilize the service, as well as for the advancement of technologies including 802.11ac.

QoS

Real time voice and video and business-critical traffic require differentiated service from the network. Network issues such as delay, loss, and jitter affect them more than standard data traffic, and their importance to an organization may be higher than standard data traffic.
Auto Detection Auto Configuration (ADAC) support in the access layer is enabled, allowing automatic discovery of an IP phone when it is connected and honoring the QoS marking that the phone sends.

**Security/Resiliency Features**

The access layer contributes to the overall security and resiliency of the network through a number of features designed to protect against human error and also attack.

**BPDU Filtering**

To help prevent a network loop from forming when two switches are incorrectly cabled together, bridge protocol data unit (BPDU) filtering is enabled on all client-facing interfaces. Spanning tree BPDUs should never be seen on a client-facing interface, and when they are, the switch will shut the interface down to protect the network.

**DHCP Snooping**

Dynamic Host Control Protocol (DHCP) Snooping ensures only trusted DHCP servers are allowed to respond to a client DHCP request. This provides security to the network by preventing DHCP spoofing as well as resiliency from misconfigured clients.

DHCP Snooping is configured so that DHCP requests are only forwarded through the trusted uplinks to the aggregation layer. Any DHCP replies from untrusted client-facing interfaces are automatically dropped. A binding table is also created with the source MAC, IP address, VLAN, interface, and lease time, which is useful for troubleshooting as well as serving as a foundation for other security features.

**Dynamic ARP Inspection**

Dynamic address resolution protocol (ARP) inspection validates ARP packets in the network. Without dynamic ARP inspection, a malicious user can attach hosts, switches, and routers connected to the Layer 2 network by poisoning ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Dynamic ARP inspection prevents this type of attack. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.

When DHCP Snooping is enabled, the address binding table is dynamically built from information gathered in the DHCP request and reply. The MAC address from the DHCP request is paired with the IP address from the DHCP reply in order to create an entry in the DHCP binding table.

**IP Source Guard**

IP Source Guard provides security to the network by filtering clients with invalid IP addresses. IP Source Guard relies on information in the DHCP Snooping binding table in order to maintain IP filter entry on the client-facing interfaces. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the interface in order to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IP Source Guard–enabled interface. When this number is reached, no more filters are set up and traffic is dropped.
Campus LAN Core Layer Deployment

Procedures

Deploying Core Layer Avaya VSP 8000 Series Switch Pair

1.1 Configure Switch Identity
1.2 Configure SPB on the Avaya VSP 8000 Series Switches
1.3 Configure IP Shortcuts on the Avaya VSP 8000 Series Switches
1.4 Configure Connections to Core and Aggregation Switches

1.1 Configure Switch Identity

Table 2 Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>core-8000-1</th>
<th>core-8000-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator username</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td>avaya123</td>
<td></td>
</tr>
<tr>
<td>System name</td>
<td>core-8000-1</td>
<td>core-8000-1</td>
</tr>
<tr>
<td>NTP server</td>
<td>10.10.130.123</td>
<td></td>
</tr>
</tbody>
</table>

Complete this procedure on all Avaya VSP 8000 series core switches.

The default username and password for the full access account ("read write all") are user rwa and password rwa. Only one account local to the switch has “read write all” permissions. You are going to change the username to admin and set a new password. Follow your organization’s security policy for configuring user accounts and passwords.

Step 1: Change the username and password.

```bash
enable
cfg t
username admin level rwa
Enter the old password : ********
Enter the New password : ********
Re-enter the New password : ********
```

Step 2: Set the system name. The system name is used for the prompt, simple network management protocol (SNMP) system name, and SPB host name.

```bash
sys name core-8000-1
```
Step 3: Enable connectivity fault management (CFM). This allows Layer 2 ping and traceroute across the network. Because SPB operates at Layer 2, this allows you to troubleshoot connectivity issues.

   cfm spbm enable

Step 4: Enable and configure SSH. This enables secure CLI access and file-copy to the switch.

   boot config flags sshd
   ssh

You can now access the switch via SSH to the management interface with the username and password you configured previously. You can copy files to and from the switch with secure copy (SCP). If you cannot use SSH, there are a number of other unencrypted access methods available, including FTP, telnet, and tftp. Configure them using the `boot config flags` command.

Step 5: Enable NTP.

   ntp server 10.10.130.123 enable
   ntp

Step 6: Enable web access.

