Virtual Switching Extension (VSX)
- für Profis

2020-06-02 Percy Jahn <percy.jahn@hpe.com>
Virtual Switching Extension (VSX)

Agenda

1. Introduction
2. Active Forwarding
3. Layer 3 upstream options
4. Layer 2 upstream options
5. VSX upstream
6. VSX Peer startup
7. Best Practice examples
Introduction
Introduction
Aruba OS Configuration Guides / Webinars

ArubaOS-CX 10.04 Virtual Switching Extension (VSX) Guide
6400, 8320, 8325, 8400 Switch Series

<table>
<thead>
<tr>
<th>Art</th>
<th>Webinar-Name</th>
<th>Datum</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Practice</td>
<td>VSX für Profis</td>
<td>02.06.2020</td>
<td>zur Anmeldung</td>
</tr>
<tr>
<td>Best Practice</td>
<td>VSX Grundlagen</td>
<td>19.05.2020</td>
<td>zur Anmeldung</td>
</tr>
</tbody>
</table>
VSX LAG and upstream routing

Diversity of constraints

- Single VRF / Multiple VRFs
- L2 or L3 links with upstream core nodes?
- Static, OSPF point-to-point, OSPF broadcast, BGP?
- Sizing / limitations
- Best practice for high-availability

In all scenarios, **both VSX switches run independent control planes** (separate OSPF/BGP processes) and present themselves as different routers with their own Router_IDs in the network.

In the **data path**, they function as a single router and support **active-active forwarding**.
When thinking about upstreams design, you’ve to imagine an equivalent diagram:
Some Definitions
SVI / ROP

- **ROP**
  - A **Routed Only Port** is a physical port on a switch that processes all Layer 3 functions for packets to or from the said port without any binding to VLAN processing.

- **SVI**
  - A **Switched Virtual Interface** (SVI) is a logical Layer 3 interface configured per VLAN (one-to-one mapping) that performs all Layer 3 processing for packets to or from all switch ports associated with that VLAN.

- **Transit VLAN**
  - An dedicated interconnection VLAN used to transport a VRF over an associated (attached) SVI
VSX Active-Forwarding
VSX Active-Forwarding
Example Topology
VSX Active-Forwarding
Example Topology – Traffic from Core to Access

Two NextHops (LACP)
Two paths

One NextHop

Core Layer

Access SW1

Access SW2

AOS-CX Agg-1

AOS-CX Agg-2

Core-1

Aggregation VSX pair

Two Paths!
50 % traffic on ISL!
**VSX Active-Forwarding**

Example Topology – Traffic from Core to Access

Four Paths to two MACs.
50 % traffic ends up on ISL!
VSX Active-Forwarding
Example Topology – Aggregation switch failure

Two NextHops (ECMP)

Two Paths to two NextHops (i.e. MACs).
50 % traffic loss till routing update renders AGG-1 dead!
VSX Active-Forwarding
Solution Description

### Active-Active Layer 3 Gateway
- Each VSX Node configures VSX peer MAC additionally
  - Even in case of peer failure
- L3 processing is done for both MACs
- Generated traffic always sourced by own MACs
- Active-Forwarding configured on upstream SVIs
- Icmp redirect must be disabled on Active-Forwarding interfaces
- Active-Forwarding and Active-Gateway are mutually exclusive
- TTL count is decreased by 1 (routing), except the destination IP address belongs to peer (important to maintain routing protocol connectivity)
Upstream routing to Core
With VSX Active-Forwarding

- No data traffic over ISL in nominal case.
- Each VSX node configures its VSX peer MAC as its own MAC.
- 8400-2 will process L3 function for the received packet as the DMAC is equal the its VSX peer MAC.
Layer 3 Upstream Options
Basic VSX Layer 3 Upstream options
Layer 3 Upstream Options
Assumptions

– Core Switches have to be independent
  – Reliability
  – Scaling
– Routing between Core Switches is available / established
– Downstream Switches / Devices have to be dual-attached.
– BGP and OSPF differ heavily and may impact design
Layer 3 upstream
Routed upstream port for single VRF routing model

2 routed ports on VSX cluster
Layer 3 upstream
Routed upstream port for single VRF routing model

2 routed ports on VSX cluster

- Benefits:
  - Only two lines needed
  - Simple design

- Drawbacks:
  - AOS-CX 10.4 does not support sub-interfaces for routed ports
  - Link failure leads to L3 failure
    - expensive route recalculation

- Recommendation, use this if:
  - only two lines are available
  - a single VRF is sufficient
Layer 3 upstream
Routed upstream port for single VRF routing model

4 routed ports on VSX cluster
Layer 3 upstream
Routed upstream port for single VRF routing model

4 routed ports on VSX cluster

- Benefits:
  - Optimal Load Balancing
  - Very resilient

- Drawbacks:
  - Complex Design
  - At last four lines needed
  - AOS-CX 10.4 does not support sub-interfaced for routed ports
  - Link failure leads to L3 failure
    - expensive route recalculation

- Recommendation, use this if:
  - at least 4 links are available
  - a single VRF is sufficient
Layer 3 upstream
Routed upstream port for single VRF routing model

2 routed aggregations on VSX cluster
Layer 3 upstream
Routed upstream port for single VRF routing model

2 routed aggregations on VSX cluster

- Benefits:
  - Simple design
  - Optimal Load Balancing
  - Link failure covered by LACP
    - Quick recalculation

- Drawbacks:
  - AOS-CX 10.4 does not support routed aggregations
  - Next Hop is hidden by LACP

- Recommendation, use this when:
  - Never (you can't use it with AOS-CX 10.4)
Layer 2 Upstream Options
Basic VSX Upstream options
Layer 2 Upstream Options
Assumptions

– Core Switches have to be independent
  – Reliability
  – Scaling

– Routing between Core Switches is available / established

– Downstream Switches / Devices have to be dual-attached.

