Private VLAN Updates

Presenters

Steve Baker, TME

Daryl Wan, TME

Agenda

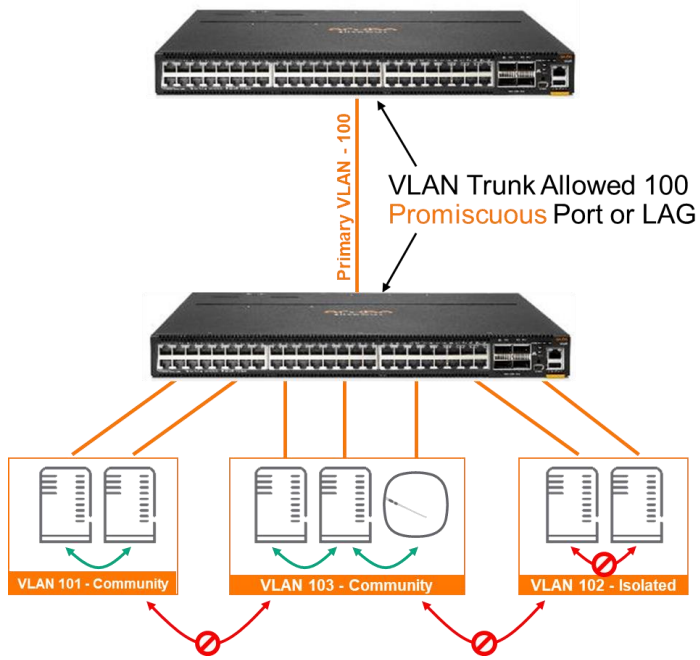
1. Overview / Review
2. Use Cases / Platforms
3. Details / Caveats
4. Troubleshooting
5. Demo

Overview/Review

Private VLAN - Review

Layer 2 Micro-Segmentation

Terminology	Description
Primary VLAN/ Promiscuous port	Root of PVLAN domain. Can be multiple secondary VLANs associated with a primary VLAN, which uses the Primary VLANs to communicate with hosts outside the PVLAN domain. Ports that are member of Primary VLAN can send packets to all ports of primary VLAN and ports of associated isolated and community VLANs. Used to communicate outside the PVLAN domain.
Isolated VLAN/Port	A secured VLAN where a hosts in isolated VLANs cannot communicate with each other through L2
Community VLAN/Port	Hosts in same C-VLAN can communicate with each other through L2. Can be multiple C-VLANs associated with a primary VLAN
Secondary VLAN/Port	Isolated and community VLAN/Ports are together called secondary VLAN/Ports
Private VLAN ISL	PVLAN domain can be extended across supported devices using Inter switch link (ISL) provided PVLAN VLAN configurations are same on all the devices. ISL ports carry both the primary and secondary VLAN. Any non-Secondary and non-Promiscuous ports can be made an ISL by making it a member of all VLANs in the PVLAN domain. Recommendation is to configure “trunk allowed all” on the port this is used as ISL. No PVLAN specific configuration is required on the ISL port.



Please refer to 10.8 ToI for additional PVLAN details

Capabilities, Restrictions and Exclusions

Promiscuous / regular primary port

Can be member of multiple primary VLANs (VLAN trunk)

Can be member of multiple normal VLANs (VLAN trunk)

Cannot be member of any secondary VLAN even those mapped to other Primary VLANs

Secondary port

Can be member of multiple isolated/community VLANs mapped different primary VLANs

Can be member of multiple normal VLANs

Cannot be member of any multiple secondary VLANs for a given Primary VLAN

PVLAN feature

Cannot be enabled when some features such as VLAN translation, GVRP, RPVST, MVRP are already configured.

