DisNØG 1

Death to FHRP: EVPN in the Wild

Jason R. Rokeach

Hello!

I am Jason R. Rokeach

Solutions Architect @ Juniper

incutio#0179 (Jason)   @JasonRokeach

https://github.com/jrokeach   jasonrokeach

2

Typical Considerations of EVPN

EVPN-VXLAN

Near-ubiquitous technology stack for building a new datacenter

Eliminates STP problems, MC-LAG limitations, VLAN quantity limitations

EVPN-MPLS

Enables [active-active] dual-homing of Layer 2 VPN customer locations

[More] scalable approach to building L2VPNs with reduced operator overhead

Not the purpose of this discussion

EVPN offers tools that we can use in other ways

ESI (VES)

- Enables multihoming - active/active or active/passive
- Marks two interfaces as belonging to the same Ethernet Segment (stops loops!)

Distributed Anycast Gateway

- Enables multiple L3 gateways without FHRP (VRRP/HSRP/GLBP)
- Enables the same L3 gateway in multiple locations, independent of topology.

1 Scenario 1: Internet Gateway Redundancy

Internet Gateway Redundancy

Traditional Model:

- 2 Gateway Routers (GRs) as 1 router cluster
- 2 Agg PEs as 1 router cluster
- GR cluster connected to Agg PE cluster via LAG w/ 802.1Q
- MPLS PW from Acc PE to Agg PE

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON

GW1   GW2

PE1   PE2

Access 1   Access 2   Access 3
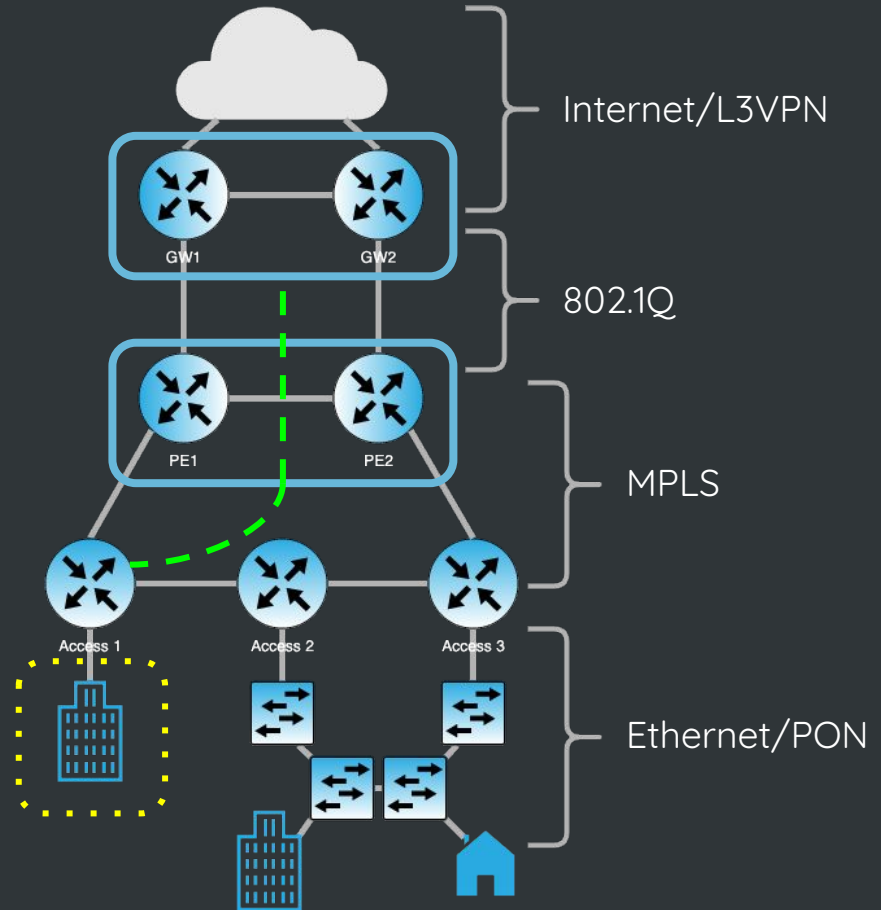
Internet Gateway Redundancy
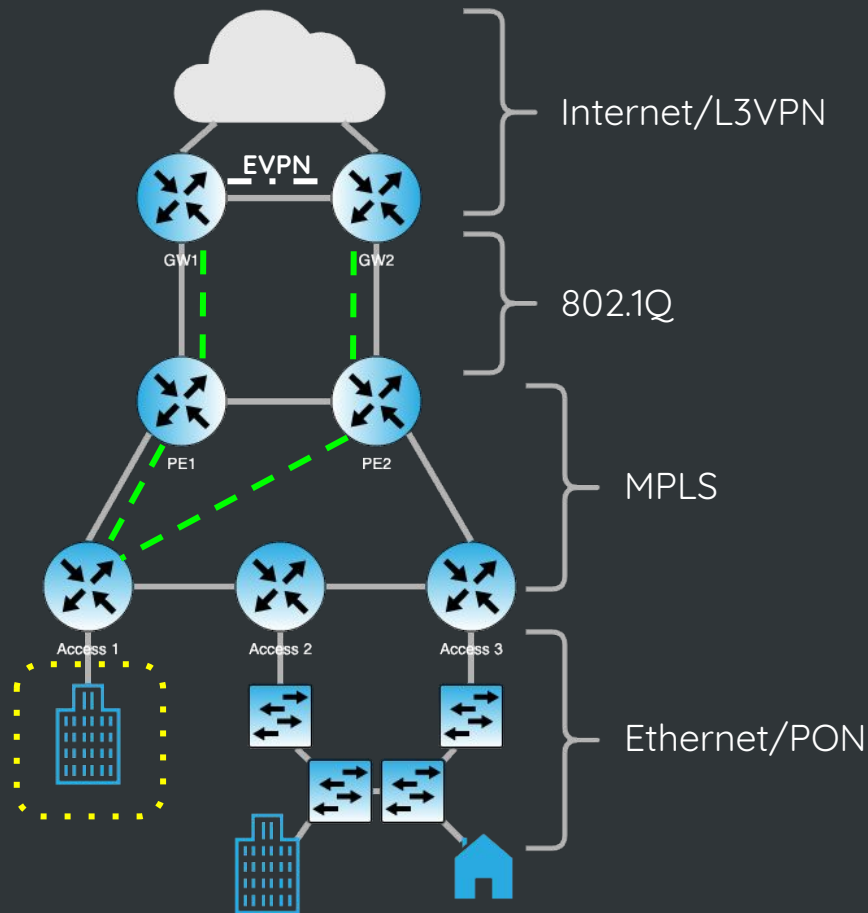
Traditional Model Drawbacks:

- Vendors deprioritizing clustering
- Can be complex
- Requires shared location or additional complexity
- 3 single points of failure
  - *Yes*, your shared control and management planes are SPOFs.

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON
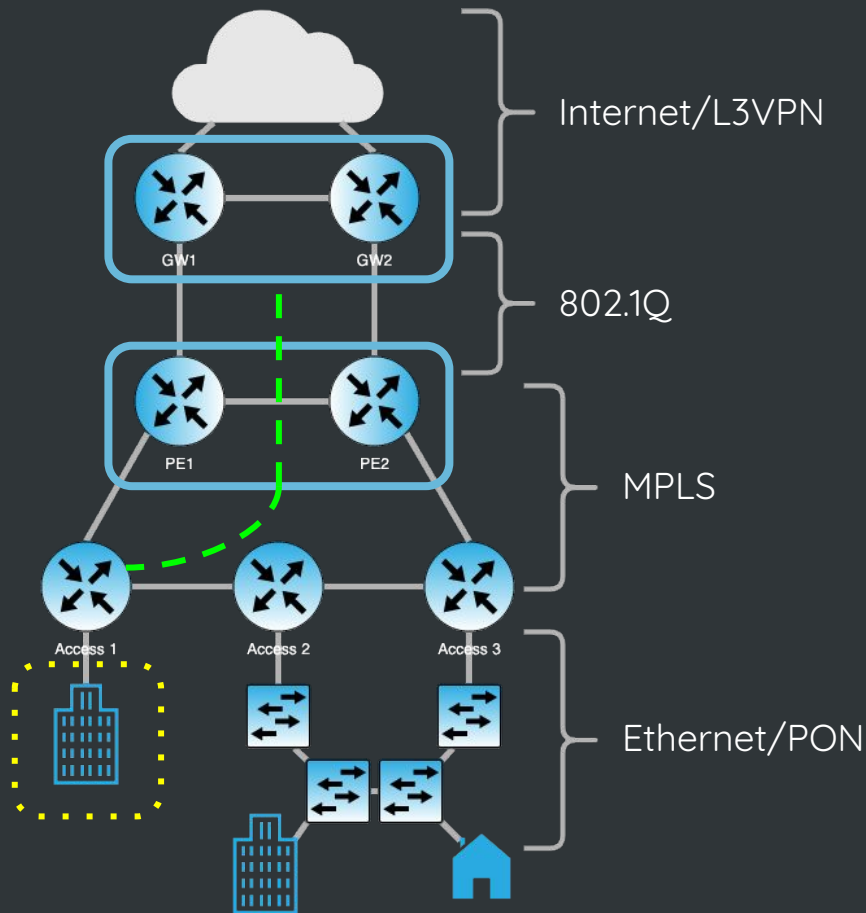
Internet Gateway Redundancy