You can configure the VSP 8000 series switch by web browser with Enterprise Device Manager (EDM), which is not covered in this guide. To enable secure HTTPS access to EDM, enter the following configuration. Web access uses a different set of credentials than the CLI username and password that you configured previously.

   web-server enable
   web-server password rwa admin avaya123

Step 7: Save the configuration.

   write memory

---

**Note** To adjust the time before the CLI times-out the connection and you have to re-login, you can use the command `CLI timeout [30-65535]`. 65,535 seconds is about 18 hours.
### 1.2 Configure SPB on the Avaya VSP 8000 Series Switches

#### Table 3  Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>core-8000-1</th>
<th>core-8000-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPBM instance</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>SPBM nick-name</td>
<td>1.15.01</td>
<td>1.15.02</td>
</tr>
<tr>
<td>Backbone VLANs</td>
<td>4051,4052</td>
<td></td>
</tr>
<tr>
<td>ISIS area</td>
<td>49.0010</td>
<td></td>
</tr>
</tbody>
</table>

**Step 1:** Enable SPBM globally on the switch.

```
spbm
```

**Step 2:** Enter the SPB instance, backbone VLANs, nick-name, and area. The nick-name must be unique for the network. Use a nick-name that maps to something easily recognizable, in this case the system name. This design uses **4051** and **4052** for the backbone VLANs and **49.0010** for the ISIS area.

```
router isis

spbm 10
spbm 10 nick-name 1.15.01
spbm 10 b-vid 4051-4052 primary 4051
manual-area 49.0010
exit
```

**Note**  Some settings in SPB can’t be removed without removing the SPBM instance but can be overwritten. If you are trying to change a value, and no followed by the command doesn’t allow you to remove the command, try overwriting the previous value by entering the command with the new value.

**Step 3:** Create the VLANs that you defined in the ISIS configuration that SPB will use to carry traffic across the network. Only one backbone VLAN is required, but two should be used so that SPB can load-balance traffic across the network.

```
  vlan create 4051 type spbm-bvlan
  vlan create 4052 type spbm-bvlan
```

**Step 4:** Enable ISIS on the VSP 8000 series switch.

```
  router isis enable
```
### 1.3 Configure IP Shortcuts on the Avaya VSP 8000 Series Switches

#### Table 4  Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>core-8000-1</th>
<th>core-8000-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback number</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>10.10.15.254</td>
<td>10.10.15.253</td>
</tr>
</tbody>
</table>

**Step 1:** Add a loopback interface to the switch and an IP address with a /32 subnet mask. For IP shortcuts to operate, SPB switches only need a single IP address.

```bash
interface loopback 10
ip address 10.10.15.254/32
exit
```

**Step 2:** Add the loopback address to the ISIS instance and enable IP shortcuts.

```bash
router isis
ip-source-address 10.10.15.254
spb 10 ip enable
```

**Step 3:** Redistribute connected routes to the rest of the network. Now the loopback and any other interface subnets on the switch will be advertised to the rest of the network.

```bash
redistribute direct
redistribute direct enable
exit
isis apply redistribute
```

**Step 4:** Enable equal cost multi-path (ECMP) in order to allow SPB to load-balance across equal cost paths.

```bash
ip ecmp
```

### 1.4 Configure Connections to Core and Aggregation Switches

Connections between core-layer switches and between core and aggregation layer switches use SPB. There are two options when connecting switches: a multi-link connection or a single-link connection. Multi-link connections are useful when added resiliency or bandwidth is required between switches (for example, between two core switches). Single-link connections are useful when there are physical plant limitations and when resiliency is provided not via the links between two boxes, but via a different set of switches.
Option 1: Multi Link SPB Connections

Step 1: Create multi-link trunking (MLT) with the interfaces that you want to connect to the other SPB-capable switch.

```
mlt 11 enable
mlt 11 member 1/39-1/40
mlt 11 encapsulation dot1q
```

Step 2: Apply the ISIS SPB configuration to the MLT interface.

```
interface mlt 11
isis
isis spbm 10
isis enable
exit
```

Step 3: Enable the interfaces that are part of the MLT and disable STP.

```
interface gigabitEthernet 1/39-1/40
no spanning-tree mstp force-port-state enable
no shutdown
exit
```

Option 2: Single Link SPB Connections

To connect to other switches with a single link, you place the configuration on the interface.

Step 1: Configure SPB on the interface connecting to the other SPB-capable switch.

```
interface gigabitEthernet 1/32
isis
isis spbm 10
isis enable
no spanning-tree mstp force-port-state enable
no shutdown
exit
```

Step 2: Save the configuration.

```
write memory
```
Step 3: Verify that SPB connections are up and functioning between switches.

```
show isis adjacencies
```

```
=======================================================================
ISIS Adjacencies
=======================================================================

INTERFACE | L | STATE | UPTIME | PRI | HOLDTIME | SYSID       | HOST-NAME
-----------|----|-------|--------|-----|----------|-------------|-------------
Mlt10      | 1  | UP    | 2d 03:02:04 | 127 | 1         | b0ad.aa42.9c84 | core-8000-2

1 out of 1 interfaces have formed an adjacency
```
Campus LAN Aggregation Layer Deployment

The campus aggregation is made up of a pair of Avaya VSP 8000 or 4000 series switches. They connect to the access layer with 10 Gbps Ethernet and to the campus core with 10 Gbps or 40 Gbps Ethernet. VSP 8000 series switch connects with SPB to core and other aggregation switches with a single- or a multi-link trunk. Access layer switches are dual-homed to the aggregation switches with SMLT connection for high availability. There is a pair of links between the switches to act as the primary links for the vIST configuration, although any SPB-capable path can carry vIST traffic as needed.