Default VLAN (1)

Cannot be configured primary or secondary VLANs (same for reserved VLANs)

Secondary VLANs

Cannot have an SVI interface

Primary VLANs per Secondary VLAN

1

Please refer to 10.8 ToI for additional PVLAN details

State Details

Operational State
If Primary VLAN is administratively down: All its Secondary VLAN(s) will be "down" with reason "pvlan_primary_down"
If Secondary VLAN is set to administratively down, it will be "ignored"
If there is no primary VLAN association for a secondary VLAN, that secondary will be set to "down"

PVLAN Configurations Limitations
The default VLAN (VLAN 1) cannot be configured as a PVLAN.
An access port—which is directly connected to a host—can belong to one secondary VLAN in the PVLAN only.
Promiscuous ports can be members of the primary VLAN only.
Ports can be one type only: promiscuous, secondary

Enabled at primary SVI only.
Local-proxy ARP / Proxy ARP / IPv4/v6 Address / ND / Jumbo-MTU / DHCP Server / VRRP / BGP / OSPF / OSPF3 / RIP / MSTP vlan-instance map / Static routes / Ping (source VLAN configuration) / Voice VLAN

Please refer to 10.8 ToI for additional PVLAN details

Use Cases / Platforms

Use Cases / Platforms

Campus

- Isolated VLANs: hospitality with wired guest connections
- Community VLANs: multiple small tenants
  - Shopping center: many small shops with wired connection and single IP subnet

Datacenter

- Isolated VLANs
  - Backup network: all endpoints need to send information to a single backup server/cluster
- Community VLANs
  - Multitenant DC

In 10.8

- CX 6200F
- CX 6300F and 6300M
- CX 6400
- CX 8360

In 10.9

- CX 8325
- CX 10000

No Support

- CX 6100
- CX 4100i
- CX 8320
- CX 8400

Please refer to 10.8 ToI for additional PVLAN details

Details and Caveats

10.9 PVLAN Enhancements

VXLAN PVLAN

PVLAN w/PIM

- PIM can be enabled only on the Primary VLAN SVI
- PIM handles unknown Multicast on a VLAN when it is enabled on an SVI
- Support for enabling L3 multicast/Unicast on Primary VLANs on a device where there is also Secondary VLAN mapping for those Primary VLANs
  - Is-Never: L3 feature configuration on Secondary VLANs.

IGMP/MLD Snooping

- When IGMP/MLD Snooping is enabled/disabled on Primary VLAN, it is automatically enabled/disabled on all secondary VLANs
- When a Secondary VLAN is created + Snooping is enabled, any newly associated secondary VLANs will automatically inherit the IGMP/MLD snooping config from Primary VLAN.
  - **When Join/Leave/Query Received on:**
    - Primary VLAN it is replicated to all Secondary VLANs
    - Community/Isolated VLAN it is replicated to the corresponding Primary VLAN

VSF support – CX 6200/6300

- Switchover/failover is supported
- PVLAN secondary/promiscuous ports can be on any member device

VSX support – CX 6400/8360/8325/10000

- MC-LAG can be a PVLAN port, the PVLAN config can be sync'd across to a standby VSX pair

Please refer to 10.8 ToI for additional PVLAN details

Scale

Maximum # Private Primary VLANs	
32	CX 6200/6300/6400/8360/8325
512	CX 10000

Maximum # Secondary VLANs per Primary	
24	CX 6200/6300/6400/8360/8325/10000

Maximum number of physical ports in a PVLAN	
24	CX 6200/6300/6400/8360
No Limit	CX 8325/10000

```
show capacities private-vlan

System Capacities: Filter Private-VLAN
Capacities Name                                                                                                  Value
-----------------------------------------------------------------------------------------------------------------------
Maximum number of primary VLANs allowed to be created for Private-VLAN on the system                              32
Maximum number of Private-VLAN secondary ports per LC allowed to be created on the system                         24
Maximum number of secondary VLANs allowed to be created for a specific private VLAN                               24
```

Please refer to 10.8 ToI for additional PVLAN details

Configuration

Primary and Secondary VLANs

Primary VLAN

```
vlan 1100
  name PRIV-PRIM
  private-vlan primary
```

Secondary VLANs

```
vlan 1111
  name PRIV-COMM
  private-vlan community primary-vlan 1100

vlan 1121
  name PRIV-ISOL
  private-vlan isolated primary-vlan 1100
```