– BGP and OSPF differ heavily and may impact design
Layer 2 upstream
L2 upstream for multiple VRFs

One transfer network
Layer 2 upstream
L2 upstream for multiple VRFs

One transfer networks

- **Benefits:**
  - Only two lines needed
  - Simple design

- **Drawbacks:**
  - Link failure leads to L3 failure
    - expensive route recalculation

- **Recommendation, use this if:**
  - Never (use two transfer networks instead)
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks – single peer
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks – single peer

- Benefits:
  - Only two lines needed
  - Simple design

- Drawbacks:
  - Link failure leads to L3 failure
    - expensive route recalculation

- Recommendation, use this if:
  - only two lines are available
  - multiple VRFs are needed
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks – dual peer
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks – dual peer

- Benefits:
  - Only two lines needed
  - Simple design

- Drawbacks:
  - Link failure leads to L3 failure
    - expensive route recalculation
  - L3 nexthop is hidden by routing protocol

- Recommendation, use this if:
  - Never (use two transfer networks – single peer instead)
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks

Access SW1
AOS-CX Agg-1
6400 / 8320 / 8325 / 8400

AOS-CX Core-1
6400 / 8320 / 8325 / 8400

AOS-CX Core-2
6400 / 8320 / 8325 / 8400

Access SW2

Core Layer

Aggregation VSX pair

AOS-CX Agg-1
6400 / 8320 / 8325 / 8400

AOS-CX Agg-2
6400 / 8320 / 8325 / 8400

VLAN A

VLAN B

VSX

ISL

Core-1

Core-2

AOS-CX Agg-1

AOS-CX Agg-2

#ArubaAirheads
Layer 2 upstream
L2 upstream for multiple VRFs

Two transfer networks

- **Benefits:**
  - Simple design
  - At least four lines needed

- **Drawbacks:**
  - Aggregation might be used as transfer

- **Recommendation, use this if:**
  - Never
Layer 2 upstream
L2 upstream for multiple VRFs

LACP - single transfer network
Layer 2 upstream
L2 upstream for multiple VRFs

LACP - single transfer network

- Benefits:
  - Simple design
  - At least 4 lines needed
  - Link-Failure is handled by LACP
    - Quick failover

- Drawbacks:
  - Routing Protocol hides next-hop distance
  - Aggregation may be used as transfer network

- Recommendation, use this if:
  - Core is active / passive (e.g. firewall)
  - Active-Forwarding should be enabled
Layer 2 upstream
L2 upstream for multiple VRFs

LACP – two transfer networks – dual peer
## Layer 2 upstream
L2 upstream for multiple VRFs

### LACP – two transfer networks – dual peer

- **Benefits:**
  - Simple design
  - At least 4 lines needed
  - Link-Failure is handled by LACP
    - Quick failover

- **Drawbacks:**
  - Routing Protocol hides next-hop distance

- **Recommendation, use this if:**
  - Active-Forwarding is enabled
  - more than one VRF is needed
  - At least four uplinks are available
Layer 2 upstream
OSPF Options for multiple VRFs comparison

OSPF point-to-point

ECMP

10.3.1.0/24 Agg1-IP VLAN131
10.3.1.0/24 Agg2-IP VLAN133

LAG

VRF3 Transit VLAN 133
VRF2 Transit VLAN 123
VRF3 Transit VLAN 131
VRF2 Transit VLAN 121
VRF1 Transit VLAN 112

OSPF broadcast

ECMP + VSX LAG

10.3.1.0/24 Agg1-IP VLAN131
10.3.1.0/24 Agg2-IP VLAN133

LAG

VRF3 Transit VLAN 133
VRF2 Transit VLAN 123
VRF3 Transit VLAN 131
VRF2 Transit VLAN 121
VRF1 Transit VLAN 112

3 VRFs: 15 SVIs and associated OSPF peering

Recommended

3 VRFs: only 6 SVIs and associated OSPF peering
VSX Upstream
Solution Details
VSX Upstream

Use case summary

- Optimize Network design
  - Number of VRFs
  - L3 Routing calculations
- L2 only aggregation Layer
- LACP on Core required (e.g. Servers connected to core)
- Reduced number of fibers and fast failover required
  - Square topology, LACP

- Recommendation:
  - Use standalone L3 cores
VSX in the Core Layer
Reduced number of fibers and routing impact

Core nodes with VSX
• Fast – No convergence

Legacy Core nodes
• Routing convergence

route NH is unchanged
VSX active-forwarding

new route has to be set in FIB
VSX peer startup
Initial Synchronization and Linkup delay
VSX peer startup
Initial synchronization – Linkup Delay

Synchronisation and Linkup Delay

- VSX device is booted or rebooted. MAC, ARP, Routes are empty.

- Initial Sync Phase
  - VSX peer sends state DB entries (e.g. LACP, MAC, ARP, STP, …)
  - Dynamic in time …

- Linkup Delay Phase
  - Installing entries to ASIC
  - Establish adjacencies with routers
  - Reboot: Linkup Delay defaults to 180s, but timer is adjusted to network size.
  - Boot: Linkup Delay is 0

- VSX LAGs get activated
VSX peer startup
Linkup Delay issues

Linkup Delay issues
– In Linkup Delay Phase route adjacencies get established
– Upstream LAGs has to be excluded from linkup-delay

Isolated Layer 3 vsxds
– LACP states, MAC, ARP/ND, STP, route state
Linkup Optimization
Initial Sync and Linkup Delay

- **Until 10.2:**
  The Initial Sync timer is not configurable, for LACP/MAC/ARP/STP bulk sync completion at DB level. The linkup-delay timer (default 180s, user configurable) is used for ARP/MAC program at HW level.

- **In 10.3:**
  The Initial Sync timer is fully dynamic, using a bailout-timer value for LACP/MAC/ARP/STP and route_state sync completion at DB level and having auto notification to finish this bailout-timer. The linkup-delay timer (default 180s, user configurable) is still used for ARP/MAC program at HW level.

- **In 10.4:**
  There is an auto-notification mechanism for DB and HW sync completion: the bailout and linkup-delay timer are auto handled:
  - If the ASIC hardware programming completes within the linkup-delay timer expiry, then the links are brought up immediately by the auto-handling mechanism.
  - If the ASIC hardware programming is not completed and the linkup delay timer expires, VSX daemon will go ahead and bring up the VSX LAGs.

