Campus Network Design Best Practices

with ArubaOS-CX

Aruba Campus TME - June 2018
Leading Practices

- Features & Function
- Performance Optimization
- Platform Evolution
- Field Experience
Agenda

Focus Points

1. Campus Architecture
2. Aruba VSX Technology Overview
3. Routing Design & Impact
4. Loop Protection
5. Network Management
6. Miscellaneous
Campus Architectures
Aruba Mobile-First Solution Components
Wired and wireless

- Core switches : 8400 / 8320
- Aggregation switches : 8320 / 8400 or 3810 / 5400R
- Access switches : 2930F / 2930M / 3810 / 5400R
- Mobility Controllers : 7280 / 7240 / 7220 / 7210 (AppRF, WebCC, UCC, Firewall), Mobility Master
- Access Points : AP3xx, AP2xx
- Policy Mngt server : ClearPass
- NMS : Airwave (Central)
- 3rd party Firewall and IPS
Aruba Mobile-First Design
Impact on core/aggregation design

- Distributed access:
  - Wired endpoint traffic bypasses the Mobility Controller

- Centralized access using Dynamic Segmentation ("Role Based / Port Based" Tunneling technologies)
  - All wired & wireless traffic goes through Mobility Controllers
  - Core and aggregation switches are seen as underlay nodes

- Mix:
  - most user traffic going through the Mobility Controller, some exception bypassing the Mobility Controller
    (Management traffic, edge/local servers, legacy access switches during migration)
Two-Tier Campus Network
Small campus - STP
Two-Tier Campus Network
Small campus - VSX

Diagram showing a two-tier campus network with Mobility Master, Mobility Controller Cluster, Core_Agg1, Core_Agg2, Access1, Access2, and VSX LAGs. The diagram also includes FWs, ISL, L2 link, and L3 link.
Two-Tier Campus Network
Small campus - VSX
Two-Tier Campus Network
Small campus - VSX
Two-Tier Campus Network
Traditional L2/L3 Model

**Mobility Controller**
- L2

**Access Layer**
- L2

**Aggregation Layer**
- L2 + L3
- Multi VRFs

**L3 Firewall**

**Aruba Switch Proposal**
- 8320
- 2930F/M

**VSX**

**MC1**
- Mobility Controller Cluster

**MC2**
- Mobility Controller Cluster

**Core_Agg1**
- Default Gateway

**Core_Agg2**
- Default Gateway

**FWs**

**GPE**

**L2 link**

**L3 link**
Three-Tier Campus Network
When to have separated Core and Aggregation Layers?

- Number of access switches > number of ports in core switch
- Limited number of fibers between access and core (IDF required)
- Optics distance limitation between access and core (MDF)
- Off-loading L2 processes from the core for large scale
- Fault domains isolation:
  - Easier manageability
  - Better stability
  - Higher scalability: ARP, MAC, template
Three-Tier Campus Network – medium size

Traditional Topology
Three-Tier Campus Network
L2/L3 or routed access (L3 only)?

L2 access - L2/L3 aggregation

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-known design model</td>
<td>L2 Loop avoidance requirements</td>
</tr>
<tr>
<td>VSX Benefits (MCLAG to avoid Spanning Tree)</td>
<td>LACP requirement (for VSX LAG)</td>
</tr>
<tr>
<td>Large choice of access switches</td>
<td></td>
</tr>
</tbody>
</table>

L3 access - L3 aggregation

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>No L2 protocols, no Spanning Tree</td>
<td>GRE/VXLAN extra configuration for VLAN spanning</td>
</tr>
<tr>
<td>Good interoperability</td>
<td>Increase IPAM complexity (try using /31)</td>
</tr>
<tr>
<td>Well-known OSPF design Convergence Time</td>
<td>Not commonly used by operational teams</td>
</tr>
<tr>
<td>Reduced ARP table size</td>
<td>Access Platform restrictions: OSPF and potentially VRF support</td>
</tr>
</tbody>
</table>
## Campus Size

<table>
<thead>
<tr>
<th>L2/L3 Model</th>
<th>Small Campus</th>
<th>Medium Campus (multiple floors)</th>
<th>Large Campus (multiple buildings)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2-Tier architecture: collapsed Core/Aggregation layers.</td>
<td>3-Tier architecture: Separate Core, Aggregation and Access layers</td>
<td>3-Tier architecture: Separate Core, Aggregation and Access layers</td>
</tr>
<tr>
<td></td>
<td>Distributed or Centralized.</td>
<td>Distributed or Centralized.</td>
<td>Distributed or Centralized.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L3 only Model (routed access)</th>
<th>Small Campus</th>
<th>Medium Campus (multiple floors)</th>
<th>Large Campus (multiple buildings)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized. (Distributed if single VRF.)</td>
<td>Centralized.</td>
<td>Centralized.</td>
<td>Inter-Core routing</td>
</tr>
<tr>
<td>Not attractive.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Inter-Core routing
Three-Tier Campus Network
Mobility Controller attachment

To Core
• Core must perform L2 and L3

To dedicated aggregation switches
• Recommended for large number of dual-stack (v4+v6) clients
• Off-load L2/L3 processing from Core
• Fault Domain isolation between wireless and core
Three-Tier Campus Network
Traditional L2+L3
Three-Tier Campus Network
In few cases: L2+L3 with L2 FW/IPS
Three-Tier Campus Network
In few cases: L2+L3 with L2 FW/IPS
Three-Tier Campus Network
10% of cases: L2+L3 with L3 FW
Three-Tier Campus Network
L3 Access Model for Centralized Access