Secondary VLAN Ports

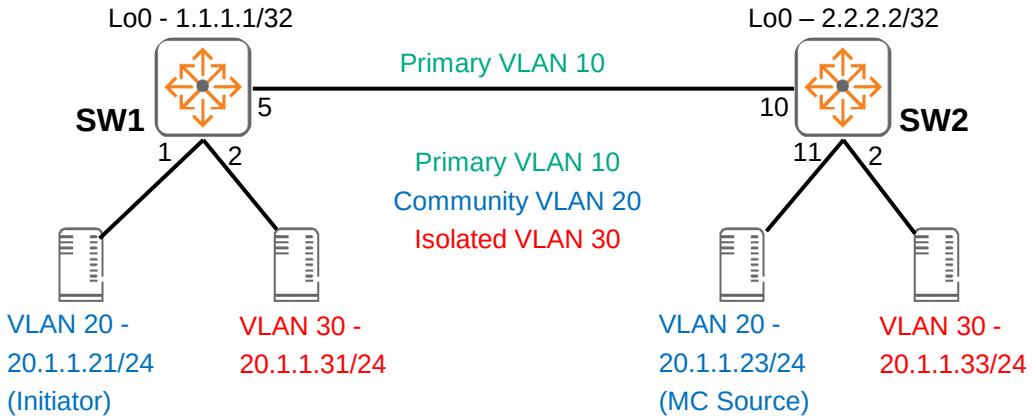
```
interface 1/1/9
    [. . .]
    vlan access 1121
    private-vlan port-type secondary
```

Primary VLAN Promiscuous Port / Uplink

```
interface lag 62
    [. . .]
    vlan trunk allowed 1100
    private-vlan port-type promiscuous
```

L2 Multicast PVLAN Scenario

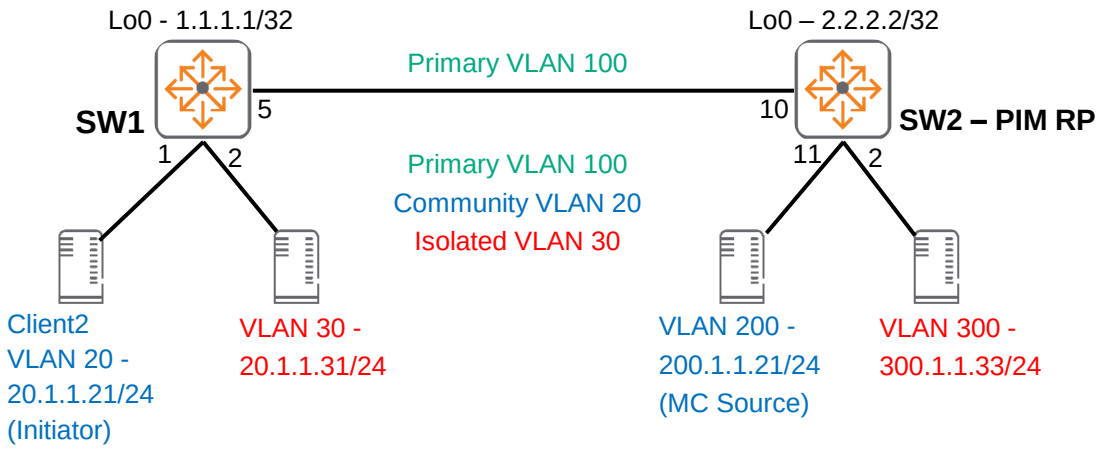
Switch2 receives IGMP Join on Primary VLAN 10



1. Join sent to Switch2 via P5 (P5 is querier port)
   a. Join replicated to Primary if received on Secondary VLANs on Switch1
2. Switch2 P10 receives original join from Switch1 – Forwards Join to P11
   a. Join replicated to any Secondary VLANs on Switch2 - (Replicated join not forwarded to Switch1)
3. Switch1 receives mcast traffic/stream on P5 from Switch2 P10 – Forwards to P1