**Benefits:**
- For smaller scale, it would avoid long linkup delays.
- Linkup delay is now considered as upper time limit for the ASIC programming and it is recommended to configure the linkup-delay timer to the maximum value (as programming completion is expected sooner).
L3 Upstream Example
Aggregation VSX with single VRF routing model
**Access Configuration**

### ACC-1 (AOS-S)

- **hostname** "ACC-1"
- **jumbo** max-frame-size 9122

<table>
<thead>
<tr>
<th>LAG to AGG</th>
<th>VLANs and endpoints I/F</th>
</tr>
</thead>
<tbody>
<tr>
<td>trunk 49-50 Trk1 lacp</td>
<td>spanning-tree (enhanced loop-protect)</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>spanning-tree bpdu-protection-timeout 3600</td>
</tr>
<tr>
<td>spanning-tree Trk1 loop-guard</td>
<td>spanning-tree 1 tcn-guard bpdu-protection</td>
</tr>
<tr>
<td>spanning-tree 1 admin-edge-port</td>
<td>spanning-tree 2 admin-edge-port</td>
</tr>
<tr>
<td>spanning-tree 2 tcn-guard bpdu-protection</td>
<td>spanning-tree 48 admin-edge-port</td>
</tr>
<tr>
<td>loop-protect 1-48</td>
<td>spanning-tree 48 tcn-guard bpdu-protection</td>
</tr>
<tr>
<td>loop-protect disable-timer 3600</td>
<td>loop-protect disable-timer 3600</td>
</tr>
</tbody>
</table>

- **vlan 1**
  - name "DEFAULT_VLAN"
  - no untagged Trk1
  - untagged 1-48, 51-52
  - no ip address
  - exit

- **vlan 10**
  - name "VLAN10"
  - tagged 1, Trk1
  - no ip address
  - jumbo
  - exit

- **vlan 20**
  - name "VLAN20"
  - tagged 5, Trk1
  - no ip address
  - jumbo
  - exit

### ACC-2 (AOS-CX)

- **hostname** ACC-2
- **loop-protect** re-enable-timer 3600

<table>
<thead>
<tr>
<th>LAG to AGG</th>
<th>VLANs</th>
<th>Loop-protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>loop-protect 2</td>
<td>spanning-tree</td>
<td>spanning-tree (enhanced loop-protect)</td>
</tr>
<tr>
<td>vlan 1, 10, 20</td>
<td>spanning-tree</td>
<td>spanning-tree</td>
</tr>
<tr>
<td>interface lag 1</td>
<td>loop-protect</td>
<td>spanning-tree</td>
</tr>
<tr>
<td>no shutdown</td>
<td>description UPLINK to AGG</td>
<td>spanning-tree</td>
</tr>
<tr>
<td>no routing</td>
<td>no routing</td>
<td>spanning-tree</td>
</tr>
<tr>
<td>vlan trunk native 1</td>
<td>vlan trunk allowed 10, 20</td>
<td>spanning-tree</td>
</tr>
<tr>
<td>lacp mode active</td>
<td>spanning-tree loop-guard</td>
<td>loop-protect</td>
</tr>
</tbody>
</table>

- **interface 1/1/1**
  - no shutdown
  - mtu 9000
  - description Endpoint1
  - no routing
  - vlan access 10
  - spanning-tree bpdu-guard
  - spanning-tree port-type admin-edge
  - spanning-tree tcn-guard
  - loop-protect

- **interface 1/1/49**
  - no shutdown
  - mtu 9100
  - lag 1

- **interface 1/1/50**
  - no shutdown
  - mtu 9100
  - lag 1

---

*Source: ArubaAirheads*
# Aggregation Configuration (part1)

### AGG-1

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname AGG-1</code></td>
<td></td>
</tr>
<tr>
<td><code>no ip icmp redirect</code></td>
<td>Disable ICMP redirect</td>
</tr>
<tr>
<td><code>vrf KA</code></td>
<td>Dedicated KA VRF</td>
</tr>
<tr>
<td><code>router ospf 1</code></td>
<td>OSPF config</td>
</tr>
<tr>
<td><code>router-id 10.0.1.1</code></td>
<td></td>
</tr>
<tr>
<td><code>max-metric router-lsa on-startup</code></td>
<td></td>
</tr>
<tr>
<td><code>passive-interface default</code></td>
<td></td>
</tr>
<tr>
<td><code>graceful-restart restart-interval 300</code></td>
<td></td>
</tr>
<tr>
<td><code>trap-enable</code></td>
<td></td>
</tr>
<tr>
<td><code>area 0.0.0.0</code></td>
<td></td>
</tr>
<tr>
<td><code>access-list ip IOT-1</code></td>
<td>ACL</td>
</tr>
<tr>
<td><code>vsx-sync</code></td>
<td></td>
</tr>
<tr>
<td><code>5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080</code></td>
<td>vsx-sync</td>
</tr>
<tr>
<td><code>10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0</code></td>
<td>1</td>
</tr>
<tr>
<td><code>1000 permit any any</code></td>
<td>5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080</td>
</tr>
<tr>
<td><code>vlan 1</code></td>
<td>10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0</td>
</tr>
<tr>
<td><code>vlan 2</code></td>
<td>1000 permit any any</td>
</tr>
<tr>
<td><code>vlan 10</code></td>
<td><code>description TRANSIT VLAN</code></td>
</tr>
<tr>
<td><code>vlan 20</code></td>
<td><code>vsx-sync</code></td>
</tr>
<tr>
<td><code>vlan 21</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 22</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 23</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 24</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 25</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 30</code></td>
<td></td>
</tr>
<tr>
<td><code>vsx-sync</code></td>
<td></td>
</tr>
</tbody>
</table>