The following section shows how to configure the aggregation layer pair of VSP 8000 or 4000 series switches and connect to the campus access layer and campus core.

### Procedures

**Deploying Aggregation Layer Switch Pair**

2.1 Configure Switch Identity

2.2 Configure SPB on the Aggregation Switches

2.3 Configure vIST on the Aggregation Switches

2.4 Configure IP Shortcuts on the Aggregation Switches

2.5 Configure Connections to Core and Aggregation Switches

2.6 Configure In-Band Management Network for Layer 2 Network Switches

2.7 Create Client Access VLANs

2.8 Connect Access Layer Switches to Aggregation Switches

#### 2.1 Configure Switch Identity

**Table 5 Configuration variables**

<table>
<thead>
<tr>
<th>Value</th>
<th>agg1-vsp-1</th>
<th>agg1-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator username</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td>avaya123</td>
<td></td>
</tr>
<tr>
<td>System name</td>
<td>agg1-vsp-1</td>
<td>agg1-vsp-2</td>
</tr>
<tr>
<td>NTP server</td>
<td>10.10.130.123</td>
<td></td>
</tr>
</tbody>
</table>

Complete this procedure on both aggregation switches.
The default username and password for the full access account ("read write all") are user rwa and password rwa. Only one account local to the switch has "read write all" permissions. You are going to change the username to admin and set a new password. Follow your organization’s security policy for configuring user accounts and passwords.

Step 1: Change the username and password.
```
enable
config t
username admin level rwa
Enter the old password : ********
Enter the New password : ********
Re-enter the New password : ********
```

Step 2: Set the system name. The system name is used for the prompt, SNMP system name, and SPB host name.
```
sys name agg1-vsp-1
```

Step 3: Enable CFM. This allows Layer 2 ping and traceroute across the network. Because SPB operates at Layer 2, this allows you to troubleshoot connectivity issues.
```
cfm spbm enable
```

Step 4: Enable and configure SSH. This enables secure CLI access and file-copy to the switch.
```
boot config flags sshd
ssh
```
You can now access the switch via SSHv2 to the management interface with the username and password you configured previously. You can copy files to and from the switch with SCP. If you cannot use SSH, there are a number of other unencrypted access methods available, including FTP, telnet, and tftp. Configure them using the `boot config flags` command.

Step 5: Enable NTP.
```
ntp server 10.10.130.123 enable
ntp
```

Step 6: Enable web access.
You can configure the switch by web browser with EDM, which is not covered in this guide. To enable secure HTTPS access to EDM, enter the following configuration. Web access uses a different set of credentials than the CLI username and password that you configured previously.
```
web-server enable
web-server password rwa admin avaya123
Step 7: Save the configuration.

```bash
write memory
```

**Note** To adjust the time before the CLI times-out the connection and you have to re-login, you can use the command `CLI timeout [30-65535]`. 65,535 seconds is about 18 hours.

### 2.2 Configure SPB on the Aggregation Switches

**Table 6** Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>agg1-vsp-1</th>
<th>agg1-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPBM instance</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>SPBM nick-name</td>
<td>1.31.01</td>
<td>1.31.02</td>
</tr>
<tr>
<td>Backbone VLANs</td>
<td>4051,4052</td>
<td></td>
</tr>
<tr>
<td>ISIS area</td>
<td>49.0010</td>
<td></td>
</tr>
</tbody>
</table>

Step 1: Enable SPBM globally on the switch.

```bash
spbm
```

Step 2: Enter the SPB instance, backbone VLANs, nick-name, and area. The nick-name must be unique for the network. Use a nick-name that maps to something easily recognizable, in this case the system name. This design uses 4051 and 4052 for the backbone VLANs and 49.0010 for the ISIS area.

```bash
router isis
spbm 10
spbm 10 nick-name 1.31.01
spbm 10 b-vid 4051-4052 primary 4051
manual-area 49.0010
```

**Note** Some settings in SPB can’t be removed without removing the SPBM instance but can be overwritten. If you are trying to change a value, and `no` followed by the command doesn’t allow you to remove the command, try overwriting the previous value by entering the command with the new value.

Step 3: Enable SPB multicast.

```bash
spbm 10 multicast enable
exit
```
Step 4: Create the VLANs that you defined in the ISIS configuration that SPB will use to carry traffic across the network. Only one backbone VLAN is required, but two should be used so that SPB can load-balance traffic across the network.

