Deployment Guide For CCTV / IPTV Systems Using VSP Switches with Fabric Connect SPBm

Abstract: This technical configuration guide provides an overview and examples of an IP Video or CCTV network deployment using Extreme Networks VSP switches leveraging Shortest Path Bridging (SPBm)

Published: June 2023

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see:
https://www.extremenetworks.com/Company/legal/trademarks/

Open Source Declarations

Some software files have been licensed under certain open-source or third-party licenses. End-user license agreements and open-source declarations can be found at:
https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Prerequisites

- Five or more VSP or Universal switches running VOSS/Fabric Engine 8.6 or later.
- IPTV/CCTV system or tools that can generate IGMP multicast traffic.

Overview

Foreword

For several decades video surveillance has become a critical component of every organization's security stance. It can be used for inventory control and theft prevention for retail. Fair-play assurance for casinos. Public safety for large venues, airports, and sporting events. Perimeter security for secure access areas. Video surveillance systems are everywhere and require near 100% uptime.

These video systems (or CCTV systems) were deployed using analog signaling technologies which required massive cabling infrastructure. As a result, they lacked scale.

With the introduction of IP based CCTV systems, security integrators have been able to deploy large scale systems using a single ethernet network of switches and routers. However, these systems were traditionally deployed in either of two ways:

- One large broadcast domain where all IP cameras, viewing stations, and recording appliances are in the same network. This is easy to deploy but will require spanning tree that may be susceptible to topology re-convergence and outages. All devices being in one large IP range also creates security concerns because all devices are accessible to anyone that can get on the network.
- A CCTV system using a routed network, which is far more scalable and reliable. However, routed networks are far more complex to deploy and manage as they require many underlying protocols such as RIP or OSPF, spanning tree and PIM for multicast.

This document will outline an optimal example of CCTV deployment using Extreme Networks' VSP switches which leverage SPBm. Delivering the scale and security and reliability of a routed network without the complexity seen in traditional networks.

Multicast Routing with SPBm Overview

Multicast allows information to be efficiently forwarded from a source device to many receivers who have expressed an interest in joining the multicast group. There are many examples of applications that benefit from or require multicast support, such as Video Surveillance, IPTV, Video Conferencing, Financial market data distribution on trading floors, and Ghost distribution of backup disk images to multiple computers simultaneously.

For every multicast packet that the source generates, the network must be able to replicate it to every receiver in the group. This should be done in an efficient manner such that packet

replication occurs at every branch in the multicast delivery tree and delivery to each and every receiver is along the shortest path towards that receiver. This is exactly what Fabric Connect does.

Shortest Path Bridging is the only networking technology to date that has been engineered to properly handle multicast from the ground up. This contrasts with IP and MPLS, where IP Multicast was retrofitted as an afterthought and is the reason why the IP multicast control planes defined for operation over IP (PIM), and MPLS IPVPNs (draft Rosen) as well as EVPN are so complex and inefficient.

Layer 2 Edge vs Layer 3 Edge

To understand the power and flexibility that Fabric Connect can deliver for a CCTV deployment, it is critical to understand the choices a network architect has when considering a network design.

Networks are generally deployed in one of two ways:

1 – L3 Core, L2 Edge: In a L3 Core L2 Edge network, all routing takes place in the core switches. Edge access switches are deployed as L2 access switches using only VLAN separation. VLANs are extended to the edge access switches using 802.1q tagging.

2- L3 routing at the edge: In this network design, routing is configured on the core and the edge access switches. Layer 2 domains are not extended beyond the local switch.

When CCTV is the application on the network, the advantages of a routed edge network far outweigh the benefits of an L2 edge network.

Using a Fabric Connect solution with VSP switches gives network architects the flexibility to choose either L2 or L3 edge.

This guide will demonstrate a routed L3 edge design.

Objectives

This guide describes the preparation and steps required to deploy a VSP network for a CCTV system leveraging Shortest Path Bridging (SPBm).

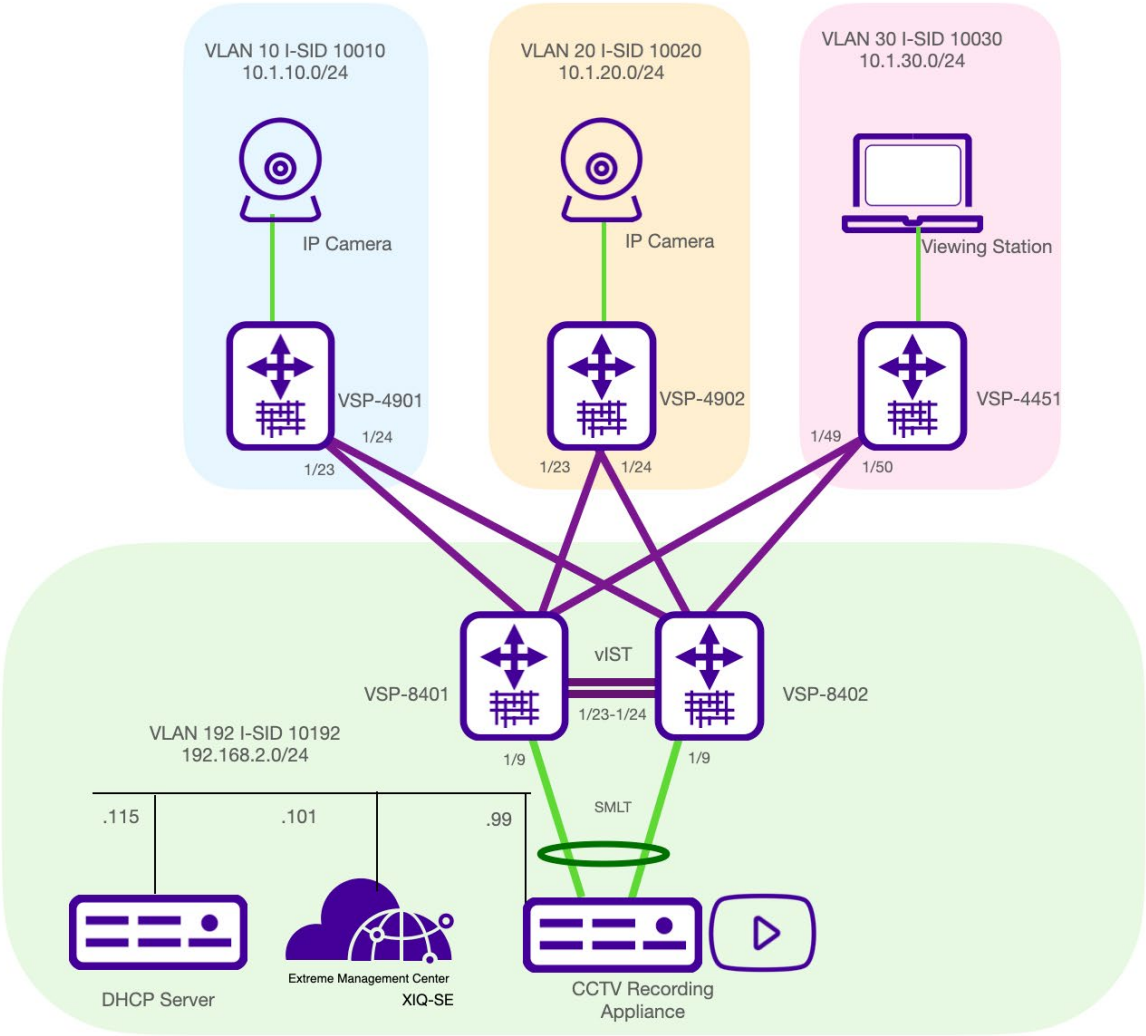
- Build VLAN, IP and switching naming convention plan.
- Build a dual VSP vIST cluster as the campus core that will connect all edge switches, video appliances and servers in a redundant manner.
- Build example configuration for three VSP edge switches.
- Validate multicast routing.