### AGG-2

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname AGG-2</code></td>
<td></td>
</tr>
<tr>
<td><code>no ip icmp redirect</code></td>
<td></td>
</tr>
<tr>
<td><code>vrf KA</code></td>
<td></td>
</tr>
<tr>
<td><code>router ospf 1</code></td>
<td></td>
</tr>
<tr>
<td><code>router-id 10.0.1.2</code></td>
<td></td>
</tr>
<tr>
<td><code>max-metric router-lsa on-startup</code></td>
<td></td>
</tr>
<tr>
<td><code>passive-interface default</code></td>
<td></td>
</tr>
<tr>
<td><code>graceful-restart restart-interval 300</code></td>
<td></td>
</tr>
<tr>
<td><code>trap-enable</code></td>
<td></td>
</tr>
<tr>
<td><code>area 0.0.0.0</code></td>
<td></td>
</tr>
<tr>
<td><code>access-list ip IOT-1</code></td>
<td></td>
</tr>
<tr>
<td><code>vsx-sync</code></td>
<td></td>
</tr>
<tr>
<td><code>5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080</code></td>
<td>vsx-sync</td>
</tr>
<tr>
<td><code>10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0</code></td>
<td>1</td>
</tr>
<tr>
<td><code>1000 permit any any</code></td>
<td>5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080</td>
</tr>
<tr>
<td><code>vlan 1</code></td>
<td>10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0</td>
</tr>
<tr>
<td><code>vlan 2</code></td>
<td>1000 permit any any</td>
</tr>
<tr>
<td><code>vlan 10</code></td>
<td><code>description TRANSIT VLAN</code></td>
</tr>
<tr>
<td><code>vlan 20</code></td>
<td><code>vsx-sync</code></td>
</tr>
<tr>
<td><code>vlan 21</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 22</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 23</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 24</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 25</code></td>
<td></td>
</tr>
<tr>
<td><code>vlan 30</code></td>
<td></td>
</tr>
<tr>
<td><code>vsx-sync</code></td>
<td></td>
</tr>
</tbody>
</table>

## Aggregation Configuration (part2)

### AGG-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag 1</td>
<td>Access-Switch-1 VSX LAG</td>
</tr>
<tr>
<td></td>
<td>ISL LAG</td>
</tr>
<tr>
<td></td>
<td>I/F in VSX LAG</td>
</tr>
</tbody>
</table>

- spanning-tree priority 4
- spanning-tree trap topology-change instance 0
- qos trust dscp
- interface lag 1 multi-chassis
  - no shutdown
  - description Access-Switch-1 VSX LAG
  - no routing
  - vlan trunk native 1
  - vlan trunk allowed 10,20-30
  - lacp mode active
  - spanning-tree root-guard
  - apply access-list ip IOT-1 in

### AGG-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag 256</td>
<td>ISL LAG</td>
</tr>
<tr>
<td></td>
<td>I/F for VSX keepalive</td>
</tr>
</tbody>
</table>

- spanning-tree priority 4
- spanning-tree trap topology-change instance 0
- qos trust dscp
- interface lag 1 multi-chassis
  - no shutdown
  - description Access-Switch-1 VSX LAG
  - no routing
  - vlan trunk native 1
  - vlan trunk allowed 10,20-30
  - lacp mode active
  - spanning-tree root-guard
  - apply access-list ip IOT-1 in

- interface lag 256
  - no shutdown
  - description ISL link
  - no routing
  - vlan trunk native 1 tag
  - vlan trunk allowed all
  - lacp mode active

- interface 1/1/1
  - no shutdown
  - mtu 9100
  - description ACC-1
  - lag 1

- interface 1/1/48
  - no shutdown
  - vrf attach KA
  - description VSX keepalive
  - ip address 192.168.0.0/31

To reduce configuration length, only one VSX LAG (to Acc-1) is shown.
### Aggregation Configuration (part3)

#### AGG-1

<table>
<thead>
<tr>
<th>Interface 1/1/49</th>
<th>Description</th>
<th>IP Address</th>
<th>OSPF Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>Core-1 1/1/1</td>
<td>10.0.0.1/31</td>
<td>no passive, cost 1000, network point-to-point, message-digest, key 1 md5 ciphertext</td>
</tr>
</tbody>
</table>

#### AGG-2

<table>
<thead>
<tr>
<th>Interface 1/1/49</th>
<th>Description</th>
<th>IP Address</th>
<th>OSPF Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>Core-1 1/1/2</td>
<td>10.0.0.5/31</td>
<td>no passive, cost 1000, network point-to-point, message-digest, key 1 md5 ciphertext</td>
</tr>
</tbody>
</table>

#### Routed Uplinks

<table>
<thead>
<tr>
<th>Interface 1/1/50</th>
<th>Description</th>
<th>IP Address</th>
<th>OSPF Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>Core-2 1/1/1</td>
<td>10.0.0.3/31</td>
<td>no passive, cost 1000, network point-to-point, message-digest, key 1 md5 ciphertext</td>
</tr>
</tbody>
</table>

#### I/F in ISL LAG

<table>
<thead>
<tr>
<th>Interface 1/1/55</th>
<th>Description</th>
<th>Lag</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>ISL physical link</td>
<td>256</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface 1/1/56</th>
<th>Description</th>
<th>Lag</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>ISL physical link</td>
<td>256</td>
</tr>
</tbody>
</table>

#### Loopback

<table>
<thead>
<tr>
<th>Interface loopback 0</th>
<th>IP Address</th>
<th>OSPF Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address 10.0.1.1/32</td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>ip ospf 1 area 0.0.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#ArubaAirheads
## Aggregation Configuration (part4)

### AGG-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| vlan2     | interface vlan2  
          |   ip mtu 1500  
          |   ip address 10.0.3.1/30  
          |   ip ospf 1 area 0.0.0.0  
          |   no ip ospf passive  
          |   ip ospf cost 50  
          |   ip ospf network point-to-point  
          |   ip ospf authentication message-digest  
          |   ip ospf message-digest-key 1 md5 ciphertext A...X |
| vlan10    | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.2.10.2/24  
          |   ip address 10.2.10.2/24 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.2.10.1  
          |   ip helper-address 10.99.10.9  
          |   ip ospf 1 area 0.0.0.0  
| vlan20    | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.2.20.2/24  
          |   ip address 10.2.20.2/24 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.2.20.1  
|          | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.1.20.1/30  
          |   ip address 10.1.20.1/30 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.1.20.1  
|          | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.1.20.1/30  
          |   ip address 10.1.20.1/30 secondary  