```
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
```

Step 5: Repeat this procedure on the second switch (agg1-vsp-2).

### 2.3 Configure vIST on the Aggregation Switches

**Table 7  Configuration variables**

<table>
<thead>
<tr>
<th>Value</th>
<th>agg1-vsp-1</th>
<th>agg1-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPBM instance</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>System ID</td>
<td>b0ad.aa42.b884</td>
<td>b0ad.aa42.9c84</td>
</tr>
<tr>
<td>MLT number</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>MLT member interfaces</td>
<td>1/15,1/16</td>
<td></td>
</tr>
<tr>
<td>vIST I-SID</td>
<td>100031</td>
<td></td>
</tr>
<tr>
<td>vIST VLAN</td>
<td>4042</td>
<td></td>
</tr>
<tr>
<td>vIST IP address</td>
<td>10.10.31.1</td>
<td>10.10.31.2</td>
</tr>
</tbody>
</table>

**Figure 13  vIST Interface Detail**

Step 1: On the second switch (agg-vsp-2), record the ISIS system ID.
```
show isis system-id
```

```
ISIS System-Id

SYSTEM-ID

b0ad.aa42.9c84
```

Step 2: On the first switch (agg-vsp-1), enter the SMLT peer system-id.
```
router isis
spbm 10 smlt-peer-system-id b0ad.aa42.9c84
exit
```
Step 3: Create a multi-link trunk between the vIST pair. This is not strictly necessary because vIST runs over any SPB connection between the two boxes, but if they are near each other physically, a direct connection is recommended. No ISIS configuration is applied on the physical MLT member interfaces.

```bash
mlt 10 enable
mlt 10 member 1/15,1/16
mlt 10 encapsulation dot1q
```

Step 4: Configure ISIS SPB on the MLT interface.

```bash
interface mlt 10
isis
isis spbm 10
isis enable
exit
```

Step 5: Enable the physical interfaces that make up the MLT.

```bash
interface gigabitEthernet 1/15-1/16
no spanning-tree mstp force-port-state enable
no shutdown
```

Step 6: To carry the vIST traffic, create the VLAN and map it to the associated services identifier (I-SID) for the connection between the two peers. The I-SID must be unique to each aggregation pair, but the VLAN number can be the same across all aggregation blocks.

```bash
vlan create 4042 name vIST type port-mstprstp 1
vlan i-sid 4042 100031
```

Step 7: Add an IP address to the VIST VLAN interface.

```bash
interface Vlan 4042
ip address 10.10.31.1 255.255.255.252
exit
```

Step 8: Specify the IP address configured on the vIST peer.

```bash
virtual-ist peer-ip 10.10.31.2 vlan 4042
```

Step 9: Enable ISIS on the aggregation switch.

```bash
router isis enable
```

Step 10: Repeat Step 1 through Step 9 on the second aggregation switch.
Step 11: Validate that the vIST configuration is working.

```
show virtual-ist
```

<table>
<thead>
<tr>
<th>PEER-IP ADDRESS</th>
<th>VLAN ID</th>
<th>ENABLE IST</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.31.2</td>
<td>4042</td>
<td>true</td>
<td>up</td>
</tr>
</tbody>
</table>

NEGOTIATED

<table>
<thead>
<tr>
<th>DIALECT</th>
<th>IST STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4.0</td>
<td>Up</td>
</tr>
</tbody>
</table>

2.4 Configure IP Shortcuts on the Aggregation Switches

**Table 8 Configuration variables**

<table>
<thead>
<tr>
<th>Value</th>
<th>agg-vsp-1</th>
<th>agg-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback number</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>10.10.31.254</td>
<td>10.10.31.253</td>
</tr>
</tbody>
</table>

Add a loopback interface to the switch and an IP address with a /32 subnet mask. For IP shortcuts to operate, SPB switches only need a single IP address.

```
interface loopback 10
ip address 10.10.31.254 255.255.255.255
exit
```

**Step 1:** Add the loopback address to the ISIS instance and enable IP shortcuts.

```
router isis
ip-source-address 10.10.31.254
spbm 10 ip enable
```

**Step 2:** Redistribute connected routes to the rest of the network. Now the loopback and any other interface subnets on the switch will be advertised to the rest of the network.

```
redistribute direct
redistribute direct enable
exit
isis apply redistribute
```
Step 3: Enable ECMP in order to allow SPB to load-balance across equal cost paths.

   ip ecmp

Step 4: Repeat this procedure on the second switch (agg1-vsp-2).

2.5 Configure Connections to Core and Aggregation Switches

Connections between core layer switches and between core and aggregation layer switches use SPB. There are two options when connecting switches: a multi-link connection or a single link connection. Multi-link connections are useful when added resiliency or bandwidth is required between switches (for example, between two core switches). Single-link connections are useful when there are physical plant limitations and when resiliency is provided not via the links between two boxes, but via a different set of switches.

Note Do not adjust the default ISIS metric on an interface unless you have interfaces of different speeds connecting between aggregation blocks.

For example, if one aggregation block uses 10 gigabit and another 40 gigabit, connecting to the core adjustment is not necessary. If one aggregation block uses a mixture of 10 gigabit and 40 gigabit to connect to the core, then adjusting the metric down for the higher speed links would be necessary.

Option 1: Multi Link SPB Connections

Step 1: Create an MLT with the interfaces that you want to connect to the other SPB-capable switch.

   mlt 11 enable
   mlt 11 member 1/13-1/14
   mlt 11 encapsulation dot1q

Step 2: Apply the ISIS SPB configuration to the MLT interface.

   interface mlt 11
   isis
   isis spbm 10
   isis enable
   exit

Step 3: Enable the interfaces that are part of the MTL and disable STP.

   interface gigabitEthernet 1/13-1/14
   no spanning-tree mstp force-port-state enable
   no shutdown
   exit
Option 2: Single Link SPB Connections

To connect to other switches with a single link, you place the configuration on the interface.

Step 1: Configure SPB on the interface connecting to the other SPB-capable switch.