Network Diagram

This guide uses the following network setup as an example of a VSP L3 edge deployment for CCTV. It consists of the following devices and software:

- Two VSP core/distribution switches running VOSS/Fabric Engine 8.6 or laterin a dual vIST MC-LAG cluster.
- Three VSPs edge switches running VOSS/Fabric Engine 8.6 or later.
- Two IP video cameras. In lieu of IP cameras, we are using raspberry PIs as IGMP traffic generators using open-source video software.
- One or more laptops as a viewing station using open-source video software.
- One Linux server acting as the CCTV recording and steaming media appliance using open-source video software.

One host VM for hosting the virtual appliance of XMC/XIQ-SE and a Linux DHCP server (optional).



Caution
This Technical Configuration Guide for CCTV deployments does not provide details into the inner workings and fundamentals of Shortest Path Bridging/802.1aq. One should consult the SPBVOSS_TSC.CG.PDF and NETWORK VIRTUALIZATION USING FABRIC CONNECT documents for a comprehensive view into the Fabric Connect solution, protocols, and terminology. Both documents can be found on the Extreme Networks Product Documentation page.

Switch, VLAN, I-SID, and IP Address Plan

The following tables detail the unique VLAN, IP, and SPBm values required for each VSP in the network.

vIST Core VSP 8400s

Table 1. Core VSP SPBm and IP address values

	VSP-CORE-01	VSP-CORE-02
System Name	8401-Core01	8402-Core02
System- ID	0000.0001.8401	0000.0001.8402
Nick Name	0.84.01	0.84.02
BLVANS	4051-4052	
Manual Area	49.0001	
vIST VLAN & I-SID	2 / 10002	
SMLT V-BMAC	XX:XX:XX:XX:84:FF (where “84” can be unique for you)	
vIST VLAN IP	172.16.2.1/30	172.16.2.2/30
Management CLIP	172.16.84.1/32	172.16.84.2/32
Loopback CLIP	172.17.84.1/32	172.17.84.2/32
Server VLAN & I-SID	192 / 10192	
Server VLAN IP	192.168.2.2/24	192.168.2.3/24
Server VLAN VRRP VIP	192.168.2.1	192.168.2.1

Edge VSP SPBm, VLAN, and IP values

Table 2. Edge VSP SPBm and IP address values

	VSP-Edge-01	VSP-Edge-02	VSP-Edge-03
System Name	4901-edge-01	4901-edge-02	4451-edge-03
System- ID	0000.0001.4901	0000.0001.4902	0000.0001.4451
Nick Name	0.49.01	0.49.02	0.44.51
BLVANS	4051-4052		
Manual Area	49.0001		
Management CLIP	172.16.49.1/32	172.16.49.2/32	172.16.44.51/32
Loopback CLIP	172.17.49.1/32	172.17.49.2/32	172.17.44.51/32
Video VLAN & I-SID	10 / 10010	20 / 10020	30 / 10030
Video VLAN IP	10.1.10.1/24	10.1.20.1/24	10.1.30.1/24

Note

For the data centre services and edge routed VLANs we are using a /24-bit (or 255.255.255.0) subnets as an example only. However, /24-bit subnets are favourable since they are concise, easy to work with and do allow for growth. IP address exhaustion is often not a concern in closed CCTV systems. VOSS switches do support all the standard CIDR subnet ranges should you wish to use smaller or larger subnet ranges.

VSP CORE vIST MC-LAG Configuration

vIST Core Creation

SPBm combined with Extreme's SMLT/MLAG and vIST offers an active-active solution with redundant distribution between two VSP switches. vIST allows network architects to deploy two VSP switches in a dual MC-LAG cluster that behaves as a single unit that will share forwarding data, topology, and route calculations.

The creation of the vIST requires five values and is detailed in the examples below.

- Dedicated vIST VLAN.

- I-SID value for the vIST VLAN.
- Two IP addresses, one per switch.
- SPBm peering configuration.
- Virtual Backbone MAC address shared on both VSP peers.

For the purpose of this design we will use a Multi-Link-Trunk (MLT) between the two core VSPs. This will deliver redundancy in the event of a port, optical transceiver, or fiber failure. The MLT will also add traffic capacity in its normal state. MLT is the preferred link aggregation protocol to use between Extreme VSP, ERS and EXOS switches.

To manage and route IP traffic we will demonstrate how to configure management interfaces and a routed network for data center services with failover redundancy.

To deliver redundancy between the dual vIST cluster and the server appliances we will demonstrate how to configure LACP/802.3ad. Most enterprise grade networking, server, and operating system vendors support the 802.3ad LACP standard for added capacity and redundancy. Consult 3rd-party manufacturer's literature for the optimal LAG protocol to use on your VSP core.

Core Design

The following image is the design of the vIST core we will be configuring:

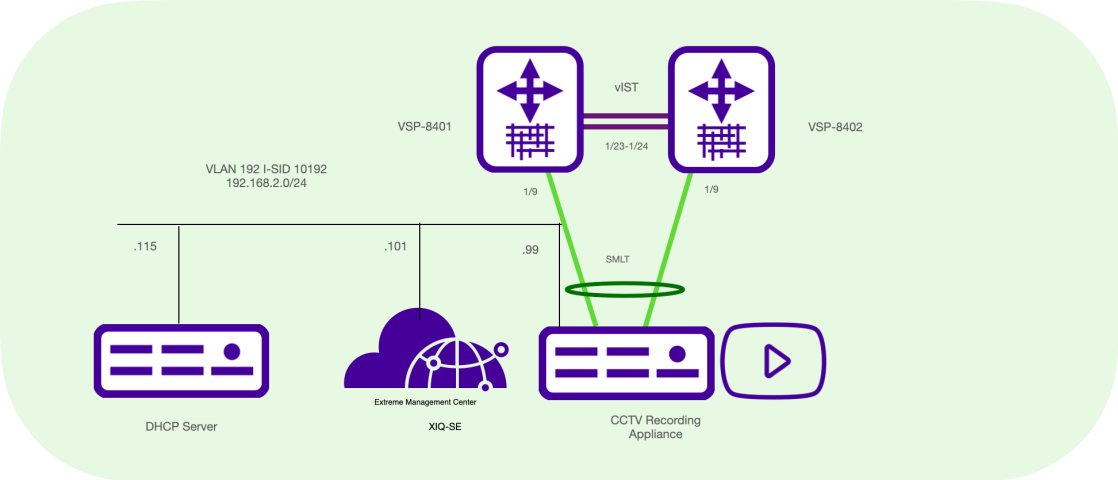


Figure 1.