### AGG-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| vlan2     | interface vlan2  
          |   ip mtu 1500  
          |   ip address 10.0.3.1/30  
          |   ip ospf 1 area 0.0.0.0  
          |   no ip ospf passive  
          |   ip ospf cost 50  
          |   ip ospf network point-to-point  
          |   ip ospf authentication message-digest  
          |   ip ospf message-digest-key 1 md5 ciphertext A...X |
| vlan10    | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.2.10.2/24  
          |   ip address 10.2.10.2/24 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.2.10.1  
          |   ip helper-address 10.99.10.9  
          |   ip ospf 1 area 0.0.0.0  
| vlan20    | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.2.20.2/24  
          |   ip address 10.2.20.2/24 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.2.20.1  
|          | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.1.20.1/30  
          |   ip address 10.1.20.1/30 secondary  
          |   active-gateway ip mac 12:01:00:00:01:00  
          |   active-gateway ip 10.1.20.1  
|          | vsx-sync active-gateways  
          |   ip mtu 1000  
          |   ip address 10.1.20.1/30  
          |   ip address 10.1.20.1/30 secondary  

### Transit VLAN

- interface vlan2
- ip mtu 9198
- ip address 10.0.2.1/30
- ip ospf 1 area 0.0.0.0
- no ip ospf passive
- ip ospf cost 50
- ip ospf network point-to-point
- ip ospf authentication message-digest
- ip ospf message-digest-key 1 md5 ciphertext A...X

### Endpoints SVIs (inc. secondary)

- interface vlan10
  - vsx-sync active-gateways
  - ip mtu 9100
  - ip address 10.1.10.2/24
  - ip address 10.2.10.2/24 secondary
  - active-gateway ip mac 12:01:00:00:01:00
  - active-gateway ip 10.1.10.1
  - ip helper-address 10.99.10.9
  - ip ospf 1 area 0.0.0.0

- interface vlan20
  - vsx-sync active-gateways
  - ip mtu 9100
  - ip address 10.1.20.2/24
  - ip address 10.2.20.2/24 secondary
  - active-gateway ip mac 12:01:00:00:01:00
  - active-gateway ip 10.1.20.1

### VSX

- system-mac 02:01:00:00:01:00
- inter-switch-link lag 256
- role primary
- keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA
- vsx-sync aaa acl-log-timer bfd-global bgp copp-policy dhcp-relay server dhcp-snooping dns icmp-tcp lldp loop-protect-global mac-lockout mclag-interfaces neighbor ospf qos-global route-map sflow-global snmp stp-global time vsx-global
Core Configuration (part1)

**CORE-1**

hostname CORE-1

router ospf 1
   router-id 10.0.1.3
   max-metric router-lsa on-startup
   passive-interface default
   default-information originate always
   graceful-restart restart-interval 300
   trap-enable
   area 0.0.0.0

interface loopback 0
   ip address 10.0.1.3/32
   ip ospf 1 area 0.0.0.0

**CORE-2**

hostname CORE-2

router ospf 1
   router-id 10.0.1.4
   max-metric router-lsa on-startup
   passive-interface default
   default-information originate always
   graceful-restart restart-interval 300
   trap-enable
   area 0.0.0.0

interface loopback 0
   ip address 10.0.1.4/32
   ip ospf 1 area 0.0.0.0
## Core Configuration (part2)

### CORE-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| 1/1/1     | no shutdown  
mtu 9198  
ip address 10.0.0.0/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf cost 1000  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |
| 1/1/2     | no shutdown  
mtu 9198  
ip address 10.0.0.4/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |
| 1/1/3     | no shutdown  
mtu 9198  
ip address 10.0.0.252/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |

### CORE-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| 1/1/1     | no shutdown  
mtu 9198  
ip address 10.0.0.2/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf cost 1000  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |
| 1/1/2     | no shutdown  
mtu 9198  
ip address 10.0.0.6/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf cost 1000  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |
| 1/1/3     | no shutdown  
mtu 9198  
ip address 10.0.0.253/31  
ip ospf 1 area 0.0.0.0  
no ip ospf passive  
ip ospf cost 1000  
ip ospf network point-to-point  
ip ospf authentication message-digest  
ip ospf message-digest-key 1 md5 ciphertext A.X |
L2 Upstream Example
Aggregation VSX with multiple VRF routing model
Aggregation Configuration (part1)

**AGG-1**

- `hostname AGG-1`
- `no ip icmp redirect`
- `vrf KA`
- `vrf VRF1`
- `vrf VRF2`
- `router ospf 1 vrf VRF1`
  - `router-id 10.0.1.1`
  - `max-metric router-lsa on-startup`
  - `passive-interface default`
  - `graceful-restart restart-interval 300`
  - `trap-enable`
  - `area 0.0.0.0`
- `access-list ip IOT-1`
  - `vsx-sync`
  - `5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080`
  - `10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0`
  - `1000 permit any any`
- `vlan 1`
- `vlan 10`
- `vlan 10 vss-sync`
- `vlan 20`
- `vlan 30`

**AGG-2**

- `hostname AGG-2`
- `no ip icmp redirect`
- `vrf KA`
- `vrf VRF1`
- `vrf VRF2`
- `router ospf 1 vrf VRF1`
  - `router-id 10.0.1.2`
  - `max-metric router-lsa on-startup`
  - `passive-interface default`
  - `graceful-restart restart-interval 300`
  - `trap-enable`
  - `area 0.0.0.0`
- `access-list ip IOT-1`
  - `vsx-sync`
  - `5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080`
  - `10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0`
  - `1000 permit any any`
- `vlan 1`
- `vlan 10`
- `vlan 10 vss-sync`
- `vlan 20`
- `vlan 30`

---

To reduce configuration length, only VRF1 and VRF2 are exposed.