Aruba Switch Proposal

Mobility Controller
L2

Access Layer
L3

Aggregation Layer
L3

Core Layer
L3

L3 Firewall

No VRF dependency with Dynamic Segmentation
Three-Tier Campus Network
Large Campus with dark fibers
Three-Tier Campus Network
Large Campus with reduced number of fibers (square routing)
Three-Tier Campus Network
Large Campus with dark fibers and L2 extension
Large Campus Network

No inter-building L2 extension: use mobile-first design with Dynamic Segmentation
Distribution Switch Selection
Sizing Considerations

• The current max scaling is 100,000 clients per Mobility Controllers Cluster.
• Larger deployments require multiple clusters each with their own distribution layer switches.
• Switch capacity drives the number of supported clients per Mobility Controller Clusters module.

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>ARP Max. IPv4 Addresses</th>
<th>ND Max. IPv6 Addresses</th>
<th>ARP/ND Max. IPv4+IPv6 Addresses (dual-stack)</th>
<th>1 IPv4 1 IPv6 Link-Local 1 IPv6 SLAAC or DHCPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 3810 Series</td>
<td>25 000</td>
<td>12 500</td>
<td>8 300</td>
<td>5 000</td>
</tr>
<tr>
<td>Aruba 5400R Series</td>
<td>25 000</td>
<td>12 500</td>
<td>8 300</td>
<td>5 000</td>
</tr>
<tr>
<td>Aruba 8320 Series</td>
<td>125 000</td>
<td>57 344</td>
<td>38 200</td>
<td>23 000</td>
</tr>
<tr>
<td>Aruba 8400 Series</td>
<td>131 072</td>
<td>65 536</td>
<td>65 536</td>
<td>32 768</td>
</tr>
</tbody>
</table>
Aruba Virtual Switching Extension (VSX)

Overview
Aruba Virtual Switching Extension
VSX Principles

- **High Availability by design during upgrades**

- Support for active-active data-path:
  - Active-active L2
  - Active-active L3 unicast
  - Active-active L3 multicast*

- Operational simplicity and usability:
  - for configuration
  - for troubleshooting

- Similar VSF benefits with better HA during upgrade

* This requires future ArubaOS-CX release
Switch Virtualization Solutions
Comparison

Chassis 1
Management
Control
Routing
Ethernet Links

Chassis 2
Management
Control
Routing
Ethernet Links

Shared

VSX
VSS
IRF
Virtual Chassis

Chassis 1
Management
Control
Routing
Ethernet Links

Chassis 2
Management
Control
Routing
Ethernet Links

Shared

SYNC(*)
(* different levels of synchronization)
**VSX Benefits**

**Control Plane**
- Dual control plane for better resiliency
- Unified management (synchronized configuration and easy troubleshooting)
- Independently software upgradable with near zero downtime
- In-chassis redundancy (8400) & device level redundancy

**L2 Distributed LAGs (Agg to Acc)**
- No spanning-tree
- Loop-free L2 multi-pathing (active-active)
- Rapid failover
- Simple configuration

**L3 Distributed LAGs (Core to Agg)**
- Distributed L3 over VSX pair (various options: ROP, SVIs or LAG’d SVIs)
- Unified data path (active-active first hop gateway)
- L3 ECMP + L2 VSX (highly fault tolerant)

**Active Gateway**
- Active-Active first hop gateway (VIP)
- No VRRP/HSRP
- Simple configuration (1 command)
- No gateway protocol overhead
- DHCP relay redundancy
VSX - Data Plane Virtualization
Multi-Chassis Link Aggregation (MCLAG)
VSX LAG
Extend link-aggregation to ports on different chassis

- **MCLAG:**
  - ports distributed on two chassis (same speed)
  - Inter-Switch Link (ISL)
    - Used to exchange management and control information
    - data traffic between the member chassis (no encapsulation)
    - Can be a single port or a LAG
  - is seen by the LAG peer as a single group with all the ports on the same switch peer ID
  - layer 2 only
  - LACP mode: ACTIVE (default)

- **Active gateways:**
  - are virtual IP/MAC addresses pairs
  - no need for VRRP (mutually exclusive)
  - are defined at VLAN interface level for each VLAN transported across the MC-LAG
  - are the same on both chassis
VSX MCLAG
L2 Configuration Example

interface lag 11 multi-chassis
description access-sw1
no shutdown
no routing
vlan trunk native 1
vlan trunk allowed 5,10,15,20
lacp mode active

interface lag 12 multi-chassis
description access-sw2
no shutdown
no routing
vlan trunk native 1
vlan trunk allowed 5,10,15,20
lacp mode active

interface 1/1/1
no shutdown
lag 11

interface 1/1/2
no shutdown
lag 12

trunk 25-26 trk1 lacp
VSX MCLAG
L3 Active/Active Configuration Example

vrf vrf1
interface vlan10
  vrf attach vrf1
  ip address 10.10.10.3/26
  active-gateway ip 10.10.10.1 00:00:00:00:10:01

vrf vrf1
interface vlan10
  vrf attach vrf1
  ip address 10.10.10.2/26
  active-gateway ip 10.10.10.1 00:00:00:00:10:01
Routing Design & Architecture Impact
Using VSX
VSX LAG and upstream routing
Constraints Diversity

- L2 or L3 links with upstream core nodes?
- Static? OSPF? BGP?
- Single VRF / Multiple VRF
- Sizing / limitations
- Best practice for HA

- In all scenarios, the 2 VSX switches run independent control planes (OSPF/BGP) and present themselves as different routers with their own Router_IDs in the network.