EVPN Enabled Model:

- No more clusters
- L2VPN/VFI on Acc PE w/ PWs to both Agg PEs
- Both Agg PEs have 802.1Q trunk to respective GW.
- Add BGP w/ EVPN Signalling between GW1 and GW2
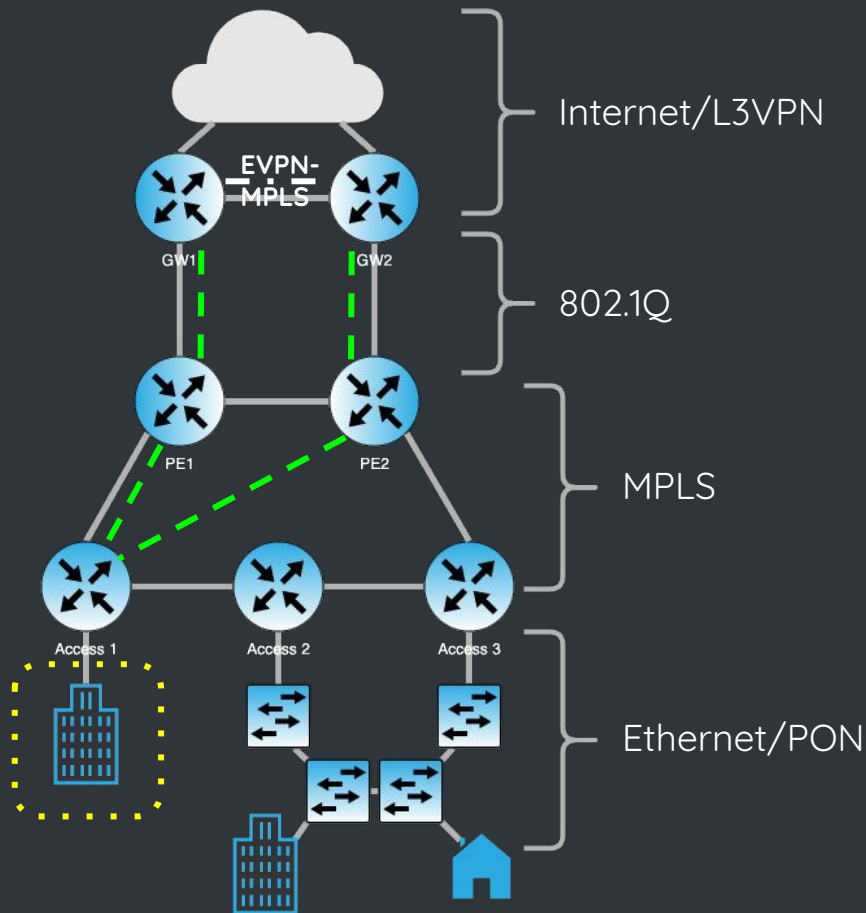- **Distributed Anycast Gateway** on GW1 and GW2

Internet/L3VPN

EVPN

GW1

GW2

802.1Q

PE1

PE2

MPLS

Access 1

Access 2

Access 3

Ethernet/PON

8

Internet Gateway Redundancy

EVPN Enabled Benefits:

- Vendor support
- No more gateway SPOF
- No full-scale EVPN-MPLS deployment in Internet network required.
- No EVPN requirement in MPLS network

EVPN Enabled Drawbacks:

- Shaping/Policing becomes problematic in active/active case.
 - Mitigate this with single-active ESIs.