L3 Multicast PVLAN Scenario

PIM Enabled – Source on Community

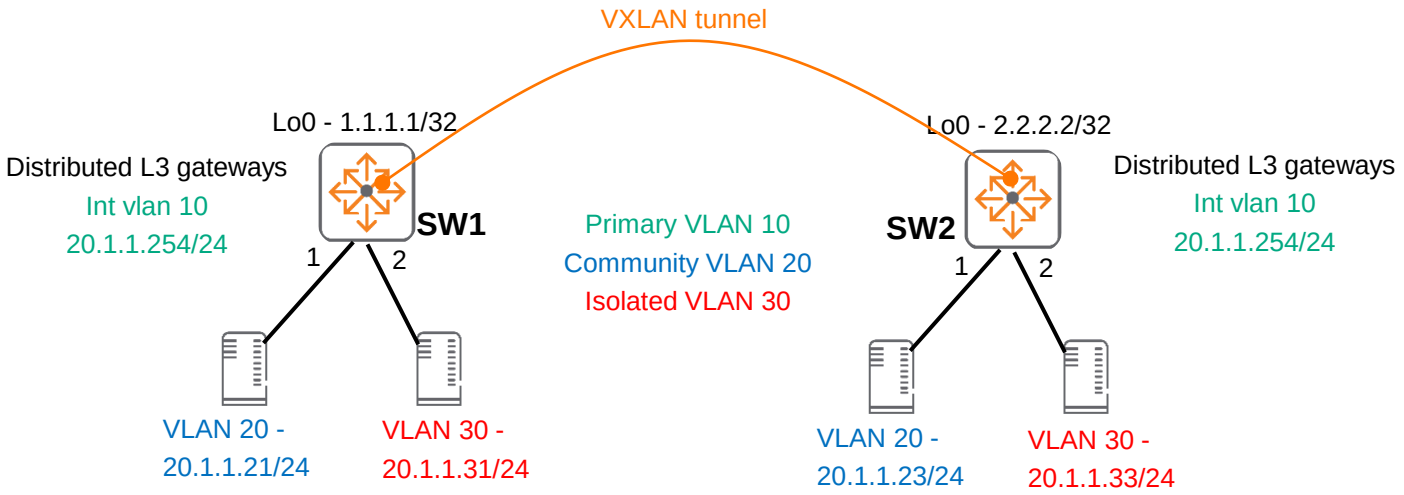


1. Join received on Switch1 P1 from Client2 VLAN 20
    a. Join replicated to Primary VLAN 100
2. Switch2 P10 receives original join from Switch1 – Forwards Join to P11
    a. Join replicated to any Community/Isolated VLANs on Switch2 - (Replicated join not forwarded to Switch1)
3. Routed multicast traffic received on Switch1 port P5 will be forwarded to port P1.

VXLAN PVLAN

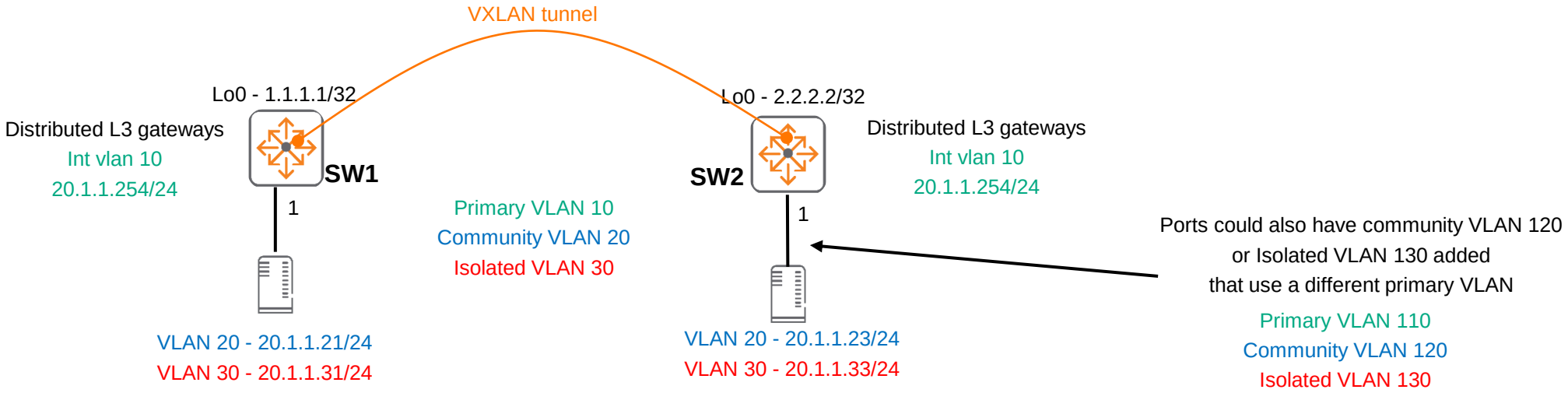
- VXLAN PVLAN provides L2 segmentation (IPv4/IPv6 unicast traffic only) between desired hosts on the same subnet
  - Hosts within the same community VLAN have network connectivity
  - Hosts in the isolated VLAN do not have network connectivity with other PVLAN hosts
  - Hosts are able to reach their default gateway in primary VLAN