- In the data path however, they function as a single router and support active-active forwarding.
Definition
SVI / ROP

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

▪ ROP:
  – A **Routed Only Port** is a physical port on a switch that process all Layer 3 functions for packets to or form the said port without any binding to VLAN processing.
L3 Link Aggregation

Features / Practices

– L3 LAG are supported
– Configuration developed/tested using L3.
– 128 LAG interfaces Max
– Can use up to 8 interfaces per LAG
– Optimal design uses LAGs between L3 blocks (see reference topology)

CLI

Configure the LAG interface

```
interface lag <LAG-ID>
  description LAG to Core Switch 1
  no shutdown
  lacp mode active
  ip address <IP-ADDR>/<Prefix-Len>
```

Associate member links with the LAG interface

```
interface <IFACE-ID>
  description LAG to Core Switch 1
  no shutdown
  lag <LAG-ID>
```
Upstream Connectivity Options
ROP, SVIs, MCLAG SVIs

ROP
(single VRF)

SVIs
(multiple VRFs)

VSX LAG SVIs

Optimize IPAM with usage of /31 for L3 point-to-point
Three-Tier Campus Network – Topologies & Routing
ECMP or LAG - multiple VRFs

OSPF point-to-point

ECMP

10.3.1.0/24  Agg1-IP  VLAN301
10.3.1.0/24  Agg2-IP  VLAN303

MCLAG

10.3.1.0/24  Agg1-IP  VLAN301
10.3.1.0/24  Agg2-IP  VLAN303

VRF3: 10.3.1.0/24

Access1  
Access2 (VSF)  

Core1  
Core2  

Agg1  
Agg2 (VSF)  

VSX  

VRF1: Transit VLAN 101
VRF2: Transit VLAN 201
VRF3: Transit VLAN 301

OSPF broadcast

L2 link

L3 link
Upstream Connectivity Options
ROP, SVIs, MCLAG SVIs
Upstream routing over point-to-point links
Multiple VRF - SVIs - OSPF

- OSPF point-to-point
Three-Tier Campus Network – Topologies & Routing

Triangles converge faster than square

**ECMP + Triangles**
- Fast - No convergence needed

**Square**
- Routing convergence

*Diagram showing network topologies and routing details.*
Three-Tier Campus Network – Topologies & Routing
ECMP or LAG - single VRF

8400-2# show ip ecmp
ECMP Configuration
---------------------
ECMP Status : Enabled
ECMP Load Balancing by
------------------------
Source IP : Enabled
Destination IP : Enabled
Source Port : Enabled
Destination Port : Enabled

8400-1(config)# maximum-paths
<1-8> Number of ECMP routes. Default is 4.

8400-1(config)# lacp hash
12-src-dst Base the hash on 12-src-dst
13-src-dst Base the hash on 13-src-dst
14-src-dst Base the hash on 14-src-dst
Three-Tier Campus Network – Topologies & Routing
More redundancy with recommended additional links - square

Link failure protection would require area 0 on Agg layer

Port from Line Card A
Port from Line Card B
Three-Tier Campus Network – Topologies & Routing

More redundancy with recommended additional links - triangles

Link failure protection would require area 0 on Agg layer

Port from Line Card A
Port from Line Card B
Three-Tier Campus Network – Topologies & Routing

Set your redundancy limit

Worth it?
Three-Tier Campus Network – Topologies & Routing

Core question: VSX - to be or not to be?

Option for some cases

Core1

Agg1
Default Gateway

Core2

Agg2
Default Gateway

VSX

Core1

Agg1
Default Gateway

Core2

Agg2
Default Gateway

L2 link
L3 link

Access1

Access2 (VSF)

Transit VLAN

Transit VLAN

Transit VLAN

Transit VLAN

Transit VLAN

Three-Tier Campus Network Topologies
VSX to help resiliency in Square Topology

Core nodes with VSX
• Fast – No convergence

Legacy Core nodes
• Routing convergence

VSX Active-forwarding
route NH is unchanged

new route has to be set in FIB
Upstream routing to IRF Core
Without VSX Active-Forwarding

- OSPF broadcast
- Additional ISL sizing considerations:
  - Statistically, 50% of data traffic will cross ISL and add one L3 node on the data-path
  - ISL BW \( \approx \) uplinks BW
Upstream routing to IRF Core
With VSX Active-Forwarding

- No data traffic over ISL in nominal case.
- Each VSX node configures the VSX peer MAC as their own MAC (as a additional MAC)
- 8400-2 will process L3 function for the received packet as the DMAC is equal the its VSX peer MAC.
### VSX and Upstream Routing

**Supported Scenarios**

<table>
<thead>
<tr>
<th></th>
<th>Single VRF</th>
<th>Multiple VRFs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L3 port (ROP)</td>
<td>L2 port (SVI)</td>
</tr>
<tr>
<td><strong>static</strong></td>
<td>Yes (simplest)</td>
<td>yes</td>
</tr>
<tr>
<td><strong>OSPF</strong></td>
<td>Yes (simplest)</td>
<td>yes</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Yes (simplest)</td>
<td>yes</td>
</tr>
</tbody>
</table>
VRF
32 VRFs