Internet/L3VPN

EVPN-MPLS

GW1   GW2

802.1Q

PE1   PE2

MPLS

Access 1   Access 2   Access 3

Ethernet/PON

2 Scenario 2: Stateless Access Ring Redundancy

Stateless Access Ring Redundancy

~~Traditional~~ Old Model:

- GWs may use FHRP, be a single router, or *use EVPN DAG such as in Scenario 1.*
- No L2 loop prevention on switches
- Switch ring dual linked to SPOF access PE
- Access PE runs single-node STP which causes blocking on a port when it sees its own BPDU

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON

11
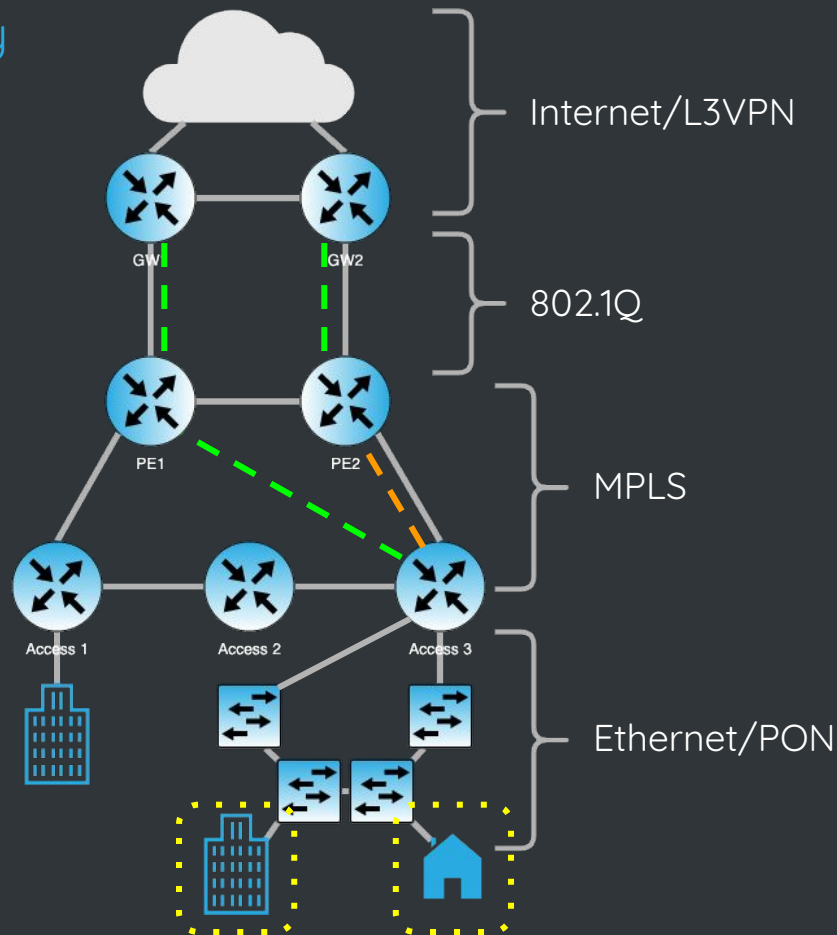
Stateless Access Ring Redundancy

~~Traditional~~ Old Model Drawbacks:

- Access Router SPOF
- Limits geographical range of rings - all must begin and end at the same physical location