Warnings
This example is using two VSP8404s, each with a single 8424XS module in slot no1. Your design and switch selection may be different. Be mindful of your port ranges and values for the switches you are working with.

Warnings (Factory default VSP before continuing)

VOSS 8.2 and later introduced a new baseline configuration with several functions pre-configured to support Zero Touch deployments. As this guide is demonstrating a manual configuration, use the following commands to delete all configurations and reboot the VSP into a default state.

`#copy config.cfg backupVSPconfig.cfg` (optional: if you wish to save the current configuration)

`#remove config.cfg` (choose YES to delete the runtime config)

```
#conf t
#boot config flags factorydefaults
#exit
```

`#boot` (choose YES to reboot the switch)

Upon reboot perform the following command to view the VLAN settings and validate defaults.

```
#show vlan adv
```

If you only see **VLAN 1** you have successfully rebooted the switch to a defaulted state.

Caution

The vIST configuration requires the architect to select a virtual Backbone MAC address (or BMAC). The BMAC address for your deployment will be unique to one shown below. It is best practice to use the first 8 characters from the Base MAC address of one the VSPs and append an FF:FF as the final 4 characters. The BMAC value is the same on both VSPs in the vIST cluster. See Line 15 in table 3.

Use the command `show sys-info` to find the base MAC address from one of the switches.

Note

It is good practise to remove VLAN 1 from all ports during the initial configuration of the switch. See line 11 from Table 3. VLAN 1 can be added if required.

Initial SPBm Configuration of VSP Cores

Table 3. Initial configuration of VSP cores

VSP-Core-01	VSP-Core-02
spbm prompt 8401 router isis sys-name 8401_CORE01 system-id 0000.0001.8401	spbm prompt 8402 router isis sys-name 8402_CORE02 system-id 0000.0001.8402

```
spbm 1                                          spbm 1
spbm 1 nick-name 0.84.01                        spbm 1 nick-name 0.84.02
spbm 1 b-vid 4051-4052 primary 4051             spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable                         spbm 1 multicast enable

manual-area 49.0001                             manual-area 49.0001

vlan member remove 1 1/1-1/24                   vlan member remove 1 1/1-1/24
vlan create 4051 name "BVLAN-1" type spbm-      vlan create 4051 name "BVLAN-1" type spbm-
bvlan                                           bvlan
vlan create 4052 name "BVLAN-2" type spbm-      vlan create 4052 name "BVLAN-2" type spbm-
bvlan                                           bvlan

router isis                                     router isis
spbm 1 smlt-virtual-bmac 64:6a:52:b8:84:FF      spbm 1 smlt-virtual-bmac 64:6a:52:b8:84:FF
spbm 1 smlt-peer-system-id 0000.0001.8402       spbm 1 smlt-peer-system-id 0000.0001.8401
exit                                            exit
vlan create 2 name IST type port-mstprstp 0     vlan create 2 name IST type port-mstprstp 0
vlan i-sid 2 2                                  vlan i-sid 2 2
interface vlan 2                                interface vlan 2
ip address 172.16.2.1/30                        ip address 172.16.2.2/30
exit                                            exit
virtual-ist peer-ip 172.16.2.2 vlan 2           virtual-ist peer-ip 172.16.2.1 vlan 2

Router isis                                     Router isis
Router isis enable                              Router isis enable
Cfm spbm enable                                 Cfm spbm enable
```

Validate Initial SPBm Configuration

SPBm should be enabled as per below. If SPBm is not enabled, validate the configuration from the example above.

```
8401X:1#show spbm
                                  spbm : enable
                             ethertype : 0x8100
                       nick-name server : disable
                    nick-name allocation : static


8402:1(config)#show isis

================================================================================================
========
                                ISIS General Info
================================================================================================
========
                              AdminState : enabled
                              RouterType : Level 1
                               System ID : 0000.0001.8402
                    Max LSP Gen Interval : 900
                                  Metric : wide
                     Overload-on-startup : 20
                                Overload : false
                           Csnp Interval : 10
```

```
                    PSNP Interval : 2
                Rxmt LSP Interval : 5
                        spf-delay : 100
                      Router Name : 8402_CORE02
```

MLT and NNI Configuration

The two VSP core switches are configured for SPBm and now require Network -to- Network Interfaces (NNIs) to connect the VSP switches together into one SPBm fabric.

For the links between the two VSP cores we will be creating an MLT LAG bonding with two ports: 1/23 and 1/24. The MLT will be enabled for SPBm by adding the MLT interface to the SPBm group.

At this time, we will also configure the individual links that will connect the three edge VSP4000 series switches to the SPBm network: Ports 1/1 -to- 1/3 on both VSP cores. This will deliver two links per edge switch in a full redundant mesh topology.

Table 4. MLT and NNI for core VSPs

VSP-Core-01 & 02 (configuration is the same for both core switches)
mlt 1 enable mlt 1 member 1/23-1/24 mlt 1 encap dot1q interface gig 1/23-1/24 no spanning-tree mstp force en yes no shut untagged-frames-discard interface mlt 1 isis isis spbm 1 isis enable exit interface gig 1/1-1/3 isis isis spbm 1 isis en untagged-frames-discard no spanning-tree mstp force-port-state enable y no shut

Validate NNI and vIST Configuration

With SPBm globally enabled and the NNIs configured the following commands shown below will validate the VSP IS-IS adjacencies and vIST state.

You will want to observe that the VSP core switches see their ISIS neighbours over MLT 1. Also notice that the vIST state as “UP”

Note
You will only need to perform the validation on one of the two VSP cores. If it is correct on one of the VSPs, it is correct on both switches in the vIST cluster.

```
8401:1#show isis adjacencies
********************************************************************************
                              ISIS Adjacencies
================================================================================================
INTERFACE         L STATE        UPTIME PRI HOLDTIME    SYSID             HOST-NAME
STATUS    AREA       AREA-NAME
------------------------------------------------------------------------------------------------
Mlt1              1 UP         00:01:10 127         20 0000.0001.8402    8402_CORE02
ACTIVE    HOME

------------------------------------------------------------------------------------------------
Home:    1 out of 1 interfaces have formed an adjacency
------------------------------------------------------------------------------------------------
8401:1#show virtual-ist

                                    IST Info
================================================================================================
PEER-IP              VLAN     ENABLE    IST
ADDRESS              ID       IST       STATUS
------------------------------------------------------------------------------------------------
172.16.2.2           2        true      up


NEGOTIATED                                    MASTER/
DIALECT      IST STATE                        SLAVE
------------------------------------------------------------------------------------------------
v6.0         Up                               Slave
```

VSP Core IP Management and Routing Configuration

VOSS 8.2 and later introduced a security and management architecture enhancement called Segmented Management. With segmented management a network architect must explicitly select what IP interfaces are able to reply to management protocols (ex. Telnet, SSH, HTTPS, SNMP).