```plaintext
interface gigabitEthernet 1/17
isis
isis spbm 10
isis enable
no spanning-tree mstp force-port-state enable
no shutdown
exit
```

Step 2: Verify that SPB connections are up and functioning between switches.

```plaintext
show isis adjacencies
```

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>STATE</th>
<th>UPTIME</th>
<th>PRI</th>
<th>HOLDTIME</th>
<th>SYSID</th>
<th>HOST-NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mlt10</td>
<td>UP</td>
<td>03:02:04</td>
<td>127</td>
<td>22</td>
<td>b0ad.aa42.9c84</td>
<td>agg1-vsp-2</td>
</tr>
<tr>
<td>Port2/41</td>
<td>UP</td>
<td>00:03:51</td>
<td>127</td>
<td>25</td>
<td>646a.529d.f884</td>
<td>core-8404-1</td>
</tr>
<tr>
<td>Port2/42</td>
<td>UP</td>
<td>00:03:51</td>
<td>127</td>
<td>23</td>
<td>646a.529e.0c84</td>
<td>core-8404-2</td>
</tr>
</tbody>
</table>

1 out of 1 interfaces have formed an adjacency

2.6 Configure In-Band Management Network for Layer 2 Network Switches

Although you use the switch loopback address for management of the aggregation switches, to manage access layer switches, create a VLAN and add interfaces at the aggregation layer for a dedicated management network. All access layer switches that need to communicate via in-band management will use these addresses as their default gateway and use an address out of this subnet for their management address.

Table 9 Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>agg1-vsp-1</th>
<th>agg2-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Management VLAN name</td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>Management VLAN IP</td>
<td>10.10.30.1</td>
<td>10.10.30.2</td>
</tr>
</tbody>
</table>
Step 1: Create the management VLAN.

```
vlan create 30 name Management type port-mstprstp 1
vlan i-sid 30 100030
```

Step 2: Put an address on the VLAN interface and enable RSMLT for default gateway redundancy.

```
interface Vlan 30
ip address 10.10.30.1 255.255.255.0
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

Step 3: Configure the peer aggregation switch VLAN.

```
vlan create 30 name Management type port-mstprstp 1
vlan i-sid 30 100030
interface Vlan 30
ip address 10.10.30.2 255.255.255.0
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

### 2.7 Create Client Access VLANs

To add VLANs to the aggregation layer for client access to the network, create a VLAN, put an address on the VLAN interface, and turn on RSMLT for gateway redundancy.

<table>
<thead>
<tr>
<th>Table 10</th>
<th>Configuration variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>agg1-vsp-1</td>
</tr>
<tr>
<td>Data VLAN</td>
<td>16</td>
</tr>
<tr>
<td>Data VLAN name</td>
<td>Data</td>
</tr>
<tr>
<td>Data VLAN IP address</td>
<td>10.10.16.1/23</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>18</td>
</tr>
<tr>
<td>Voice VLAN name</td>
<td>Voice</td>
</tr>
<tr>
<td>Voice VLAN IP address</td>
<td>10.10.18.1/23</td>
</tr>
<tr>
<td>DHCP server</td>
<td>10.10.129.100</td>
</tr>
</tbody>
</table>

Step 1: On the first switch, enable RSMLT Edge.

```
ip rsmlt edge-support
```
Step 2: Next, create a client VLAN.

```
vlan create 16 name Data type port-mstprstp 1
vlan i-sid 16 100016
```

Step 3: Add an IP address to the VLAN interface and enable RSMLT for gateway redundancy.

```
interface Vlan 16
ip address 10.10.16.1 255.255.254.0
ip spb-multicast enable
ip rsmlt
ip rsmlt holdup-timer 9999
ip dhcp-relay
ip dhcp-relay fwd-path 10.10.129.100 enable
exit
```

Step 4: Configure the peer aggregation switch.

```
ip rsmlt edge-support
vlan create 16 name Data type port-mstprstp 1
vlan i-sid 16 100016
interface Vlan 16
ip address 10.10.16.2 255.255.254.0
ip spb-multicast enable
ip rsmlt
ip rsmlt holdup-timer 9999
ip dhcp-relay
ip dhcp-relay fwd-path 10.10.129.100 enable
exit
```

Step 5: Repeat this procedure for the voice and any other client VLANs.
Step 6: Enter the following command in order to verify that RSMLT is operational.