**OSPF config VRF1**

- `router ospf 1 vrf VRF1`
  - `max-metric router-lsa on-startup`
  - `passive-interface default`
  - `graceful-restart restart-interval 300`
  - `trap-enable`
  - `area 0.0.0.0`

**OSPF config VRF2**

- `router ospf 1 vrf VRF2`
  - `max-metric router-lsa on-startup`
  - `passive-interface default`
  - `graceful-restart restart-interval 300`
  - `trap-enable`
  - `area 0.0.0.0`

**ACL**

- `access-list ip IOT-1`
  - `vsx-sync`
  - `5 permit tcp 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0 eq 1080`
  - `10 deny any 10.1.0.0/255.255.0.0 10.99.1.0/255.255.255.0`
  - `1000 permit any any`

**Endpoint VLANs**

- `vlan 1`
- `vlan 10 vss-sync`
- `vlan 20 vss-sync`
- `vlan 30 vss-sync`
## Aggregation Configuration (part2)

### AGG-1

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
<th>VSX-Sync</th>
<th>VLAN</th>
<th>Description</th>
<th>VSX-Sync</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>TRANSLIT VLAN VRF1-CORE1</td>
<td></td>
<td>102</td>
<td>TRANSLIT VLAN VRF1-CORE2</td>
<td></td>
</tr>
<tr>
<td>201</td>
<td>TRANSLIT VLAN VRF2-CORE1</td>
<td></td>
<td>202</td>
<td>TRANSLIT VLAN VRF2-CORE2</td>
<td></td>
</tr>
</tbody>
</table>

- **Spanning-Tree**
  - Spanning-tree priority 4
  - Spanning-tree trap topology-change instance 0

- **QoS Trust**
  - QoS trust dscp

- **Downstream VSX LAGs**
  - Interface lag 1 multi-chassis
    - No shutdown
    - Description Access-Switch-1 VSX LAG
  - No routing
  - VLAN trunk native 1
  - VLAN trunk allowed 10,20-30
  - LACP mode active
  - Spanning-tree root-guard
  - Apply access-list ip IOT-1 in

- **Interface lag 2 multi-chassis**
  - No shutdown
  - Description Access-Switch-2 VSX LAG
  - No routing
  - VLAN trunk native 1
  - VLAN trunk allowed 10,20-30
  - LACP mode active
  - Spanning-tree root-guard
  - Apply access-list ip IOT-1 in

### AGG-2

- **Transit VLANs**
  - VLAN 101
  - Description TRANSLIT VLAN VRF1-CORE1
  - VLAN 102
  - Description TRANSLIT VLAN VRF1-CORE2
  - VLAN 201
  - Description TRANSLIT VLAN VRF2-CORE1
  - VLAN 202
  - Description TRANSLIT VLAN VRF2-CORE2

- **Spanning-Tree**
  - Spanning-tree priority 4
  - Spanning-tree trap topology-change instance 0

- **QoS Trust**
  - QoS trust dscp

- **Downstream VSX LAGs**
  - Interface lag 1 multi-chassis
    - No shutdown
    - Description Access-Switch-1 VSX LAG
  - No routing
  - VLAN trunk native 1
  - VLAN trunk allowed 10,20-30
  - LACP mode active
  - Spanning-tree root-guard
  - Apply access-list ip IOT-1 in

- **Interface lag 2 multi-chassis**
  - No shutdown
  - Description Access-Switch-2 VSX LAG
  - No routing
  - VLAN trunk native 1
  - VLAN trunk allowed 10,20-30
  - LACP mode active
  - Spanning-tree root-guard
  - Apply access-list ip IOT-1 in
<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lag 101 multi-chassis</td>
<td>no shutdown &lt;br&gt; description CORE-1 VSX LAG &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 &lt;br&gt; vlan trunk allowed 101,201 &lt;br&gt; lacp mode active &lt;br&gt; spanning-tree bpdu-filter</td>
</tr>
<tr>
<td>Lag 102 multi-chassis</td>
<td>no shutdown &lt;br&gt; description CORE-2 VSX LAG &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 &lt;br&gt; vlan trunk allowed 102,202 &lt;br&gt; lacp mode active &lt;br&gt; spanning-tree bpdu-filter</td>
</tr>
<tr>
<td>Lag 256</td>
<td>no shutdown &lt;br&gt; description ISL link &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 tag &lt;br&gt; vlan trunk allowed all &lt;br&gt; lacp mode active</td>
</tr>
<tr>
<td>1/1/1</td>
<td>no shutdown &lt;br&gt; mtu 9100 &lt;br&gt; description ACC-1 &lt;br&gt; lag 1</td>
</tr>
<tr>
<td>1/1/2</td>
<td>no shutdown &lt;br&gt; mtu 9100 &lt;br&gt; description ACC-2 &lt;br&gt; lag 2</td>
</tr>
<tr>
<td>Lag 101 multi-chassis</td>
<td>no shutdown &lt;br&gt; description CORE-1 VSX LAG &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 &lt;br&gt; vlan trunk allowed 101,201 &lt;br&gt; lacp mode active &lt;br&gt; spanning-tree bpdu-filter</td>
</tr>
<tr>
<td>Lag 102 multi-chassis</td>
<td>no shutdown &lt;br&gt; description CORE-2 VSX LAG &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 &lt;br&gt; vlan trunk allowed 102,202 &lt;br&gt; lacp mode active &lt;br&gt; spanning-tree bpdu-filter</td>
</tr>
<tr>
<td>Lag 256</td>
<td>no shutdown &lt;br&gt; description ISL link &lt;br&gt; no routing &lt;br&gt; vlan trunk native 1 tag &lt;br&gt; vlan trunk allowed all &lt;br&gt; lacp mode active</td>
</tr>
</tbody>
</table>
# Aggregation Configuration (part 4)