In VSP and Universal Hardware platforms that support VOSS 8.2 or later, one can create three interfaces for remote management and monitoring.

- Out of band interface.

- VLAN IP interface.
- In-band CLIP interface

For remote management in a routed network it is best practice to create a routed circuit-less interface (CLIP) as the interface to reply to management protocols. This is referred to as the “mgmt clip” address.

It is optional, but highly recommended to configure a loopback address as well. A loopback interface is only required for troubleshooting with ICMP/PING. Without a pre-configured loopback interface any ping command will require an explicit source IP in the ping command syntax.

Management CLIP and Loopback CLIP

Table 5. Management CLIP and Loopback CLIP.

VSP-Core-01	VSP-Core-02
mgmt clip ip address 172.16.84.1/32 enable interface loopback 1 ip address 1 172.17.84.1/32 router isis ip-source-address 172.17.84.1 spbm 1 ip en router isis redistribute direct redistribute direct enable exit isis apply redistribute direct	mgmt clip ip address 172.16.84.2/32 enable interface loopback 1 ip address 1 172.17.84.2/32 router isis ip-source-address 172.17.84.2 spbm 1 ip en router isis redistribute direct redistribute direct enable exit isis apply redistribute direct

Note

The Management CLIP and Loopback clips must be /32-bit IP addresses.

Data Centre Services VLAN and IP Configuration

In a routed data network, it is ideal to have all services localized within their own VLANs. In this scenario all data center applications, servers, and appliances are in their own VLAN localized on the two VSP core switches. These services and VLANs are not extended beyond the core switches. This allows for broadcast domains to be localized to each switch or vIST cluster. Only Multicast and unicast traffic is forwarded to each SPBm node.

In this example we are configuring a VLAN 192 between both VSP vIST switches using VRRP. Each VSP switch will have a logical address for VLAN 192 and will share a virtual IP address (or VIP). The commands to configure VLAN 192, routing and VRRP for each switch is identical except for line # 4. Each VSP must have a unique logical address. In the example below VSP 1 has 192.168.2.2, VSP 2 has 192.168.2.3. Both VSPs share a VRRP VIP address of 192.168.2.1.

Table 6. Vlan 192 and VRRP configuration

VSP-Core-01	VSP-Core-02

vlan create 192 type port-mstprstp 0
vlan i-sid 192 10192
interface Vlan 192
ip address 192.168.2.2/24
ip spb-multicast en
ip vrrp version 2
  ip vrrp address 1 192.168.2.1
  ip vrrp 1 adver-int 30 backup-master
enable holddown-timer 60
  ip vrrp 1 priority 200
  ip vrrp 1 enable
	vlan create 192 type port-mstprstp 0
	vlan i-sid 192 10192
	interface Vlan 192
	ip address 192.168.2.3/24
	ip spb-multicast en
	ip vrrp version 2
	  ip vrrp address 1 192.168.2.1
	  ip vrrp 1 adver-int 30 backup-master
	enable holddown-timer 60
	  ip vrrp 1 enable

Note

1 – Core #1 should have a VRRP priority of 200. Core #2 can be set with the default VRRP priority of 100 which does not require an explicit configuration entry.

2- BackupMaster creates an active-active environment for routing. If you enable BackupMaster on the backup router, the backup router no longer switches traffic to the VRRP Master. Instead, the BackupMaster routes all traffic received on the BackupMaster IP interface according to the switch routing table.

Note

VOSS supports two different first hop redundancy protocols. 1- VRRP, which is based on the industry standard. 2 - The Extreme proprietary R-SMLT. If you know for certain your campus network core is only ever going to be two VSP switches you can use R-SMLT. VRRP is more flexible as it allows for growth should you wish to add more switches to your core or extend a routed VRRP domain to another switch in the network.

Validate IP Management and Routing

From one of the two vIST core switches the following commands will validate that the management CLIP, Loopback CLIP and routed VRRP interface for VLAN 192 is active from both switches. Below is the example from VSP-Core-02

Table 7. Show VRRP commands from VSP Core 2

```
8402:1(config)#show ip route
================================================================================================
                                        IP Route - GlobalRouter
================================================================================================
                                                    NH                          INTER
```

```
DST             MASK            NEXT                VRF/ISID        COST    FACE     PROT
AGE TYPE   PRF
-------------------------------------------------------------------------------------------
172.16.2.0      255.255.255.252 172.16.2.2          -               1       2        LOC  0
DB     0
172.16.84.1     255.255.255.255 8401_CORE01         GlobalRouter    10      4051     ISIS 0
IBS    7
172.16.84.2     255.255.255.255 172.16.84.2         -               1       4090     LOC  0
DB     0
172.17.84.1     255.255.255.255 8401_CORE01         GlobalRouter    10      4051     ISIS 0
IBS    7
172.17.84.2     255.255.255.255 172.17.84.2         -               1       0        LOC  0
DB     0
192.168.2.0     255.255.255.0   192.168.2.3         -               1       192      LOC  0
DB     0
```

You should see the IP routing information for the vIST, CLIP addresses and the new data centre VLAN

Table 8. Show VRRP commands from VSP Core 1

```
8401:1(config)#show ip vrrp address
                           VRRP Info - GlobalRouter
===============================================================================================

VRRP ID  P/V      IP              MAC                STATE    CONTROL  PRIO  ADV VERSION
-----------------------------------------------------------------------------------------------
---------------
1        192      192.168.2.1     00:00:5e:00:01:01  Backup   Enabled  100   30  2

1 out of 1 Total Num of VRRP Address Entries displayed.


VRRP ID  P/V      MASTER          UP TIME               HLD DWN  CRITICAL IP(ENABLED)
VERSION
-----------------------------------------------------------------------------------------------
1        192      192.168.2.3     0 day(s), 00:05:46    0        0.0.0.0          (No)  2

1 out of 1 Total Num of VRRP Address Entries displayed.
```

From the output above we can see from VSP Core 1 VRRP is enabled for VLAN 192, the VIP is configured for 192.168.2.1 and the neighbour at 192.168.2.3 is the master.

LACP LAG to Video Server

To offer the most capacity and resiliency it is best practice to enable two links across the vIST cluster as a bonded pair or LAG group. This will deliver the best resiliency and service to the servers and appliances in the event of a link or switch failure in the core, or a NIC failure on the server appliance. The industry standard to accomplish this is 802.3ab LACP and is the best option when connecting to 3rd party devices as LACP is supported widely across the industry. In the example below, ports 1/9 will be configured for VLAN 192, enabled as an MLT/SMLT for LACP, connected to two NIC interfaces on the server appliance. Fail-over will be sub-second in normal environments.