- Supported platforms:
  - 6300, 6400, 8325, 8360, 8400, CX 10000



PVLAN Caveats

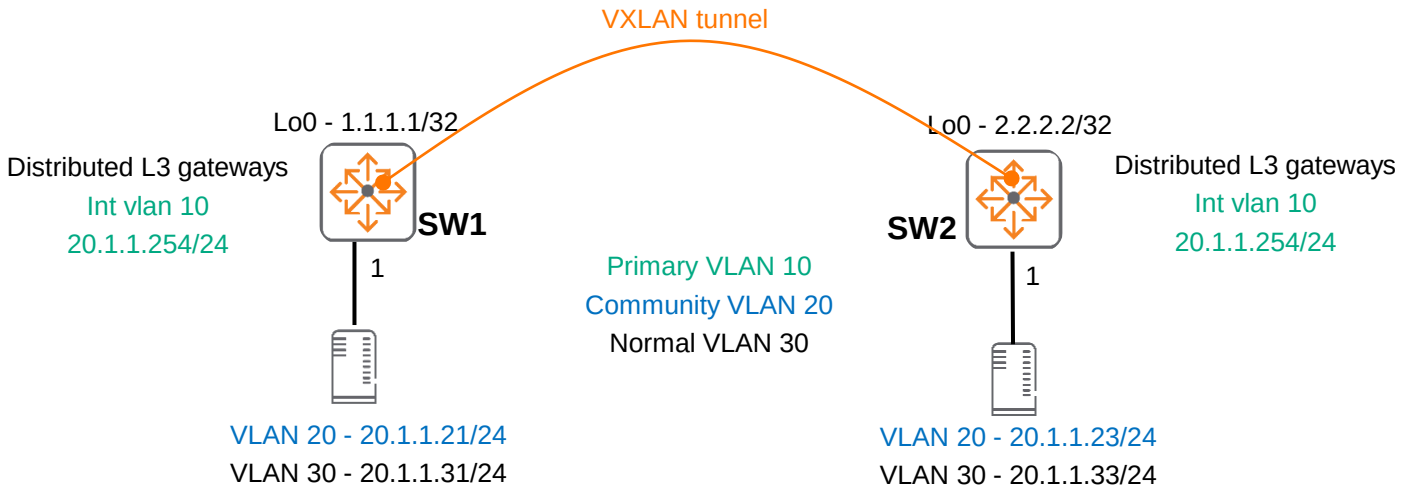
- Can’t have server facing port with multiple secondary VLANs (community and isolated) associated to same primary VLAN (in most environments) on 1 port
  - However, if the server has a vSwitch or blade switch that is PVLAN aware, below can be done



- It’s mandatory to add “private-vlan port-type secondary” to the server facing ports for PVLAN to function (in most environments)
  - However, if the server has a vSwitch or blade switch that is PVLAN aware and has the secondary VLANs configured, “private-vlan port-type secondary” is not required

PVLAN Caveats

- Server facing ports can have normal and secondary VLAN
- However, normal VLAN 30 hosts will not be able to reach their default gateway on SVI 10 used by PVLAN
- Solution: Move normal VLAN hosts to a different subnet
  - e.g. from VLAN 30(20.1.1.X/24) to VLAN 30(30.1.1.X/24) and utilize 30.1.1.254/24 as gateway



Troubleshooting

1. Check PVLAN configs are correctly configured

– Refer to config slide for sample configs

2. Verify PVLAN associations

– Verify the correct isolated/community VLANs are associated with the primary VLAN
– This should be consistent on all connected switches

```
SW1# sh private-vlan association

-------------------------------------------
Primary   Isolated          Community
-------------------------------------------
10        -                 20
110       -                 120
```