## AGG-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/48</td>
<td>no shutdown&lt;br&gt;vrf attach KA&lt;br&gt;description VSX keepalive&lt;br&gt;ip address 192.168.0.0/31</td>
</tr>
<tr>
<td>1/1/49</td>
<td>no shutdown&lt;br&gt;mtu 9198&lt;br&gt;description CORE-1 1/1/1&lt;br&gt;lag 101</td>
</tr>
<tr>
<td>1/1/50</td>
<td>no shutdown&lt;br&gt;mtu 9198&lt;br&gt;description CORE-2 1/1/1&lt;br&gt;lag 102</td>
</tr>
<tr>
<td>loopback 0</td>
<td>vrf attach VRF1&lt;br&gt;ip address 10.0.0.1/32&lt;br&gt;ip ospf 1 area 0.0.0.0</td>
</tr>
</tbody>
</table>

## AGG-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/48</td>
<td>no shutdown&lt;br&gt;vrf attach KA&lt;br&gt;description VSX keepalive&lt;br&gt;ip address 192.168.0.0/31</td>
</tr>
<tr>
<td>1/1/49</td>
<td>no shutdown&lt;br&gt;mtu 9198&lt;br&gt;description CORE-1 1/1/1&lt;br&gt;lag 101</td>
</tr>
<tr>
<td>1/1/50</td>
<td>no shutdown&lt;br&gt;mtu 9198&lt;br&gt;description CORE-2 1/1/1&lt;br&gt;lag 102</td>
</tr>
<tr>
<td>loopback 0</td>
<td>vrf attach VRF1&lt;br&gt;ip address 10.0.0.1/32&lt;br&gt;ip ospf 1 area 0.0.0.0</td>
</tr>
</tbody>
</table>

## Uplink

- Interface in VSX LAG
- Interface in ISL LAG

## Loopback

- Interface loopback 0
- vrf attach VRF1
- ip address 10.0.0.1/32
- ip ospf 1 area 0.0.0.0
### Aggregation Configuration (part5)

#### AGG-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| interface vlan10 | vsx-sync active-gateways  
| vrf attach VRF1  
| ip mtu 9100  
| ip address 10.1.10.2/24  
| ip address 10.2.20.2/24 secondary  
| active-gateway ip mac 12:01:00:00:01:00  
| active-gateway ip 10.1.10.1  
| active-gateway ip 10.2.10.1  
| ip helper-address 10.99.10.9  
| ip ospf 1 area 0.0.0.0 |

#### AGG-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| interface vlan10 | vsx-sync active-gateways  
| vrf attach VRF1  
| ip mtu 9100  
| ip address 10.1.20.2/24  
| ip address 10.2.20.2/24 secondary  
| active-gateway ip mac 12:01:00:00:01:00  
| active-gateway ip 10.1.20.1  
| active-gateway ip 10.2.20.1  
| ip helper-address 10.99.10.9  
| ip ospf 1 area 0.0.0.0 |

### VRF1 Endpoints SVIs (inc. secondary)

- AGG-1
- AGG-2

### VRF2 Endpoints SVIs (inc. secondary)

- AGG-1
- AGG-2
## Aggregation Configuration (part6)

### AGG-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan101</td>
<td>interface vlan101</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.101.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan102</td>
<td>interface vlan102</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.102.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan201</td>
<td>interface vlan201</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF2</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.201.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan202</td>
<td>interface vlan202</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF2</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.202.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>

### AGG-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan101</td>
<td>interface vlan101</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.101.3/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan102</td>
<td>interface vlan102</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.102.3/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan201</td>
<td>interface vlan201</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF2</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.201.3/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
<tr>
<td>vlan202</td>
<td>interface vlan202</td>
</tr>
<tr>
<td></td>
<td>vrf attach VRF2</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>vsx active-forwarding</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.202.3/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>
## Aggregation Configuration (part7)

<table>
<thead>
<tr>
<th>AGG-1</th>
<th>AGG-2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VSX</strong></td>
<td><strong>VSX</strong></td>
</tr>
<tr>
<td>system-mac 02:01:00:00:01:00</td>
<td>system-mac 02:01:00:00:01:00</td>
</tr>
<tr>
<td>inter-switch-link lag 256</td>
<td>inter-switch-link lag 256</td>
</tr>
<tr>
<td>role primary</td>
<td>role secondary</td>
</tr>
<tr>
<td>keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA</td>
<td>keepalive peer 192.168.0.0 source 192.168.0.1 vrf KA</td>
</tr>
<tr>
<td>linkup-delay-timer exclude lag 101-102</td>
<td>linkup-delay-timer exclude lag 101-102</td>
</tr>
</tbody>
</table>
### Core Configuration (part 1)

**CORE-1**

<table>
<thead>
<tr>
<th>VRF + VRF2</th>
<th><strong>OSPF config VRF1</strong></th>
<th><strong>OSPF config VRF2</strong></th>
<th><strong>Core Transit VLANs</strong></th>
<th><strong>Agg Transit VLANs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname CORE-1</td>
<td>vrf VRF1 vrf VRF2</td>
<td>router ospf 1 vrf VRF1 router-id 10.0.1.3 max-metric router-lsa on-startup passive-interface default default-information originate always graceful-restart restart-interval 300 trap-enable area 0.0.0.0</td>
<td>router ospf 1 vrf VRF1 router-id 10.0.1.4 max-metric router-lsa on-startup passive-interface default default-information originate always graceful-restart restart-interval 300 trap-enable area 0.0.0.0</td>
<td>vlan 11 description Transit CORE VRF1 vlan 12 description Transit CORE VRF2</td>
</tr>
</tbody>
</table>

**CORE-2**

<table>
<thead>
<tr>
<th><strong>VRF1 + VRF2</strong></th>
<th><strong>OSPF config VRF1</strong></th>
<th><strong>OSPF config VRF2</strong></th>
<th><strong>Core Transit VLANs</strong></th>
<th><strong>Agg Transit VLANs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname CORE-2</td>
<td>vrf VRF1 vrf VRF2</td>
<td>router ospf 1 vrf VRF1 router-id 10.0.1.3 max-metric router-lsa on-startup passive-interface default default-information originate always graceful-restart restart-interval 300 trap-enable area 0.0.0.0</td>
<td>router ospf 1 vrf VRF1 router-id 10.0.1.4 max-metric router-lsa on-startup passive-interface default default-information originate always graceful-restart restart-interval 300 trap-enable area 0.0.0.0</td>
<td>vlan 11 description Transit CORE VRF1 vlan 12 description Transit CORE VRF2</td>
</tr>
</tbody>
</table>
Core Configuration (part2)