– Default VRF
– 31 network VRF

+ “mgmt” VRF (Management-Plane only, not accessible from data-plane)
Features / Practices

- Define an OSPF Router-ID
  Ideally being equal to loopback address
- Define the associated VRF
- Use Passive-Default
- Enable OSPF on loopback interface
- Authenticate OSPF adjacencies
- Define OSPF Network Types
- Define OSPF Priority
- Minimize number of OSPF neighbors
  Max = 32
- Route-map support for controlled redistribution

CLI

```plaintext
router ospf 10
  router-id 10.10.10.10
  passive-interface default
  area 0.0.0.0

router ospf 11 vrf vrf1
  router-id 11.11.11.11
  passive-interface default
  area 0.0.0.0

interface loopback 0
  ip address <IP-ADDR>/<Prefix-Len>
  ip ospf <PROCESS-ID> area <AREA-ID>
  no ip ospf <PROCESS-ID> passive
  ip ospf authentication message-digest
  ip ospf message-digest-key md5 ciphertext <CIPHER>

interface 1/1/1
  vrf attach vrf1
  ip address 172.20.21.21/24
  ip ospf 10 area 0.0.0.0
  no ip ospf 10 passive
  ip ospf network point-to-point
  ip ospf message-digest-key md5 ciphertext <CIPHER>
```
8400-2# show interface 1/10/7

Interface 1/10/7 is up
  Admin state is up
  Description:
    Hardware: Ethernet, MAC Address: 94:f1:28:1d:ad:00
    IPv4 address 192.168.10.2/29
    MTU 1500
    Type SFP+SR
    QoS trust none
    Speed 10000 Mb/s
  L3 Counters: Rx Disabled, Tx Disabled
  Auto-Negotiation is off
  Input flow-control is off, output flow-control is off
  Rx
    287617 input packets  26387794 bytes
    0 input error                0 dropped
    0 CRC/FCS
  L3:
    0 packets, 0 bytes
  Tx
    287618 output packets  26387909 bytes
    0 input error                0 dropped
    0 collision
  L3:
    0 packets, 0 bytes

8400-2(config)# int 1/10/7
8400-2(config-if)# l3-counters
rx  Enable Rx L3 counters
tx  Enable Tx L3 counters
<cr>

8400-2# show interface 1/10/7

Interface 1/10/7 is up
  Admin state is up
  Description:
    Hardware: Ethernet, MAC Address: 94:f1:28:1d:ad:00
    IPv4 address 192.168.10.2/29
    MTU 1500
    Type SFP+SR
    QoS trust none
    Speed 10000 Mb/s
  L3 Counters: Rx Enabled, Tx Enabled
  Auto-Negotiation is off
  Input flow-control is off, output flow-control is off
  Rx
    287643 input packets  26390184 bytes
    0 input error                0 dropped
    0 CRC/FCS
  L3:
    0 packets, 0 bytes
  Tx
    287644 output packets  26390299 bytes
    0 input error                0 dropped
    0 collision
  L3:
    0 packets, 0 bytes
Loop Protection
MCLAG
And L2 loop avoidance mechanism

- VSX LAG is mutually exclusive with Spanning tree:
- Instead, use loop-protect functionality
- On MCLAG interface or on individual L2 ports
- Not on ISL

- Not on L3 port

- For configuration:
  - loop-protect on the interface
  - + per VLAN
  - Limited to 4k port-VLAN pairs (i.e. 1 port configured for 4K VLANs, or 4 ports configurable over 1K VLANs etc.)
  - loop-protect actions:
    - do-not-disable  Do not disable the sending port when a loop is detected
    - tx-disable      Disable the sending port when a loop is detected
    - tx-rx-disable   Disable the sending and receiving port when a loop is detected
Loop-protect
Native VLAN 1

No loop detected on 1/1/4
8320-1# show loop-protect 1/1/4

Status and Counters - Loop Protection Information
Transmit Interval : 5 (sec)
Port Re-enable Timer : Disabled

Interface 1/1/4
  Loop-protect enabled : Yes
  Action on loop detection : TX disable
  Loop detected count : 0
  Loop detected : No
  Interface status : down

Loop detected on 1/1/3
8320-1# show loop-protect 1/1/3

Status and Counters - Loop Protection Information
Transmit Interval : 5 (sec)
Port Re-enable Timer : Disabled

Interface 1/1/3
  Loop-protect enabled : Yes
  Action on loop detection : TX disable
  Loop detected count : 1
  Loop detected : Yes
  Detected on VLAN : 1
  Detected at : 2018-03-09T14:25:41
  Interface status : down
### Loop-protect

#### Per VLAN

8320-1# show loop-protect

**Status and Counters - Loop Protection Information**

<table>
<thead>
<tr>
<th>Transmit Interval</th>
<th>5 (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Re-enable Timer</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Interface 1/1/3**

- Loop-protect enabled: Yes
- Loop-Protect enabled VLANs: 111
- Action on loop detection: TX disable
- Loop detected count: 1
- Loop detected: Yes
- Detected on VLAN: 111
- Detected at: 2018-03-09T14:49:37
- Interface status: down

**Interface 1/1/4**

- Loop-protect enabled: Yes
- Loop-Protect enabled VLANs: 111
- Action on loop detection: TX disable
- Loop detected count: 0
- Loop detected: No
- Interface status: down