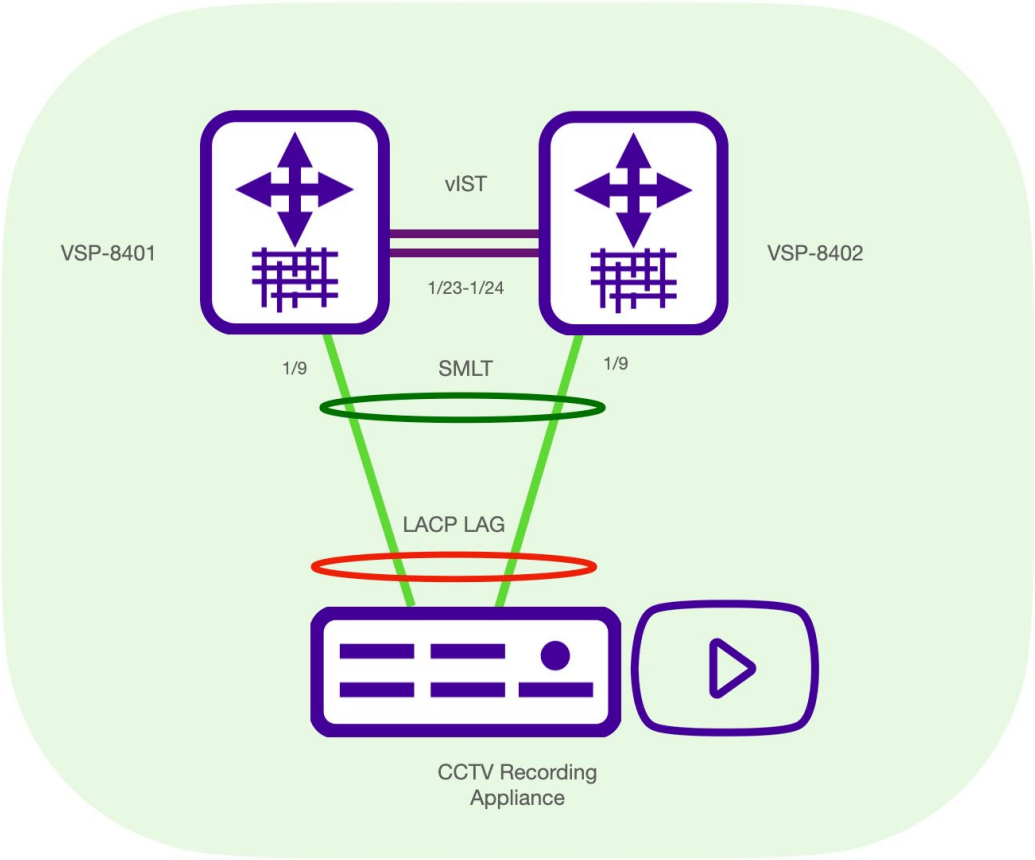


Table 9. VSP vIST core lacp configuration.

VSP-Core-01 & 02 (configuration is the same for both switches)

```
vlan members add 192 1/9
mlt 9 enable name "LACP_VideoServer"
interface mlt 9
smlt
lacp enable key 9
Exit
lacp enable

interface gigabitEthernet 1/9
lacp key 9
lacp aggregation en
lacp timeout-time short
Lacp enable
Exit
lacp smlt-sys-id XX:XX:XX:XX:XX:XX /// Chose the Base MAC from VSP_Core_01
Lacp enable

Int gig 1/9
No shut
no spanning-tree mstp force-port-state en
Yes
```

Note

The configuration above is an example of 1/9 as an access port. An example of how to configure LACP for a tagged port is available on the Extreme GTAC website. Any port attributes such as tagging and vlan assignment must be made before configuring the LACP/LAG group.

You must choose an LACP MAC address for the MC-LAG cluster which needs to be unique to the network. To create the LACP address you can use the base MAC address from one of the two switches in your vIST cluster and apply that MAC address to the config on both switches. A "`show sys-info`" command will expose the base MAC address.

Caution

Consult the LACP/LAG configuration materials from your 3rd party devices for the optimal LAG/LACP configuration on the VSP. Some server virtualization vendors do not require switch NICs to be in LAG/LACP groups for active-active links.

Example: Microsoft uses NIC teaming.

Validate LACP/SMLT

The two following show commands, "show lacp" and "show smlt mlt", will validate your LACP configuration and demonstrate if both links in the SMLT/LACP LAG group are up, active, and balanced. For MLT ID ADMIN and CURRENT Type the optimal status is SMLT

```
8401:1#show lacp
                            Lacp Global Information
================================================================================================
               SystemId: 64:6a:52:b8:f0:00
           SmltSystemId: 40:88:2f:54:ac:00
                   Lacp: enable
        system-priority: 32768
                timeout-admin: 3
     fast-periodic-time-admin: 1000
     slow-periodic-time-admin: 30000
         aggr-wait-time-admin: 2000
                timeout-oper: 3
     fast-periodic-time-oper: 1000
     slow-periodic-time-oper: 30000
         aggr-wait-time-oper: 2000
```

```
8401:1#show smlt mlt
                                    Mlt SMLT Info
================================================================================================
========
MLT    ADMIN     CURRENT
ID     TYPE
------------------------------------------------------------------------------------------------
---------------
9      smlt
```

Caution

If the output for “show smlt mlt” indicates SMLT and NORM: NORM is not an ideal state. This means that only one of the two links is active, and the LAG is in a normal state, not an active-active state with two good links. Ensure all links are connected to the correct ports and configuration is validated.

Edge VSP Configuration

The network core is now ready to accept the edge switches into the SPBm fabric network. As detailed in the overview we will be demonstrating how to configure an SPBm network with an L3 edge design.

Each VSP will be the owner of its own routed network. Only unicast and multicast will be forwarded between the VSP switches.

Two SPB NNIs connected to both cores for redundancy in a full mesh topology:

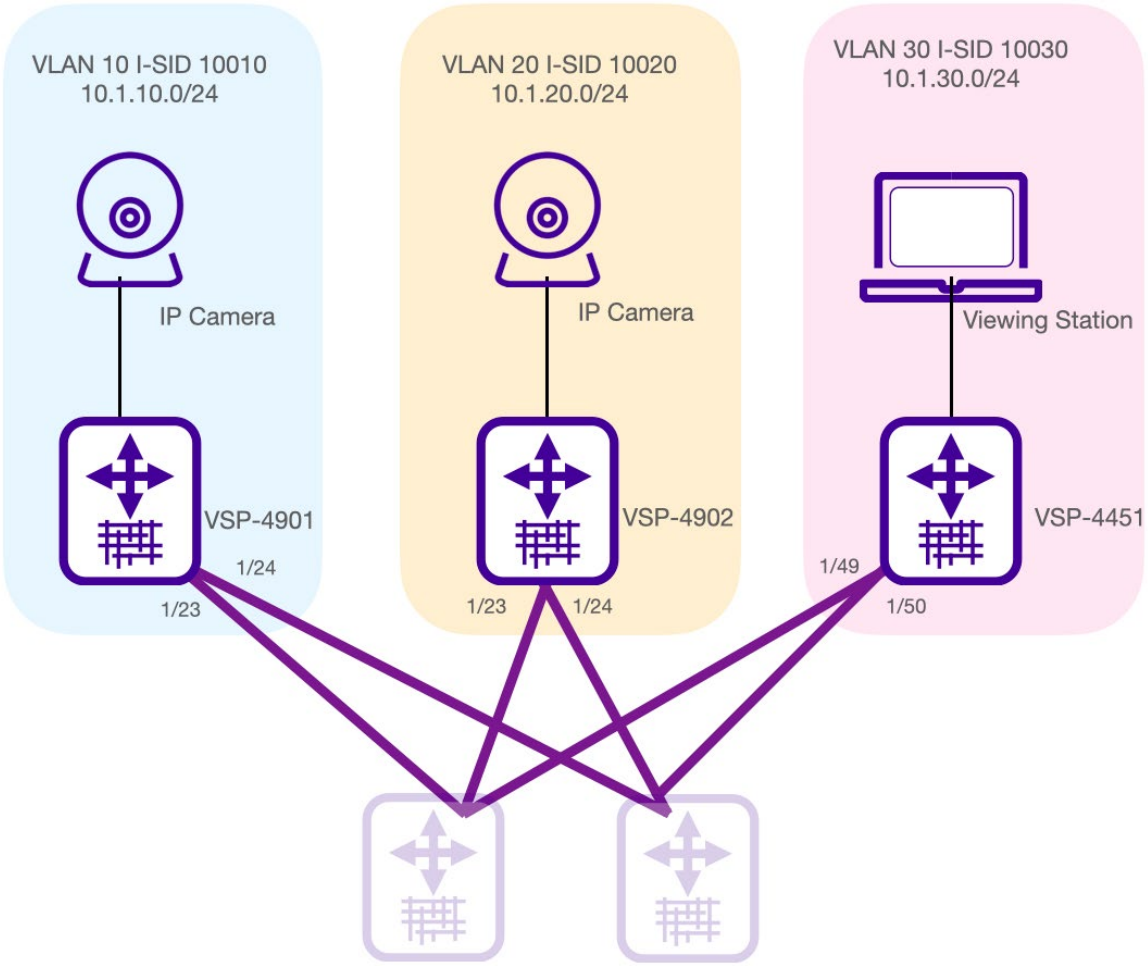


Table 10. VSP 4901 Configuration

VSP-Edge-01

```
spbm
prompt 4901
router isis
sys-name 4901-edge-01
system-id 0000.0001.4901
spbm 1
spbm 1 nick-name 0.49.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable

manual-area 49.0001

vlan member remove 1 1/1-1/24
vlan create 4051 name "BVLAN-1" type spbm-bvlan
vlan create 4052 name "BVLAN-2" type spbm-bvlan

Router isis
Router isis enable
Cfm spbm enable

mgmt clip
ip address 172.16.49.1/32
enable

interface loopback 1
ip address 1 172.17.49.1/32
router isis
ip-source-address 172.17.49.1
spbm 1 ip en
router isis
redistribute direct
redistribute direct enable
exit
isis apply redistribute direct

vlan members remove 1 1/1-1/24
interface gig 1/23-1/24
isis
isis spbm 1
isis en
untagged-frames-discard
no spanning-tree mstp force-port-state enable
y
no shut

vlan create 10 type port-mstprstp 0
vlan i-sid 10 10010
interface Vlan 10
ip address 10.1.10.1/24
ip spb-multicast en

vlan members add 10 1/1-1/12
int gig 1/1-1/12
no shut
```

Table 11. VSP 4902 Configuration

VSP-Edge-02

```
spbm
prompt 4902
router isis
sys-name 4902-edge-02
system-id 0000.0001.4902
spbm 1
spbm 1 nick-name 0.49.02
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable

manual-area 49.0001

vlan member remove 1 1/1-1/24
vlan create 4051 name "BVLAN-1" type spbm-bvlan
vlan create 4052 name "BVLAN-2" type spbm-bvlan

Router isis
Router isis enable
Cfm spbm enable

mgmt clip
ip address 172.16.49.2/32
enable

interface loopback 1
ip address 1 172.17.49.2/32
router isis
ip-source-address 172.17.49.2
spbm 1 ip en
router isis
redistribute direct
redistribute direct enable
exit
isis apply redistribute direct

interface gig 1/23-1/24
isis
isis spbm 1
isis en
untagged-frames-discard
no spanning-tree mstp force-port-state enable
y
no shut

vlan create 20 type port-mstprstp 0
vlan i-sid 20 10020
interface Vlan 20
ip address 10.1.20.1/24
ip spb-multicast en

vlan members add 20 1/1-1/12
int gig 1/1-1/12
no shut
```

Table 12. VSP 4451 Configuration

VSP-Edge-03

```
spbm
prompt 4451
router isis
sys-name 4451-edge-03
system-id 0000.0001.4451
spbm 1
spbm 1 nick-name 0.44.51
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable

manual-area 49.0001

vlan member remove 1 1/1-1/24
vlan create 4051 name "BVLAN-1" type spbm-bvlan
vlan create 4052 name "BVLAN-2" type spbm-bvlan

Router isis
Router isis enable
Cfm spbm enable

mgmt clip
ip address 172.16.44.51/32
enable

interface loopback 1
ip address 1 172.17.44.51/32
router isis
ip-source-address 172.17.44.51
spbm 1 ip en
router isis
redistribute direct
redistribute direct enable
exit
isis apply redistribute direct
interface gig 1/49-1/50
isis
isis spbm 1
isis en
untagged-frames-discard
no spanning-tree mstp force-port-state enable
y
no shut

vlan create 30 type port-mstprstp 0
vlan i-sid 30 10030
interface Vlan 30
ip address 10.1.30.1/24
ip spb-multicast en

vlan members add 30 1/1-1/12
int gig 1/1-1/12
no shut
```

DHCP Relay

Should your network be configured with DHCP for cameras, PCs, and viewing stations to receive their IP address from a DHCP server; the config is as indicated below in Table 14.

Note

In the DHCP Relay example shown below you must use the gateway address of the VLAN as the relay forwarding path. For each switch it is 10.1.XX.1. In the example below the DHCP server is 192.168.2.115. You will need to adjust these parameters according to your network configuration.

Table 13.

Caution

If you wish to configure DHCP Relay within a VLAN that is enabled for VRRP, you must use the logical local address as the forwarding path configured for that local VLAN. **DO NOT** use the VRRP VIP address as the forwarding path.