```
show ip rmslt
```

```
Ip Rsmlt Local Info - GlobalRouter

VID   IP              MAC                ADMIN   OPER  HDTMR  HUTMR
------------------------------------------------------------------------
16   10.10.16.1     b0:ad:aa:42:b9:02  Enable  Up   60   infinity

VID   SMLT ID
------------------------------------------------------------------------
16

Ip Rsmlt Peer Info - GlobalRouter

VID   IP              MAC                ADMIN   OPER  HDTMR  HUTMR
------------------------------------------------------------------------
16   10.10.16.2     b0:ad:aa:42:9d:02  Enable  Up    60     9999

VID   HDT REMAIN  HUT REMAIN  SMLT ID
------------------------------------------------------------------------
16   60          infinity

2.8 Connect Access Layer Switches to Aggregation Switches

Use SMLT from the aggregation switches to connect access layer switches. For SMLT to work, ViST must have already been configured and the MLT IDs must match between the aggregation switches.

Table 11 Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>agg1-vsp-1</th>
<th>agg1-vsp-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLT identifier</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>16,18,30</td>
<td></td>
</tr>
</tbody>
</table>
Step 1: On the first switch (agg1-vsp-1), enable VLACP globally.

   vlacp enable

Step 2: Create an MLT and add the interface connecting to the access layer switch.

   mlt 110
   mlt 110 member 1/2

Step 3: On the MLT interface, enable SMLT.

   interface mlt 110
   smlt

Step 4: Enable the physical interface and configure VLACP.

   interface gigabitethernet 1/2
   no spanning-tree mstp force-port-state enable
   vlacp fast-periodic-time 500
   vlacp timeout short timeout-scale 5 funcmac-addr 180.c200.f
   vlacp enable
   no shutdown
   exit

Step 5: Add a VLAN to the MLT link.

   vlan mlt 16 110

Step 6: If you want to add multiple VLANs to the MLT, link-enable dot1q encapsulation.

   mlt 110 encapsulation dot1q

Step 7: If you have additional VLANs to add, add them to the MLT.

   vlan mlt 18 110
   vlan mlt 30 110
Step 8: If you want to remove the default VLAN from the MLT interface so that untagged traffic is dropped, enter the following.

```
interface gigabitethernet 1/2
default-vlan-id 0
exit
```

Step 9: Save the configuration.

```
write memory
```

Step 10: Repeat this procedure on the second switch (agg1-vsp-2).
Campus Access Layer Deployment

Procedures

Deploying Access Layer ERS Switch

3.1 Configure Switch Identity
3.2 Create VLANs
3.3 Create the MLT on the Edge
3.4 Create Management IP Address for Edge
3.5 Enable STP Fast Start/BPDU Filtering at the Edge
3.6 Enable Voice and Quality of Service
3.7 Enable Security Features
3.8 Enable Multicast Features

After boot, you must press CTRL+Y to access the command line interface (CLI). If you connect to the switch after boot, you may miss the message instructing you to press CTRL+Y. If there is no response when you type at the console, pressing CTRL+Y should allow you to access the CLI.

**3.1 Configure Switch Identity**

Table 12 Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>Access1-ERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator username</td>
<td>admin</td>
</tr>
<tr>
<td>Administrator password</td>
<td>avaya123</td>
</tr>
<tr>
<td>System name</td>
<td>access1-ERS</td>
</tr>
<tr>
<td>NTP server</td>
<td>10.10.130.123</td>
</tr>
</tbody>
</table>

Step 1: Configure the username and password to use for serial, SSH, telnet, and web access.

```
username add admin role-name rw password
cli password telnet local
cli password serial local
```

**Note** By default, ERS switch has a fairly strict password policy. To disable it, enter the command `no password security`. This is used for this configuration.
Step 2: Configure the hostname.

   snmp-server name access1-ERS

Step 3: Enable NTP.

   ntp server 10.10.130.123 enable
   ntp

Step 4: If the switch stack contains only two switches, enable forced-mode stacking.

   stack forced-mode

Step 5: Disable automatic saving of the configuration.

   no autosave enable

Step 6: If you are deploying an ERS 4850, enable multi-instance spanning-tree, and reload the switch.

   spanning-tree mode mst
   exit
   write memory
   reload force minutes-to-wait 1

### 3.2 Create VLANs

The following example creates the data management VLANs. The voice VLAN is created later in the deployment.

<table>
<thead>
<tr>
<th>Value</th>
<th>Access1-ERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data VLAN</td>
<td>16</td>
</tr>
<tr>
<td>Management VLAN</td>
<td>30</td>
</tr>
<tr>
<td>Uplink Interfaces</td>
<td>1/49,3/49</td>
</tr>
</tbody>
</table>

Step 1: Create Edge VLANs.

   vlan create 16 name Data type port
   vlan create 18 name Voice type port voice-vlan
   vlan create 30 name Management type port
Step 2: Assign the VLANs.