**Interface lag11**

- Loop-protect enabled: Yes
- Action on loop detection: TX disable
- Loop detected count: 0
- Loop detected: No
- Interface status: up

```bash
interface 1/1/3
  no shutdown
  no routing
  vlan trunk native 1 tag
  vlan trunk allowed 111
  loop-protect
  loop-protect vlan 111

interface 1/1/4
  no shutdown
  no routing
  vlan trunk native 1 tag
  vlan trunk allowed 111-112
  loop-protect
  loop-protect vlan 111
```
Loop protection with access switches
Loop on access switches

2018-03-09:15:05:05.496305|hpe-MC-LAGd|7011|LOG_INFO|AMM|--|MC-LAG 11 state local up, remote down
2018-03-09:15:06:23.575126|hpe-1pd|2801|LOG_WARN|AMM|--|Port lag11 is disabled by Loop-protection after loop detection
2018-03-09:15:06:23.575332|hpe-1pd|2807|LOG_INFO|AMM|--|Loop-Protection stats cleared for port lag11
2018-03-09:15:06:23.594403|intfd|404|LOG_INFO|AMM|--|Link status for interface 1/1/1 is down

8320-1# show loop-protect
Status and Counters - Loop Protection Information

Transmit Interval : 5 (sec)
Port Re-enable Timer : Disabled

Interface lag11
- Loop-protect enabled : Yes
- Loop-Protect enabled VLANs : 111
- Action on loop detection : TX disable
- Loop detected count : 1
  - Loop detected : Yes
    - Detected on VLAN : 111
    - Detected at : 2018-03-09T15:06:23
- Interface status : down

Interface lag12
- Loop-protect enabled : Yes
- Loop-Protect enabled VLANs : 111
- Action on loop detection : TX disable
- Loop detected count : 0
- Loop detected : No
- Interface status : down

8320-1# show interface brief
---------------------------------------------------------------
Port Native Mode Type Enabled Status Reason Speed VLAN
---------------------------------------------------------------
1/1/1 1 trunk SFP+SR yes down Disabled by feature 2930-3
lag11 1 trunk -- yes down -- auto
---------------------------------------------------------------
Loop-Protect
8320-2 does not see the loop

2018-03-09:15:06:23.764864|hpe-MC-LAGd|7014|LOG_INFO|AMM|--|MC-LAG 11 state local down, remote down
2018-03-09:15:06:55.737581|lldpd|106|LOG_INFO|AMM|--|LLDP neighbor e0:07:1b:c2:b5:e0 deleted on 1/1/1

8320-2# sh loop-protect

Status and Counters - Loop Protection Information

Transmit Interval : 5 (sec)
Port Re-enable Timer : Disabled

Interface lag11
Loop-protect enabled : Yes
Loop-Protect enabled VLANs : 111
Action on loop detection : TX
disable
Loop detected count : 0
Loop detected : No
Interface status : down

Interface lag12
Loop-protect enabled : Yes
Loop-Protect enabled VLANs : 111
Action on loop detection : TX
disable
Loop detected count : 0
Loop detected : No
Interface status : up
Loop-protect
Restore

- By default, when a loop is detected, the interface is blocked until loop-protect is disabled.
- Use re-enable-timer

```
8320-1(config)# loop-protect re-enable-timer
<15-604800> Enter the re-enable time interval for enabling blocked port (Default : Disabled)
```

- After configured timer, the port will be re-enable.
  If loop is persistent, loop-protect will block again the interface.
Network Management
Switch Management
In-Band / Out-of-Band

Features / Practices

▪ mgmt VRF

▪ interface mgmt
  – 1 port on 8320, 2 ports on 8400 (with 2 MMs)
  – Attached to mgmt VRF (can not be modified).
  – prefer static IP address assignment
  – default-gateway: out-of-band L3 network management infrastructure switch
  – no ACL (yet)
    (ACL has to be set on management infrastructure)

▪ No ACL on ssh or https services

▪ Shell and mgmt VRF

CLI

hostname CORE-8400-1

8400-1(config)# ip dns
  domain-list     Configure list of domains to which DNS request is sent to complete unqualified host names
  domain-name    Configure default domain name
  host           Add an entry to the IP hostname table
  server-address Configure DNS server IP address

  ip dns domain-name aruba.hpe.com
  ip dns domain-list aruba.hpe.com

  ip dns host logbox 10.20.3.4 vrf mgmt

  ip dns server-address 8.8.8.8
  ip dns server-address 4.4.4.4

switch(config)#banner motd <delimiting character>
switch(config)#banner exec <delimiting character>
Secure Shell

Features / Practices
- Must be enabled per VRF.
- Can be enabled simultaneously for multiple VRFs.
- Telnet service is not available.
- Currently, no source IP address protection on SSH service.

CLI
- `ssh server vrf mgmt`
- `ssh server vrf default`
- `ssh server vrf vrfA`
Web-UI

Features / Practices

▪ Web-UI is disabled by default
▪ https only (no http)
▪ Must be assigned to a VRF
▪ Can be assigned to ‘default’ or any other VRF
▪ Can be assigned simultaneously to multiple VRFs
▪ API is accessible in read-only or read-write
▪ No source IP address protection on https service

CLI

```console
https-server vrf <VRF NAME>
https-server rest access-mode read-write
```
Basic’s
Hostname, domain-name, dns, banner

Features / Practices

▪ Configure a hostname, domain name, and name server(s)
▪ If DNS is not available, local host entries can be made. Note that locally defined host entries are unique to each VRF
▪ Configure a Message of the day (MOTD) and an login (exec) banner