– PVLAN inconsistencies can be checked using

```
SW1(config)# sh pri inconsistency
-------------------------------------------------------------------------------
Interface/VLAN  Action  Inconsistency-Reason
-------------------------------------------------------------------------------
1/1/1           Down    Interface is a member of both primary and secondary VLAN.
```

3. Verify PVLAN port-type is correctly configured

- It's mandatory to add "private-vlan port-type secondary" to the server facing ports for PVLAN to function
  - However, if the server has a vSwitch that is PVLAN aware and has the secondary VLANs configured, "private-vlan port-type secondary" is not required

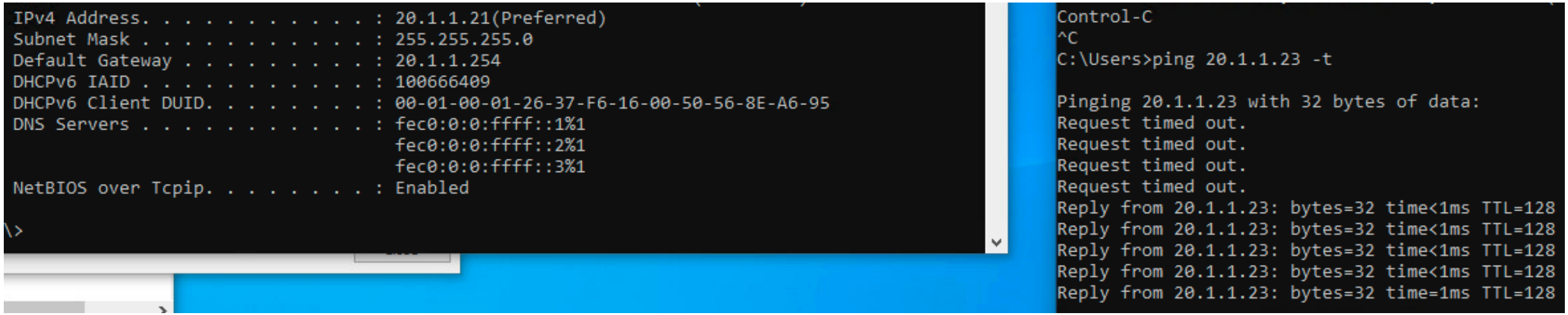
```
interface 1/1/1
    no shutdown
    mtu 9198
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed 20,30,120
    private-vlan port-type secondary
```

- This can also be checked using

```
SW1# sh private-vlan port-type
----------------------
Port       Port-type
----------------------
1/1/1      secondary
```

4. Verify traffic between hosts are allowed/blocked as expected

– Send traffic between hosts



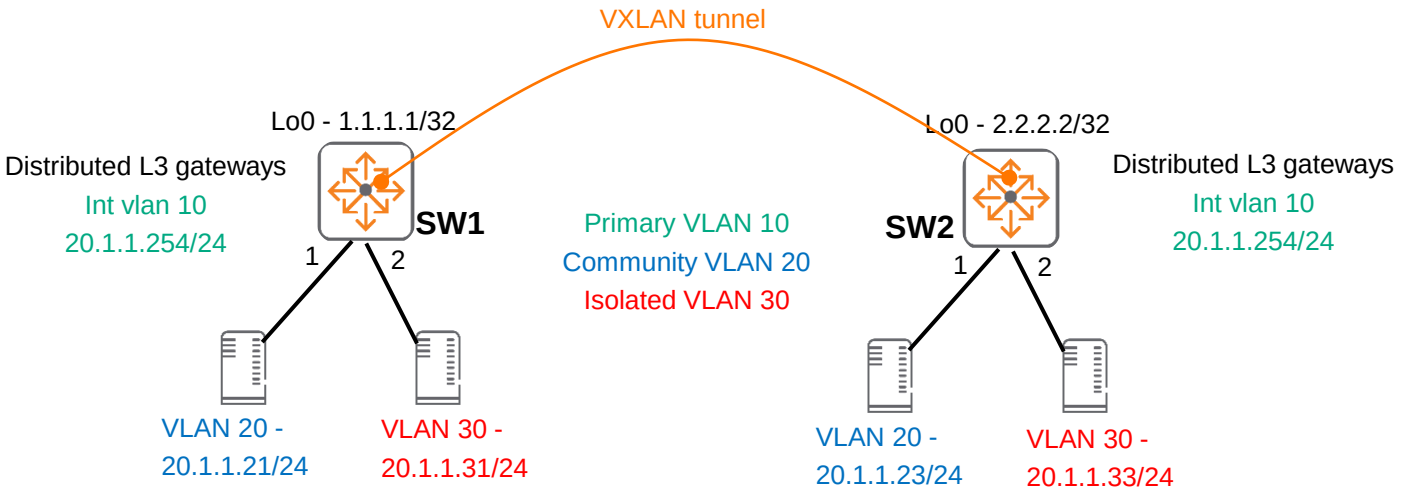
– Packet captures (port mirror) might be required