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON

GW

GW2

PE1

PE2

Access 1
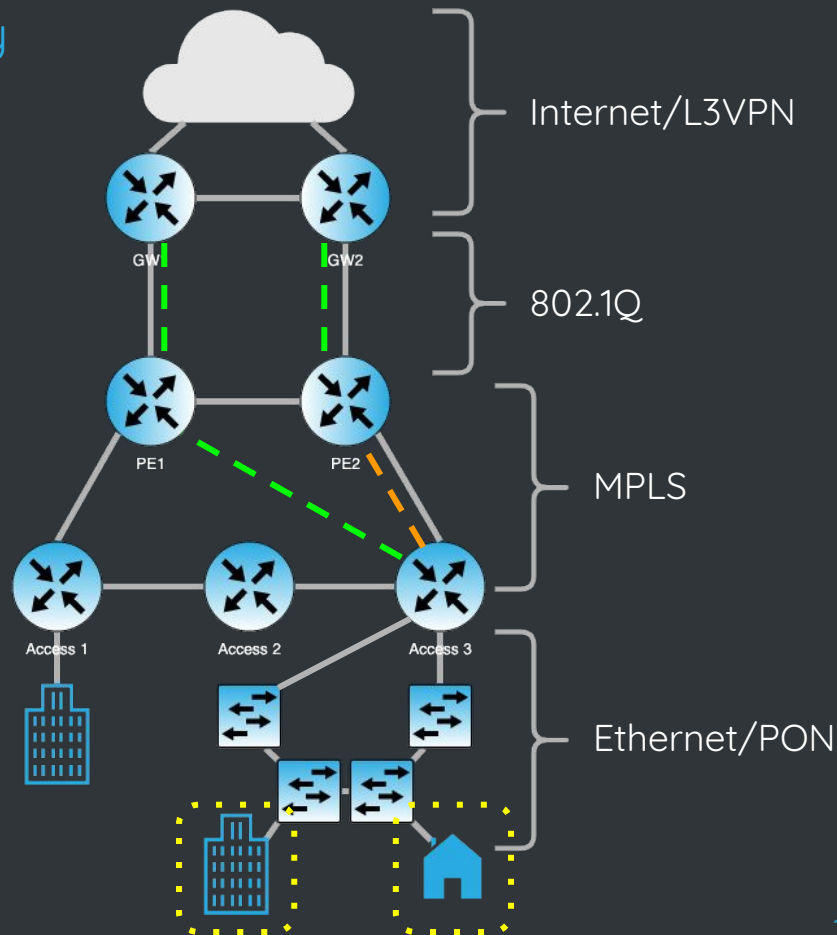
Access 2

Access 3

Stateless Access Ring Redundancy

EVPN-Enabled Model:

- GWs and Switches unchanged
- Switch ring linked to separate Access PEs
- No need for STP on Access PEs
- Access PEs have L2VPN PWs to both Agg PEs. (Or each to one, if VPLS not supported.)
- Agg PEs use VES in single-active mode for each pseudowire