CLI

hostname CORE-8400-1

8400-1(config)# ip dns
  domain-list Configure list of domains to which DNS request is
  sent to complete unqualified host names
  domain-name Configure default domain name
  host Add an entry to the IP hostname table
  server-address Configure DNS server IP address

ip dns domain-name aruba.hpe.com
ip dns domain-list aruba.hpe.com

ip dns host logbox 10.20.3.4 vrf mgmt

ip dns server-address 8.8.8.8
ip dns server-address 4.4.4.4

switch(config)#banner motd <delimiting character>
switch(config)#banner exec <delimiting character>
SNMP

Features / Practices

- Configure SNMP to send traps to no more than 2 NMS systems
- Use SNMPv3 if supported by NMS
- **Note:** CX does NOT support SNMP SET commands
- `snmp-server` can only be enabled in “mgmt” or “default” VRFs. If enabled on both VRFs, it will only work on default, as it takes precedence.

CLI

```
8400-1(config)# snmp-server
agent-port          Configure UDP port to reach SNMP Master Agent
community           The name of the community string. Default is public
host                Configure SNMP trap or inform
system-contact      Configure system contact
system-description  Configure system description
system-location     Configure system location
vrf                  Specify VRF to run SNMP on

snmp-server agent-port 161
snmp-server vrf mgmt.
snmp-server system-description TME 8400-1
snmp-server system-location Roseville
snmp-server system-contact TME
snmp-server community Aruba

version 2c
snmp-server host 10.0.1.5 trap version v2c community public

version 3
snmpv3 user myuser auth md5 auth-pass myauthpass priv aes priv-pass myprivpass
snmp-server host 10.0.1.5 trap version v3 user NETMGMT
```
Logging

Features / Practices

- Define no more than two logging destinations
- Syslog traffic is supported on a single VRF (any). By default the default VRF.
- Note: Default logging facility is 3.

CLI

```
logging 10.2.3.4 vrf vrf1
logging 10.4.3.5
logging log-server_name

8400-1(config)# logging facility
local0 Local 0
local1 Local 1
local2 Local 2
local3 Local 3
local4 Local 4
local5 Local 5
local6 Local 6
local7 Local 7

8400-1(config)# logging 10.2.6.4
include-auditable-events Forward auditable logs to the remote syslog server
severity Forward syslog messages of specified severity and above (Default:info)
tcp Forward syslog messages using TCP protocol
udp Forward syslog messages using UDP protocol (Default)
vrf VRF used to connect to remote syslog server (Default: default)
<cr>

show events
```
Network Time Protocol (NTP)

Features / Practices

▪ associate NTP with appropriate VRF (for first release: default or mgmt vrf)
▪ Define up to two NTP servers
  – Use prefer command for “most preferred server”
▪ Use ‘iburst’ option to speed-up NTP sync process
▪ Set the timezone appropriately
▪ To reduce time to synchronize with NTP server, set the date and time before entering the NTP server command

CLI

```plaintext
ntp vrf mgmt.
npt server 1.1.1.1 iburst prefer
ntp server 2.2.2.2 iburst
clock timezone <timezone>
```

8400-1# sh ntp status
NTP is enabled
NTP authentication is disabled
NTP is using the management port (oobm) for NTP server connections
Wed Feb 28 16:06:37 CET 2018
NTP uptime: 8 days, 5 hours, 48 minutes, 31 seconds
Synchronized to NTP Server 15.136.40.60 at stratum 3
Poll interval = 1024 seconds
Time accuracy is within 2.930 seconds
Reference time: Wed Feb 28 2018 15:47:06.725 as per Europe/Paris timezone

8400-1# sh ntp associations
```
ID          NAME          REMOTE        REF
-            -            -            -
* 1              15.136.40.60      15.136.40.60  15.135.123  3  594 1024   377
```

8400-1# sh ntp statistics
```
Rx-pkts 1400211
Current Version Rx-pkts 0
Old Version Rx-pkts 750
Error pkts 0
Auth-failed pkts 0
Declined pkts 0
Restricted pkts 0
Rate-limited pkts 0
KOD pkts 0
```

8400-1# sh ntp servers
```
NTP SERVER KEYID MINPOLL MAXPOLL OPTION VER
-----------------------------------------------
15.136.40.60  -       6      10 none  3
```
sFlow

Features / Practices
- Set sflow agent-ip to loopback address of the switch
- Supports up to 3 collectors, generally see no more than 2
- Use default sampling and polling timers unless you have a specific reason to change them
- Collect info from ‘meaningful’ interfaces:
  - On Core: links to Service Aggregation blocks
  - On Agg: links to Access blocks and Controllers
- Don’t enable sFlow on all interfaces
- Can be enabled on a lag interface

CLI
```
sflow
sflow agent-ip <IP-ADDR>
sflow collector <IP-ADDR>
sflow sampling 4096
sflow polling 30
interface <IFACE-ID>
sflow
```

swag-a1# show sflow

sFlow Global Configuration
-------------------------------
sFlow enabled
Collector IP/Port/Vrf 10.80.2.200/6343/default
Agent Address 10.224.68.10
Sampling Rate 4096
Polling Interval 30
Header Size 128
Max Datagram Size 1400

sFlow Status
-----------------------------------------
Running - No

Collector Status
----------------
10.80.2.200/6343/default - Not reachable

sFlow Statistics
-------------------------------
Number of Samples 0

8400-1# sh sflow int 1/3/8

sFlow Configuration - Interface 1/3/8
-------------------------------
sFlow enabled
Sampling Rate 4096
Number of Samples 0
sFlow Sampling Status success
Logrotate and Log files