**CORE-1**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag 1</td>
<td>no shutdown, no routing, vlan trunk native 1, vlan trunk allowed 101,201, lacp mode active</td>
</tr>
<tr>
<td>1/1/1</td>
<td>no shutdown, mtu 9198, lag 1</td>
</tr>
<tr>
<td>1/1/2</td>
<td>no shutdown, mtu 9198, lag 1</td>
</tr>
<tr>
<td>1/1/3</td>
<td>no shutdown, mtu 9198, no routing, vlan trunk native 1, vlan trunk allowed 11-12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loopback</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf attach VRF1, ip address 10.0.0.1.3/32, ip ospf 1 area 0.0.0.0</td>
</tr>
</tbody>
</table>

**CORE-2**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag 1</td>
<td>no shutdown, no routing, vlan trunk native 1, vlan trunk allowed 102,202, lacp mode active</td>
</tr>
<tr>
<td>1/1/1</td>
<td>no shutdown, mtu 9198, lag 1</td>
</tr>
<tr>
<td>1/1/2</td>
<td>no shutdown, mtu 9198, lag 1</td>
</tr>
<tr>
<td>1/1/3</td>
<td>no shutdown, mtu 9198, no routing, vlan trunk native 1, vlan trunk allowed 11-12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loopback</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf attach VRF1, ip address 10.0.0.1.4/32, ip ospf 1 area 0.0.0.0</td>
</tr>
</tbody>
</table>
## Core Configuration (part3)

### CORE-1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan11</td>
<td>vrf attach VRF1</td>
<td>vlan11</td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.11.1/29</td>
<td></td>
<td>ip address 10.0.11.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 20</td>
<td></td>
<td>ip ospf cost 20</td>
</tr>
<tr>
<td></td>
<td>ip ospf network point-to-point</td>
<td></td>
<td>ip ospf network point-to-point</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>

### CORE-2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan11</td>
<td>vrf attach VRF1</td>
<td>vlan11</td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.11.2/29</td>
<td></td>
<td>ip address 10.0.11.2/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 20</td>
<td></td>
<td>ip ospf cost 20</td>
</tr>
<tr>
<td></td>
<td>ip ospf network point-to-point</td>
<td></td>
<td>ip ospf network point-to-point</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>

### Core Transit SVIs

### AggTransit SVIs

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan101</td>
<td>vrf attach VRF1</td>
<td>vlan102</td>
<td>vrf attach VRF1</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.101.1/29</td>
<td></td>
<td>ip address 10.0.102.1/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf priority 100</td>
<td></td>
<td>ip ospf priority 100</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Configuration</th>
<th>Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan201</td>
<td>vrf attach VRF2</td>
<td>vlan202</td>
<td>vrf attach VRF2</td>
</tr>
<tr>
<td></td>
<td>ip mtu 9198</td>
<td></td>
<td>ip mtu 9198</td>
</tr>
<tr>
<td></td>
<td>ip address 10.0.201.1/29</td>
<td></td>
<td>ip address 10.0.202.1/29</td>
</tr>
<tr>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
<td></td>
<td>ip ospf 1 area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>no ip ospf passive</td>
<td></td>
<td>no ip ospf passive</td>
</tr>
<tr>
<td></td>
<td>ip ospf priority 100</td>
<td></td>
<td>ip ospf priority 100</td>
</tr>
<tr>
<td></td>
<td>ip ospf cost 50</td>
<td></td>
<td>ip ospf cost 50</td>
</tr>
<tr>
<td></td>
<td>ip ospf authentication message-digest</td>
<td></td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
<td></td>
<td>ip ospf message-digest-key 1 md5 ciphertext A...X</td>
</tr>
</tbody>
</table>
Multi-VRF Firewall Example
L2 upstream with static routing
Multi-VRFs Static routing – FW use-case
Next-Hop = each VSX nodes on the Transit SVIs

admin@PA-500> show routing route
flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
O1:ospf intra-area, O2:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2

VIRTUAL ROUTER: VRF1 (id 2)
===============
destination    nexthop metric flags    age     interface        next-AS
10.1.10.0/24 10.0.111.2 10 A S ae1.111
10.1.10.0/24 10.0.111.3 10 A S ae1.111

VIRTUAL ROUTER: VRF2 (id 3)
===============
destination    nexthop metric flags    age     interface        next-AS
10.1.20.0/24 10.0.121.2 10 A S ae1.121
10.1.20.0/24 10.0.121.3 10 A S ae1.121

No ip icmp redirect.

ip route 0.0.0.0/0 <firewall_ip_address> vrf VRF1
ip route 0.0.0.0/0 <firewall_ip_address> vrf VRF2

ECMP requirement on the Firewalls.

No ip icmp redirect.
Multi-VRFs Static routing – FW use-case
Next-Hop = Active-gateway on the Transit SVIs

Same level of High-Availability as with active-forwarding in case of a VSX node failure.

The active-gateway VIP is still UP if one of the VSX node fails.

No ECMP requirement on FW (like pfSense).

No ip icmp redirect.
Resources
Resources
Public resources

- **VSX Guide (10.4):**
  
  
  **PDF:** [https://support.hpe.com/hpsc/doc/public/display?docId=a00091706en_us](https://support.hpe.com/hpsc/doc/public/display?docId=a00091706en_us)

- **VSX Configuration Best Practices (10.4):**
  
  **PDF:** [https://support.hpe.com/hpsc/doc/public/display?docId=a00094242en_us](https://support.hpe.com/hpsc/doc/public/display?docId=a00094242en_us)

- **Release Notes:**
  
  - **10.4:**
  
  - **10.3:**
  
  - **10.2:**
Questions?
percy.jahn@hpe.com