By default, the ERS 4800 switches use the strict VLAN configuration mode. In this mode, you must first remove interface members from the default VLAN 1 prior to adding these interface members to a new VLAN.

```
        vlan members remove 1 ALL
        vlan members add 16 ALL
        vlan ports 1/49,3/49 tagging tagAll filter-untagged-frame enable
        vlan members add 30 1/49,3/49
```

3.3 Create the MLT on the Edge

When configuring the MLT group, spanning tree must be disabled on the MLT. The learning disable on the MLT command disables spanning tree for the MLT.

VLACP is used to detect end-to-end link failures on direct point-to-point interfaces. This is accomplished by each switch transmitting VLACP PDUs at a set timer interval in order for a link to maintain a “link-up” state. For all direct connected point-to-point links, use the reserved multicast MAC address of 01:80:c2:00:00:0f.

Both ends of the link must be configured for VLACP with the same parameters. The VLACP configuration for the aggregation switches was shown in 2.8, Connect Access Layer Switches to the Avaya VSP 8000 series.

**Table 14**  Configuration variables

<table>
<thead>
<tr>
<th>Value</th>
<th>Access1-ERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLT instance</td>
<td>1</td>
</tr>
<tr>
<td>Uplink Interfaces</td>
<td>1/49,3/49</td>
</tr>
</tbody>
</table>

**Step 1:** Create MLT 1.

```
        mlt 1 name AggBlock1 member 1/49,3/49 learning disable
        mlt 1 enable
```

**Step 2:** Configure the VLACP MAC and enable VLACP globally.

```
        vlacp macaddress 180.c200.f
        vlacp enable
```
Step 3: Enable VLACP on MLT.

```
interface Ethernet 1/49, 3/49
vlacp timeout short
vlacp fast-periodic-time 500
vlacp timeout-scale 5
vlacp enable
exit
```

### 3.4 Create Management IP Address for Edge

A single IP address is used to manage the entire stack of switches and also the address used as the source address for Syslog entries, SNMP, and other switch/stack management functions.

**Table 15 Configuration variables**

<table>
<thead>
<tr>
<th>Value</th>
<th>Access1-ERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN</td>
<td>30</td>
</tr>
<tr>
<td>Management IP address</td>
<td>10.10.30.10</td>
</tr>
<tr>
<td>Management default gateway</td>
<td>10.10.30.1</td>
</tr>
</tbody>
</table>

Step 1: Add IP address and assign the Management VLAN.

```
vlan mgmt 30
ip address 10.10.30.10 255.255.255.255.0
ip default-gateway 10.10.30.1
```

### 3.5 Enable STP Fast Start/BPDU Filtering at the Edge

Avaya recommends using the spanning tree protocol on all end-station connections in order to safeguard the network from hubs or other switches that could be inserted into the network at the end station. A modification to the normal learning of spanning tree is available in all Avaya edge switches. This feature is known as *Fast Start* or *Fast Learning*, and it is the recommended setting for all end-station interfaces.

The BPDU filtering feature protects the network because it will block loops created by connecting Edge closets directly together; therefore it is recommended that you enable BPDU Filtering on all end-user interfaces and to set the timeout to 0, which requires manual intervention to re-enable the interface.

Spanning Tree Fast Start and BPDU Filtering are recommended for all Edge access interfaces. These features should never be enabled on the uplinks from the Edge to the Core.
Step 1: Enable STP Fast Start and BPDU Filtering on all Access interfaces.

```bash
interface Ethernet 1/1-48, 2/1-48, 3/1-48
  spanning-tree mstp edge-port true
  spanning-tree bpdu-filtering timeout 0
  spanning-tree bpdu-filtering enable
exit
```

### 3.6 Enable Voice and Quality of Service

When deploying IP telephony, Avaya provides different options for the configuration of the Ethernet switches in order to ease the deployment and later moves, adds, and changes that occur within the normal Enterprise network. This procedure describes each of these options briefly and provides references to Solution Guides and Configuration Guides for more in-depth coverage.

The ADAC feature automatically discovers the IP phone when it’s plugged into the Ethernet edge switch. Once the phone is discovered, the Ethernet edge switch automatically provisions the appropriate Voice VLAN and QoS to the interface, as well as on the uplink to the core.