Features / Practices

– 3 log files:
  – Authentication logs stored in the /var/log/auth.log file.
  – Audit logs stored in the /var/log/audit/audit.log file
– Define logrotation size/frequency
– Keep default: 100MB, daily
– Export to tftp://<server_ip>

CLI

logrotate target tftp://15.136.40.99
Miscellaneous
Role-Based Authentication

Features / Practices

- Use TACACS for authentication and authorization
- Define local accounts as backup
- DO NOT use the ‘aaa authentication allow-fail-through’

CLI

Configure TACACS
switch(config)# tacacs-server key SECRETKEY
switch(config)# tacacs-server host 10.0.0.101

Configure AAA authentication to TACACS with local fallback
switch(config)# aaa authentication login default group tacacs local

Configure AAA authorization *
switch(config)# aaa authorization commands default group tacacs

Configure Local User Account
switch(config)# user backup-admin group administrators password
Adding user backup-admin
Enter password:************
Confirm password:************

Show Commands To Validate Functionality
switch# show tacacs-server detail
switch# show aaa authentication
switch# show aaa authorization

(*) RADIUS server groups are not allowed to be configured as a AAA authorization method because RADIUS command authorization is unsupported.
Control Plane Policy
CoPP

Features / Practices
▪ Factory-default copp-policy

### CLI

```
8320-1# sh copp-policy factory-default
   class                  drop priority rate pps burst pkts hardware rate pps
acl1-logging           0      50      50      50
arp-broadcast          3     7000     7000     7000
arp-unicast-ipv4      4     2500     2500     2500
bgp-ipv4             6     1500    1500    1500
bgp-ipv6             6     1500    1500    1500
dhcp-ipv4            1     1000    1000    1000
dhcp-ipv6            1     1000    1000    1000
hyptext              5      15      15      15
icmp-unicast-ipv4    4     1000    1000    1000
icmp-unicast-ipv6    4     1000    1000    1000
igmp                 6     2500    2500    2500
ip-exceptions        0      15      15      15
ipv4-options         2      150     150     150
ipv6-options         2      150     150     150
lacp                  6     1000    1000    1000
lldp                  6     500      500     500
loop-protect          7     1000    1000    1000
mvrp                  6     1000    1000    1000
ntp                   5     150      150     150
ospf-multicast-ipv4   6     2500    2500    2500
ospf-multicast-ipv6   6     2500    2500    2500
ospf-unicast-ipv4    6     2500    2500    2500
ospf-unicast-ipv6    6     2500    2500    2500
pim                   6     1500    1500    1500
sfow                  1     2000    2000    2000
ssh                   5      500     500     500
stp                   7     2500    2500    2500
telnet                5      500     500     500
udld                  7      500     500     500
unknown-multicast    2     1500    1500    1500
unresolved-ip-unicast 2     1000    1000    1000
vrrp-ipv4            6     1000    1000    1000
vrrp-ipv6            6     1000    1000    1000
default              1      500     500     500
```
DHCP relay
Active-Gateway

- 2 DHCP requests are relayed to 3\textsuperscript{rd} party DHCP server.
- Due to 2 active-gateways.
- DHCP server will only serve the first received request.
Unidirectional Link Detection

Features / Practices

▪ Utility of UDLD in the Campus:
  – Patching mistakes: A-port1-TX -to- B-port2-Rx (instead of B-port1-Rx)
  – 1G (fiber cut transition detection without UDLD, only after establishment)
  – 10G standard

▪ Use UDLD mode aruba-os when connecting HPE Aruba switches
  – Enable UDLD with ‘verify-then-forward’ mode

▪ RFC5171 mode to support interop with other network vendors
  – Enable aggressive mode

CLI

Enable UDLD
interface 1/1/1
  udlid
    udlid mode aruba-os verify-then-forward

Show Commands to Validate Functionality
show udlid
show udlid interface 1/1/1

swag-a1# show udlid interface 1/1/18

Interface 1/1/18
Config: enabled
State: active
Substate: unblocked
Link: unblock
Version: aruba os
Mode: verify then forward
Interval: 7000 milliseconds
Retries: 4
Tx: 115642 packets
Rx: 162087 packets, 0 discarded packets, 0 dropped packets
Port transitions: 1
Unidirectional Link Detection
1G - Fiber cut without UDLD

5510

5510

<5510H1-1-test>display transceiver interface g1/0/15
GigabitEthernet1/0/15 transceiver information:
  Transceiver Type : 1000_BASE_SX_SFP
  Connector Type   : LC
  Wavelength(nm)   : 850
  Transfer Distance(m) : 550 (OM2), 270 (OM1)
  Digital Diagnostic Monitoring : YES
  Vendor Name      : HPE

<5510H1-1-test>display transceiver diagnosis interface g1/0/15
GigabitEthernet1/0/15 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    32        8.56       3.33      -40.00       -5.52
  Alarm thresholds:
    Temp.(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    High 81    3.80       44.00     0.00          3.00
    Low 2.81   1.00       -16.99   -12.50

8320

8320-1# show interface 1/1/7 transceiver detail
Transceiver in 1/1/7
  Interface Name      : 1/1/7
  Type                : 1000SX
  Connector Type      : LC
  Wavelength          : 20995nm
  Transfer Distance   : 0.00m (SMF), 150m (OM1), 300m (OM2), 0m (OM3)
  Diagnostic Support  : DOM
  Product Number      : J4858C
  Serial Number       : CN817EKOXD
  Part Number         : 1990-3662