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON

13
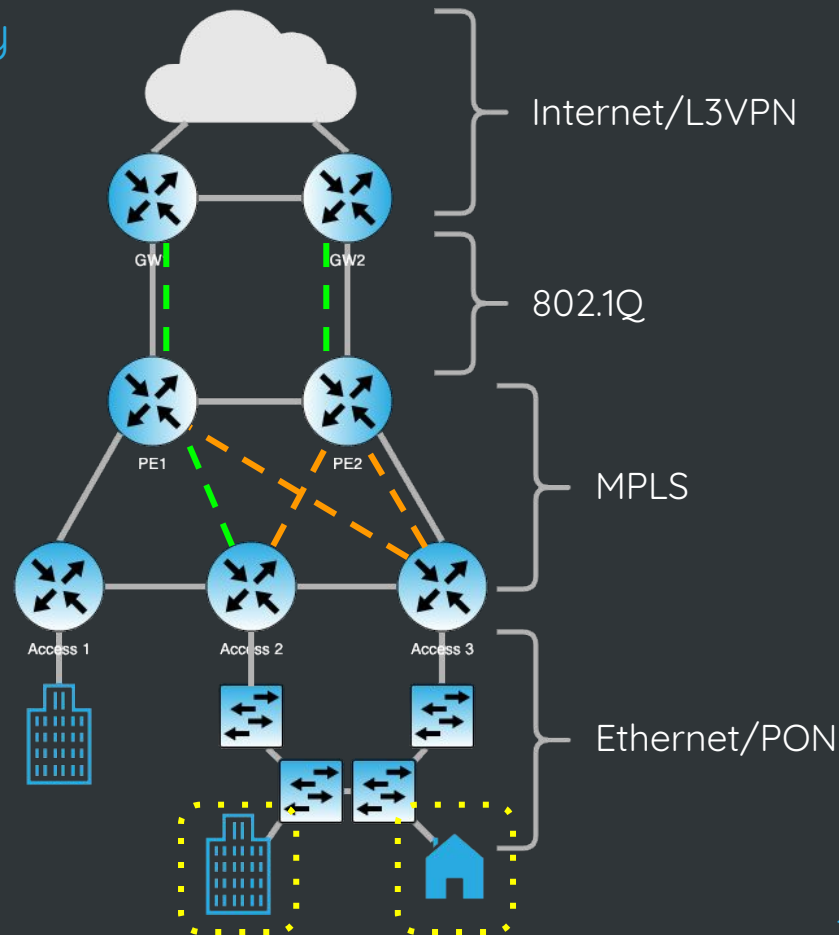
Stateless Access Ring Redundancy

EVPN-Enabled Benefits:

- GWs and Switches unchanged
- No Access PE or switch SPOF for multiple access devices
- Ends of rings can be in separate locations
- No requirement to manage PW failovers and failbacks

Internet/L3VPN

802.1Q

MPLS

Ethernet/PON

14
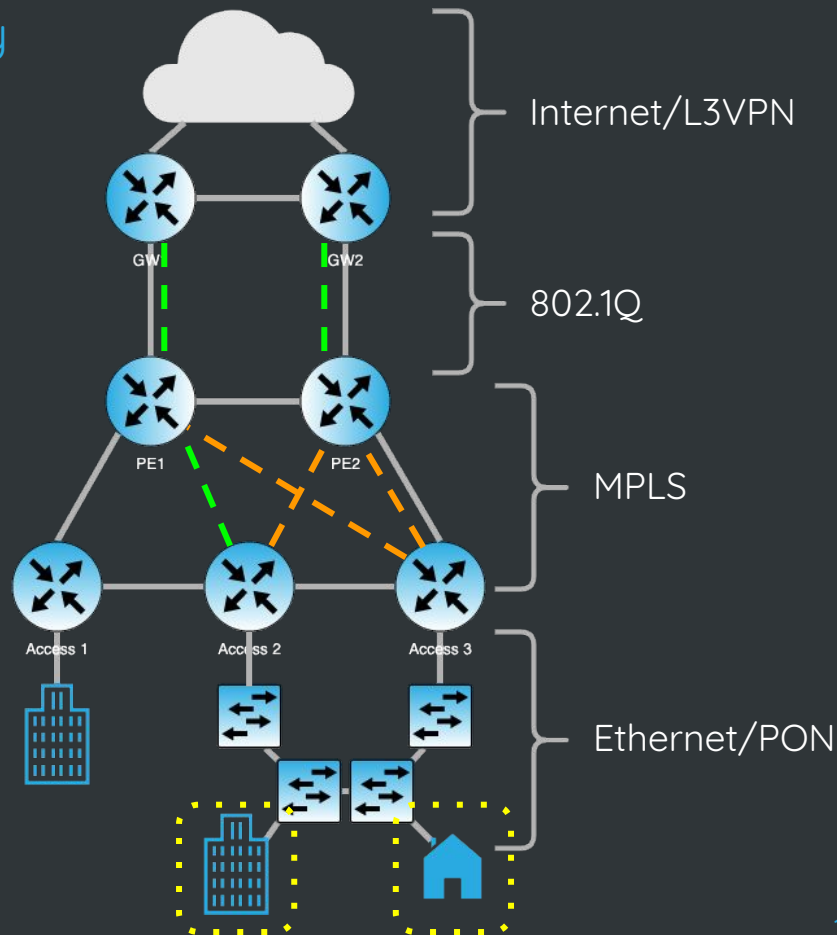
EVPN doesn't just open new L2VPN possibilities, but can and should be used inside your network to enhance other services and simplify operations.

Thank you!

Any questions?

You can find me at:

incutio#0179 (Jason)

@JasonRokeach

https://github.com/jrokeach

jasonrokeach