Table 14. VSP DCHP Configuration

VSP DHCP Configuration VSP Edge 01

```
Interface vlan 10
Ip dhcp-relay
Ip dhcp-relay broadcast
exit
ip dhcp-relay fwd-path 10.1.10.1 192.168.2.115
ip dhcp-relay fwd-path 10.1.10.1 192.168.2.115  enable
ip dhcp-relay fwd-path 10.1.10.1 192.168.2.115  mode bootp_dhcp
```

VSP DHCP Configuration VSP Edge 02

```
Interface vlan 20
Ip dhcp-relay
Ip dhcp-relay broadcast
exit
ip dhcp-relay fwd-path 10.1.20.1 192.168.2.115
ip dhcp-relay fwd-path 10.1.20.1 192.168.2.115  enable
ip dhcp-relay fwd-path 10.1.20.1 192.168.2.115  mode bootp_dhcp
```

VSP DHCP Configuration VSP Edge 03

```
Interface vlan 30
Ip dhcp-relay
Ip dhcp-relay broadcast
exit
ip dhcp-relay fwd-path 10.1.30.1 192.168.2.115
ip dhcp-relay fwd-path 10.1.30.1 192.168.2.115  enable
```

```
ip dhcp-relay fwd-path 10.1.30.1 192.168.2.115  mode bootp_dhcp
```

Validate SPBm Network

At this point you should now have a vIST core cluster configured and all three edge switches connected to the core. The following commands will validate network configuration:

'show ISIS adjacencies' -- This command should be executed on each switch. For the three edge switches you should see two ISIS adjacencies. One to VSP Core 1 and one to Core 2. On the VSP Cores you should see a single link to each edge VSP and to the vIST neighbour. The neighbours will be identified by their System-ID and Host-Name.

Table 15. 'Show ISIS adjacencies' example from VSP 4901-01

```
4901:1#show isis adjacencies
                                                        ISIS Adjacencies
================================================================================================
=====================================
INTERFACE          L STATE        UPTIME PRI HOLDTIME   SYSID             HOST-NAME
STATUS   AREA        AREA-NAME
------------------------------------------------------------------------------------------------
-------------------------------------
Port1/23           1 UP         05:08:07 127         27 0000.0001.8401    8401_CORE01
ACTIVE   HOME
Port1/24           1 UP         05:08:01 127         20 0000.0001.8402    8402_CORE02
ACTIVE   HOME
```

Table 16. Show ISIS adjacencies example from VSP Core 01.

```
8401:1#show isis adjacencies
                                                        ISIS Adjacencies
================================================================================================
INTERFACE          L STATE        UPTIME PRI HOLDTIME   SYSID             HOST-NAME
STATUS   AREA        AREA-NAME
------------------------------------------------------------------------------------------------
Mlt1               1 UP         05:10:12 127         23 0000.0001.8402    8402_CORE02
ACTIVE   HOME
Port1/1            1 UP         05:10:17 127         25 0000.0001.4901    4901-edge-01
ACTIVE   HOME
Port1/2            1 UP         05:10:17 127         22 0000.0001.4902    4902-edge-02
ACTIVE   HOME
Port1/3            1 UP         05:10:16 127         23 0000.0001.4451    4451-edge-03
ACTIVE   HOME
```

The 'show isis spbm nick-name' command can be executed from any switch in the fabric. This will validate that all switches are registered to the SPBm area. In the example below from VSP 4901, all switches are present and identified in the fabric by Nick-Name and Host-Name. As all 5 switches are present, we have validated that all five switches are configured correctly for SPBm.

Table 17. 'Show isis spbm Nick-name' output from VSP 4901.

```
8401:1#show isis spbm nick-name
                                                          ISIS SPBM NICK-NAME
================================================================================================
LSP ID                          LIFETIME  NICK-NAME VIRTUAL-BMAC         HOST-NAME
AREA       NAME
------------------------------------------------------------------------------------------------
0000.0001.4451.00-00            481       0.44.51   00:00:00:00:00:00    4451-edge-03
HOME
0000.0001.4901.00-00            1121      0.49.01   00:00:00:00:00:00    4901-edge-01
HOME
0000.0001.4902.00-00            1118      0.49.02   00:00:00:00:00:00    4902-edge-02
HOME
```

```
0000.0001.8401.00-00          496        0.84.01    64:6a:52:b8:ff:ff    8401_CORE01
HOME
0000.0001.8402.00-00          501        0.84.02    64:6a:52:b8:ff:ff    8402_CORE02
HOME
```

Note

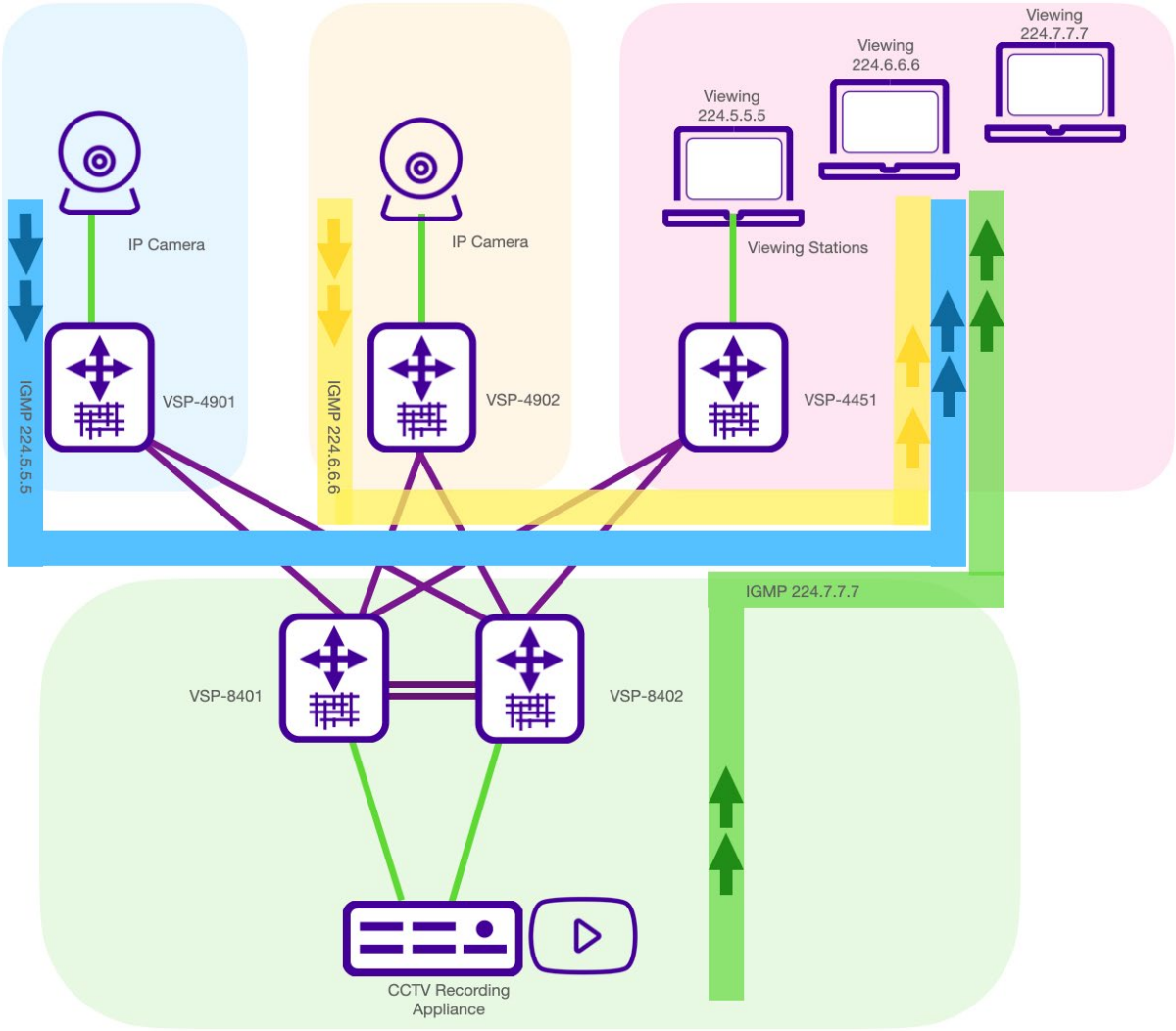
In the table above you will notice that the three edge switches do not have virtual BMACs; they are stand-alone switches, they are not part of a vIST cluster and do not require a BMAC.