Status
  Temperature : 21.47°C
  Voltage : 3.35V
  Tx Bias : 4.08mA
  Rx Power : 0.23mW, -6.38dBm
  Tx Power : 0.29mW, -5.38dBm

Recent Alarms:
Recent Errors:

8320-1# sh int 1/1/7
Interface 1/1/7 is up
  Admin state is up
  Description: to 5510 G1/0/15 - for UDLD test
  MTU 1500
  Type 1000SX
  qos trust none
  Speed 1000 Mb/s
Unidirectional Link Detection
1G - Fiber cut with UDLD

5510

<5510HI-1-test>display transceiver interface g1/0/15
GigabitEthernet1/0/15 transceiver information:
  Transceiver Type            : 1000_BASE_SX_SFP
  Connector Type              : LC
  Wavelength(nm)              : 850
  Transfer Distance(m)        : 550(OM2),270(OM1)
  Digital Diagnostic Monitoring: YES
  Vendor Name                 : HPE

<5510HI-1-test>display transceiver diagnosis interface g1/0/15
GigabitEthernet1/0/15 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(ãC)   Voltage(V)   Bias(mA)  RX power(dBm)  TX power(dBm)
    32         8.56        3.33   -40.00          -5.52
  Alarm thresholds:
    Temp.(ãC)   Voltage(V)   Bias(mA)  RX power(dBm)  TX
    High   81         3.80        44.00     0.00           3.00
    Low    0          2.81        1.00    -16.99        -12.50

8320

8320-1# show udld interface 1/1/7
Interface 1/1/7
Config: enabled
State: active
Substate: blocked
Link: block
Version: aruba os
Mode: verify then forward
Interval: 7000 milliseconds
Retries: 4
Tx: 92 packets
Rx: 0 packets, 0 discarded packets, 0 dropped packets
Port transitions: 0

8320-1# show interface 1/1/7
Interface 1/1/7 is down
Admin state is up
Description: to 5510 G1/0/15 - for UDLD test
MTU 1500
Type 1000SX
qos trust none
Speed 1000 Mb/s
Unidirectional Link Detection
10G - Fiber cut without UDLD

8320-1

8320-1# show interface 1/1/9 transceiver detail
Transceiver in 1/1/9
Interface Name : 1/1/9
Type : SFP+SR
Connector Type : LC
Wavelength : 20995nm
Transfer Distance : 0.00m (SMF), 30m (OM1), 80m (OM2), 300m (OM3)
Diagnostic Support : DOM
Product Number : J9150A
Serial Number : MY77VPD38P
Part Number : 1990-4175

Status
Temperature : 20.90C
Voltage : 3.38V
Tx Bias : 8.44mA
Rx Power : 0.00mW, -inf
Tx Power : 0.56mW, -2.52dBm

Recent Alarms:
Rx Power low alarm
Rx Power low warning

Recent Errors:

8320-1# show interface 1/1/9
Interface 1/1/9 is down
Admin state is up
State information: Waiting for link
Description:
MTU 1500
Type SFP+SR
qos trust none
Speed 10000 Mb/s

8320-2

8320-2# show interface 1/1/9 transceiver detail
Transceiver in 1/1/9
Interface Name : 1/1/9
Type : SFP+SR
Connector Type : LC
Wavelength : 20995nm
Transfer Distance : 0.00m (SMF), 30m (OM1), 80m (OM2), 300m (OM3)
Diagnostic Support : DOM
Product Number : J9150A
Serial Number : MY77VPD0XN
Part Number : 1990-4175

Status
Temperature : 26.08C
Voltage : 3.34V
Tx Bias : 8.48mA
Rx Power : 0.56mW, -2.52dBm
Tx Power : 0.65mW, -1.87dBm

Recent Alarms:

Recent Errors:

8320-2# show interface 1/1/9
Interface 1/1/9 is down
Admin state is up
State information: Waiting for link
Description:
MTU 1500
Type SFP+SR
qos trust none
Speed 10000 Mb/s
IPv4 Multicast Features

Features / Practices

- **PIM**
  - Support for sparse mode
  - Support for BSR or static RP configurations
  - Is “VRF” aware
  - Use a LAG for RP interface

- **IGMP**
  - Interop with V1, V2, and V3
  - Support for static-joins

**CLI**

Enable PIM Globally (for default VRF)
```
router pim <vrf> <VRF name>
  enable
  rp-candidate source-ip-interface lag1
  rp-candidate group-prefix 239.0.0.0/8
  bsr-candidate source-ip-interface lag1
  bsr-candidate priority 10
```

Configure PIM per interface
```
interface vlan141
  ip pim-sparce enable
```

Configure IGMP
```
interface vlan141
  ip igmp enable
  ip igmp version 2
```

Commands for Verification
```
show ip igmp
show ip mroute
show ip pim
show ip pim bsr
show ip pim interface
show ip pim nei
```
Other

Features / Practices
– DHCP snooping / trust port

CLI

dhcp-snooping
dhcp-snooping authorized-server 192.168.250.1
dhcp-snooping authorized-server 192.168.250.2
dhcp-snooping vlan 247-251

interface 1/7
dhcp-snooping trust
name "connection to ESXi"
interface Trk10
dhcp-snooping trust
name "mclag-to-8320"
Thank You