– Config to mirror traffic

```
mirror session 1
    enable
    destination interface 1/1/40
    source interface 1/1/51 both
```

PVLAN VXLAN Troubleshooting

- Have a topology diagram ready
- Ensure IPs, interface details are included
- Check physical cabling and generate “show tech” when opening a TAC case
- Check network: show LLDP neighbor
- If it’s VXLAN PVLAN: ensure underlay network works using ping and traceroute between loopbacks and interfaces, fix any issues found



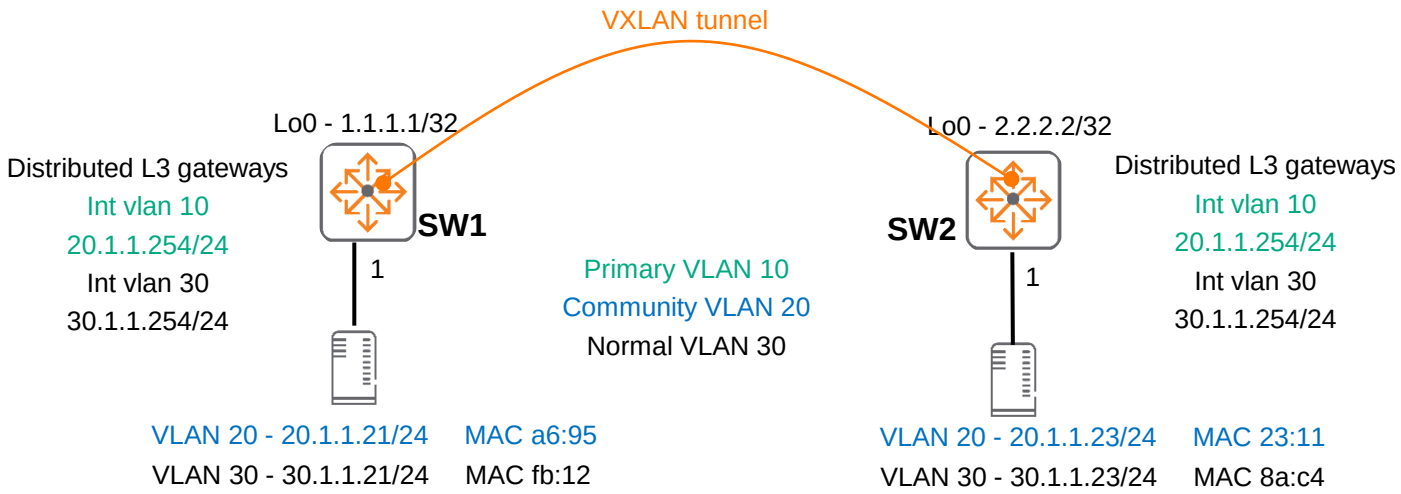
- Recommended troubleshooting flow

1. Check PVLAN configs are correctly configured
2. Verify PVLAN associations
3. Verify PVLAN port-type is correctly configured
4. Verify traffic between hosts are allowed/blocked as expected

Demo

VXLAN PVLAN Demo

- VXLAN PVLAN provides L2 segmentation (IPv4/IPv6 unicast traffic only) between desired hosts on the same subnet
  - Hosts within the same community VLAN have network connectivity
  - Hosts in the isolated VLAN do not have network connectivity with other hosts
  - Hosts are able to reach their default gateway in primary VLAN
  - L3 connectivity between normal VLAN and primary/community/isolated VLANs are not blocked



Thank you

aruba
a Hewlett Packard
Enterprise company