Validate Multicast Traffic

Using open-source multicast video tools we will generate three IGMP steams.

- Camera 1 connected to VSP 4901 is streaming IGMP group 224.5.5.5.
- Camera 2 connected to VSP 4902 is streaming IMGP group 224.6.6.6.
- CCTV Recording appliance connected to vIST cluster is steaming IGMP group 224.7.7.7.

Three viewing stations connected to VSP 4451 are requesting IGMP joins to those three IGMP groups.



Validate IMGP Senders

Table 18. VSP 4901 IGMP validation

The “show ip igmp sender” command will show the results that on port 1/1 the camera is sending on group address 224.5.5.5

```
4901:1#show ip igmp sender
                          Igmp Sender - GlobalRouter
================================================================================================
                                          PORT/
GRPADDR         IFINDEX    MEMBER         MLT        STATE           L2ISID
------------------------------------------------------------------------------------------------
224.5.5.5       Vlan 10    10.1.10.100    1/1        NOTFILTERED     10010
```

Table 19. VSP 4902 IGMP validation

The “show ip igmp sender” command will show the results that on port 1/1 the camera is sending on group address 224.6.6.6

```
4902:1#show ip igmp sender
                          Igmp Sender - GlobalRouter
================================================================================================
========
                                          PORT/
GRPADDR         IFINDEX    MEMBER         MLT        STATE           L2ISID
------------------------------------------------------------------------------------------------
---------------
224.6.6.6       Vlan 20    10.1.20.100    1/1        NOTFILTERED     10020
```

Table 20. VSP Core IGMP Validations

Note

Within the core vIST cluster you will notice that the port number is identified as the MLT/LAG number.

```
8401:1#show ip igmp sender
                          Igmp Sender - GlobalRouter
================================================================================================
========
                                          PORT/
GRPADDR         IFINDEX    MEMBER         MLT        STATE           L2ISID
------------------------------------------------------------------------------------------------
---------------
224.7.7.7       Vlan 192   192.168.2.99   MLT-9      NOTFILTERED     10192

1 out of 1 entries displayed
```

```
8402:1#show ip igmp sender
                          Igmp Sender - GlobalRouter
================================================================================================
                                          PORT/
GRPADDR         IFINDEX    MEMBER         MLT        STATE           L2ISID
```

```
-------------------------------------------------------------------------------------------
224.7.7.7       Vlan 192   192.168.2.99    MLT-9      NOTFILTERED     10192

1 out of 1 entries displayed
```

Validate IGMP Group Joins

On the third VSP edge switch 4451-edge-03, all three viewing stations have requested to join the three IGMP multicast steams that are being sent by VSP 4901, VSP 4902 and the two VSP vIST core switches.

The following two IGMP commands will validate that on VSP 4451 multicast status is active. VLAN 30 IP address is the querier address and we are seeing active joins.

Table 21. Validate IGMP Groups for VSP 4451-03

```
4451:1#show ip igmp interface
                          Igmp Interface - GlobalRouter
=============================================================================================
========
       QUERY              OPER            QUERY   WRONG              LASTMEM
IF     INTVL STATUS VERS. VERS QUERIER    MAXRSPT QUERY JOINS ROBUST QUERY   MODE
L2ISID
---------------------------------------------------------------------------------------------
---------------
V30    125   active 2     2    10.1.30.1  100     0     402   2      10      routed-spb
10030
V4051  125   inact  2     2    0.0.0.0    100     0     0     2      10                0
V4052  125   inact  2     2    0.0.0.0    100     0     0     2      10                0

3 out of 3 entries displayed
```

The following table will show that the three viewing stations on ports 1, 7 and 9 have requested the three IGMP streams. The viewing stations are identified by their IP address and the group address they have joined.

Table 22. Validate IGMP group joins.

```
4451:1#show ip igmp group
Igmp Group - GlobalRouter
=============================================================================================
========
GRPADDR         INPORT          MEMBER          EXPIRATION TYPE       L2ISID
---------------------------------------------------------------------------------------------
---------------
224.5.5.5       V30-1/1         10.1.30.102     194        Dynamic    10030
224.6.6.6       V30-1/7         10.1.30.101     186        Dynamic    10030
224.7.7.7       V30-1/9         10.1.30.100     185        Dynamic    10030

3 out of 3 group Receivers displayed
```

Supplementary Validation and Troubleshooting Commands

The following series of commands can be used to view statistics, status, settings, and state of the SPBm network and services.

Table 23. SPBm validation commands

```
show isis
show isis adjacencies
show isis interfaces
show isis spbm
show isis spbm nicknames
show isis spbm lsdb
show isis spbm i-sid all
show vlan i-sid
show virtual-ist
show cfm cmac
show cfm spbm
```

Table 24. L2 ping and traceroute commands.

```
l2 ping vlan 4051 routernodename <destination router name>
l2 ping vlan 4052 routernodename <destination router name>
l2 traceroute vlan 4051 routernodename <destination router name>
l2 traceroute vlan 4052 routernodename <destination router name>
```

Table 25. Advanced multicast validation

```
show isis spbm ip-multicast-route all
show isis spbm ip-multicast-route vlan <vlan ID>
show isis spbm ip-multicast-route vsn-isid <i-sid
l2 tracemroute source <source address> group <group address> vlan <C-VLAN id>
```

Table 26. IP routing and VRRP validation commands

```
show ip route
show ip vrrp interface
show ip vrrp interface vlan
Show ip vrrp address
show ip vrrp statistics
show vlan remote-mac <vlan#>
```

Terms and Conditions of Use

For additional information refer to: http://www.extremenetworks.com/company/legal/terms/