**Table 16 Configuration variables**

<table>
<thead>
<tr>
<th>Value</th>
<th>Access1-ERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN</td>
<td>18</td>
</tr>
<tr>
<td>Uplink interfaces</td>
<td>1/49, 3/49</td>
</tr>
<tr>
<td>Client interfaces</td>
<td>1/1-48, 2/1-48, 3/1-48</td>
</tr>
<tr>
<td>Call server</td>
<td>10.10.130.20</td>
</tr>
<tr>
<td>File server</td>
<td>10.10.130.10</td>
</tr>
</tbody>
</table>

**Step 1:** Remove the default 802.1AB/LLDP MED policies.

```bash
interface Ethernet all
  no lldp med-network-policies
exit
```

**Step 2:** Enable ADAC globally.

```bash
adac voice-vlan 18
adac op-mode tagged-frames
adac uplink-port 1/49
adac enable
```
Step 3: Enable ADAC at the interface level.

```
interface Ethernet 1/1-48,2/1-48,3/1-48
  adac detection lldp
  no adac detection mac
  adac tagged-frames-tagging untag-pvid-only
  adac enable
  exit
```

Step 4: Enable LLDP vendor-specific settings.

```
lldp vendor-specific avaya call-server 1 10.10.130.20
lldp vendor-specific avaya file-server 1 10.10.130.20
interface Ethernet 1/1-48,2/1-48,3/1-48
  lldp vendor-specific avaya dot1q-framing tagged
  exit
```

### 3.7 Enable Security Features

The access switches support security features that help protect the network from denial of service (DoS) attacks. You should enable DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard on all access switches in order to help ensure the protection and integrity of the Campus network.

Step 1: Enable DHCP Snooping.

```
ip dhcp-snooping enable
ip dhcp-snooping vlan 16
ip dhcp-snooping vlan 18
interface Ethernet 1/49,3/49
  ip dhcp-snooping trusted
  exit
```

Step 2: Enable Dynamic ARP Inspection.

```
ip arp-inspection vlan 16
ip arp-inspection vlan 18
interface Ethernet 1/49,3/49
  ip arp-inspection trusted
  exit
```

Step 3: Enable IP Source Guard on the on interfaces connected to clients.

```
interface Ethernet 1/1-48,2/1-48,3/1-48
  ip verify source
  exit
```
3.8 Enable Multicast Features

If there is a requirement to run multicast on the network, it is recommended that you enable IGMP Snooping and Proxy at the edge.

In this example, IGMP is enabled on the data and voice VLAN but not on the management VLAN.

Step 1: Enable Multicast.

```
vlan igmp 16 snooping enable
vlan igmp 16 proxy enable
vlan igmp 18 snooping enable
vlan igmp 18 proxy enable
```

Step 2: Save the configuration.

```
write memory
```
Validated Hardware and Software

The following hardware and software were validated during the creation of this guide.

<table>
<thead>
<tr>
<th>Component</th>
<th>Platform</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Switch</td>
<td>VSP 8404</td>
<td>4.2.1.1</td>
</tr>
<tr>
<td>Aggregation Switch</td>
<td>VSP 8404</td>
<td>4.2.1.1</td>
</tr>
<tr>
<td>Aggregation Switch</td>
<td>VSP 8284</td>
<td>4.2.1.1</td>
</tr>
<tr>
<td>Aggregation Switch</td>
<td>VSP 7200</td>
<td>4.2.1.1</td>
</tr>
<tr>
<td>Aggregation Switch</td>
<td>VSP 4450</td>
<td>4.2.1.1</td>
</tr>
<tr>
<td>Access Switch</td>
<td>ERS 5900</td>
<td>7.0.0.319</td>
</tr>
<tr>
<td>Access Switch</td>
<td>ERS 4850</td>
<td>5.9</td>
</tr>
<tr>
<td>Phone</td>
<td>9600 Series</td>
<td>—</td>
</tr>
<tr>
<td>Phone</td>
<td>1600 Series</td>
<td>—</td>
</tr>
</tbody>
</table>
New in this version

- Incorporated the Avaya VSP 7200 into the aggregation
- Incorporated the Avaya ERS 5900 into the access
- Updated the validated software on the VSP and ERS switches
- Minor improvements that make the document easier to read
Glossary

ADAC  Auto Detection Auto Configuration
ARP  address resolution protocol
Avaya ERS  Avaya Ethernet Routing Switch
Avaya VSP  Avaya Virtual Services Platform
BPDU  bridge protocol data unit
CFM  connectivity fault management
CLI  command line interface
DToR  distributed top-of-rack
ECMP  equal cost multi-path
EDM  Enterprise Device Manager
ERS  Avaya Ethernet Routing Switch
ESM  Ethernet Switch Module
IGP  interior gateway protocol
IST  interstitch trunking
L2VSN  Layer 2 virtual services network
L3VSN  Layer 3 virtual service network
LAN  local area network
MLT  multi-link trunking
MPLS  multi-protocol label switching
OSPF  open shortest path first
PIM  protocol-independent multicast
PoE  Power over Ethernet
RP  rendezvous point
RSMLT  routed split multi-link trunking
SCP  secure copy
SMLT  split multi-link trunking
SNMP  simple network management protocol
SPB  shortest path bridging
STP  spanning tree protocol
vIST  virtual interswitch trunking
VRF  virtual routing and forwarding
VSP  Avaya Virtual Services Platform
Send us your comments and suggestions.