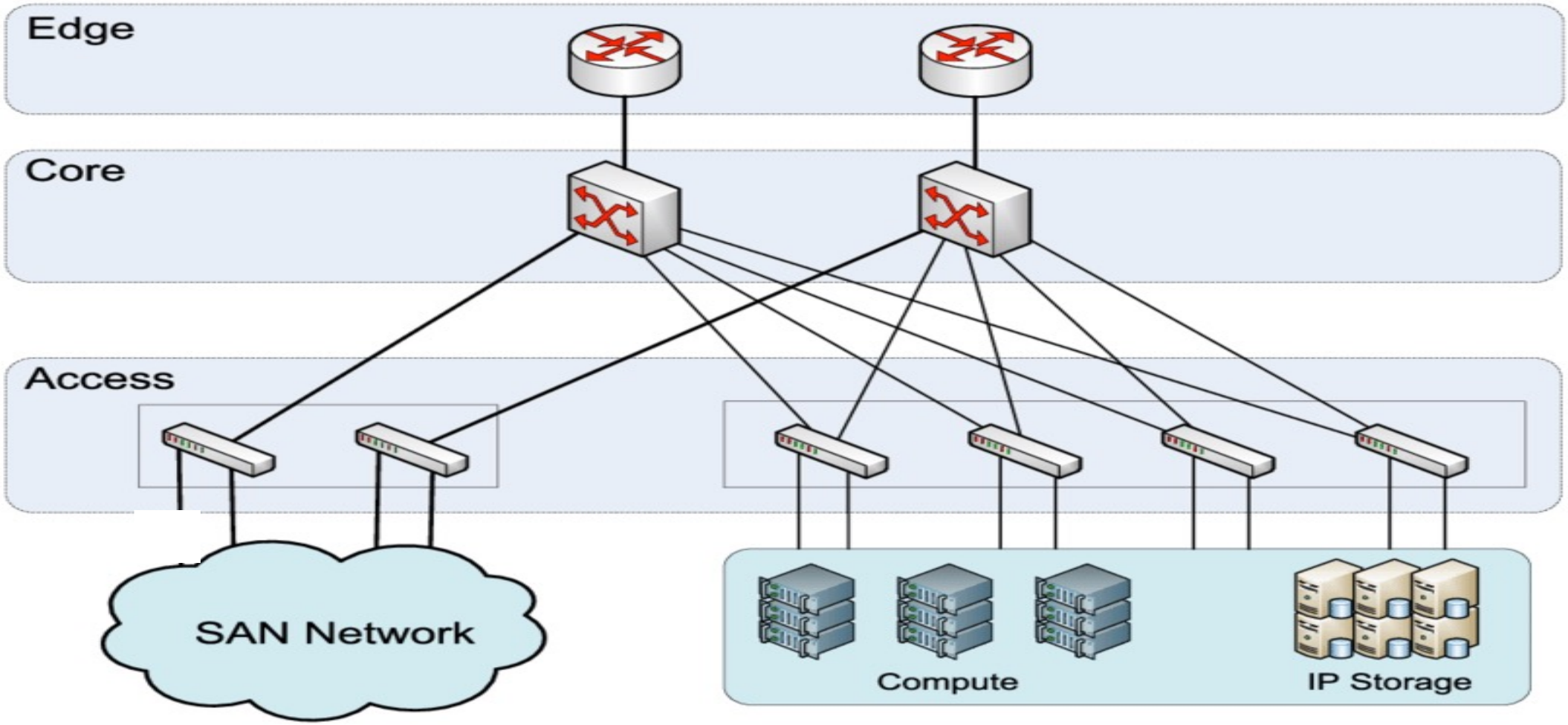
Basics of EVPN

Let’s Learn BGP EVPN Concepts

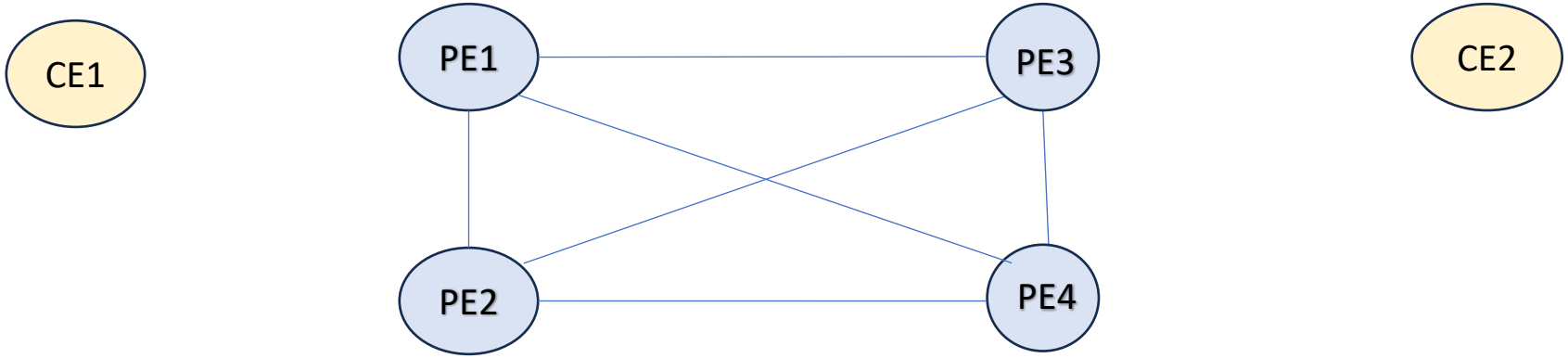
Emergingtechbytes by Sunil Pareek

Let’s Discover Why you should learn BGP EVPN

A View of Network Deployment



Challenges highlighted by Customer



All Active Multi-Homing Missing

Looping of Traffic

Duplicate Frames

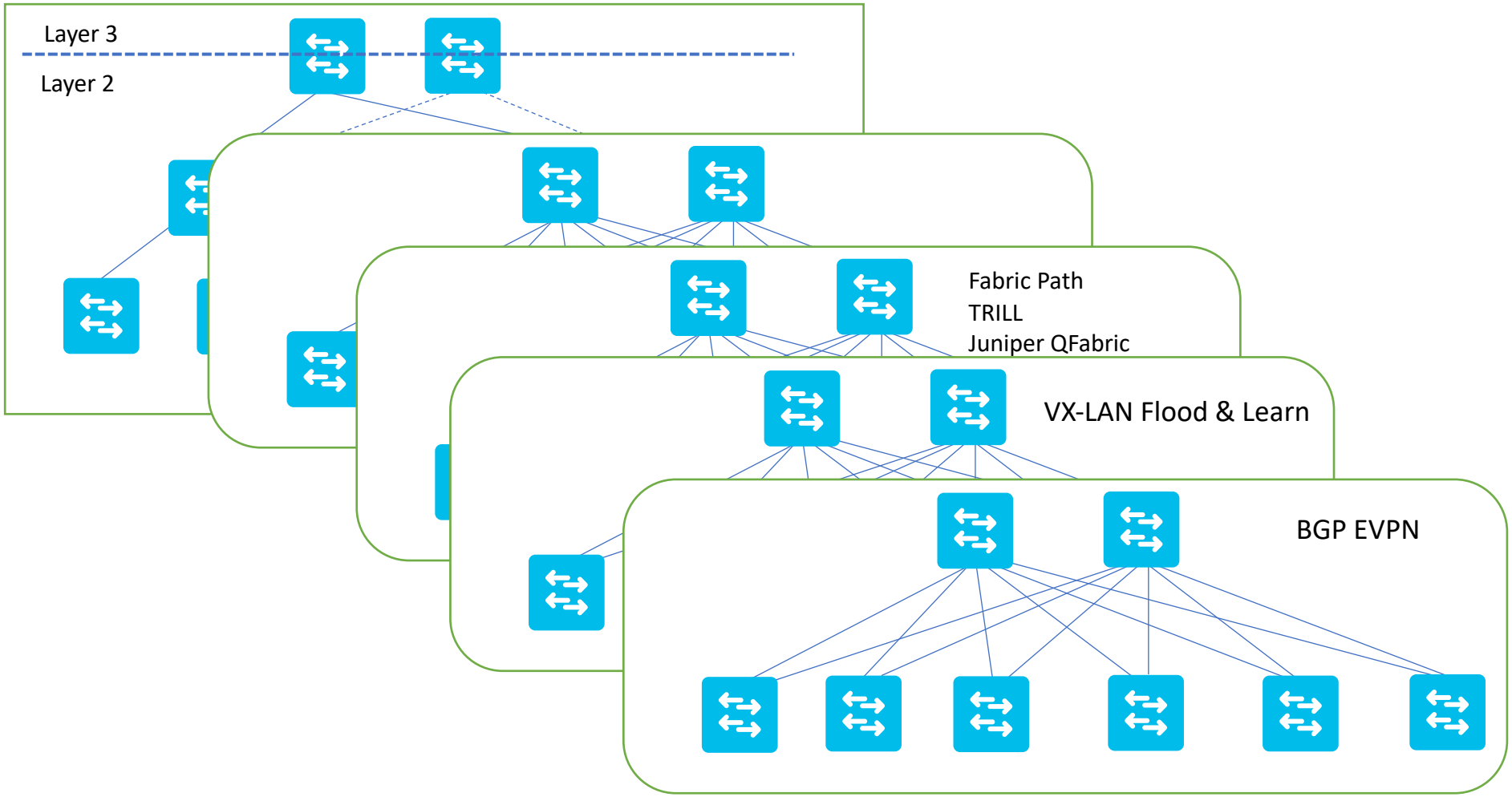
MAC Flaps

Application Ecosystem

- Applications still communicate at layer 2, stringent requirement period!!!
- Newer Applications architecture often uses a micro services architecture where application components are distributed across different servers.
- Applications access stuff at layer 2 and layer 3

Why DATA CENTERS NETWORKS Need EVPN

Data Center Network Evolution

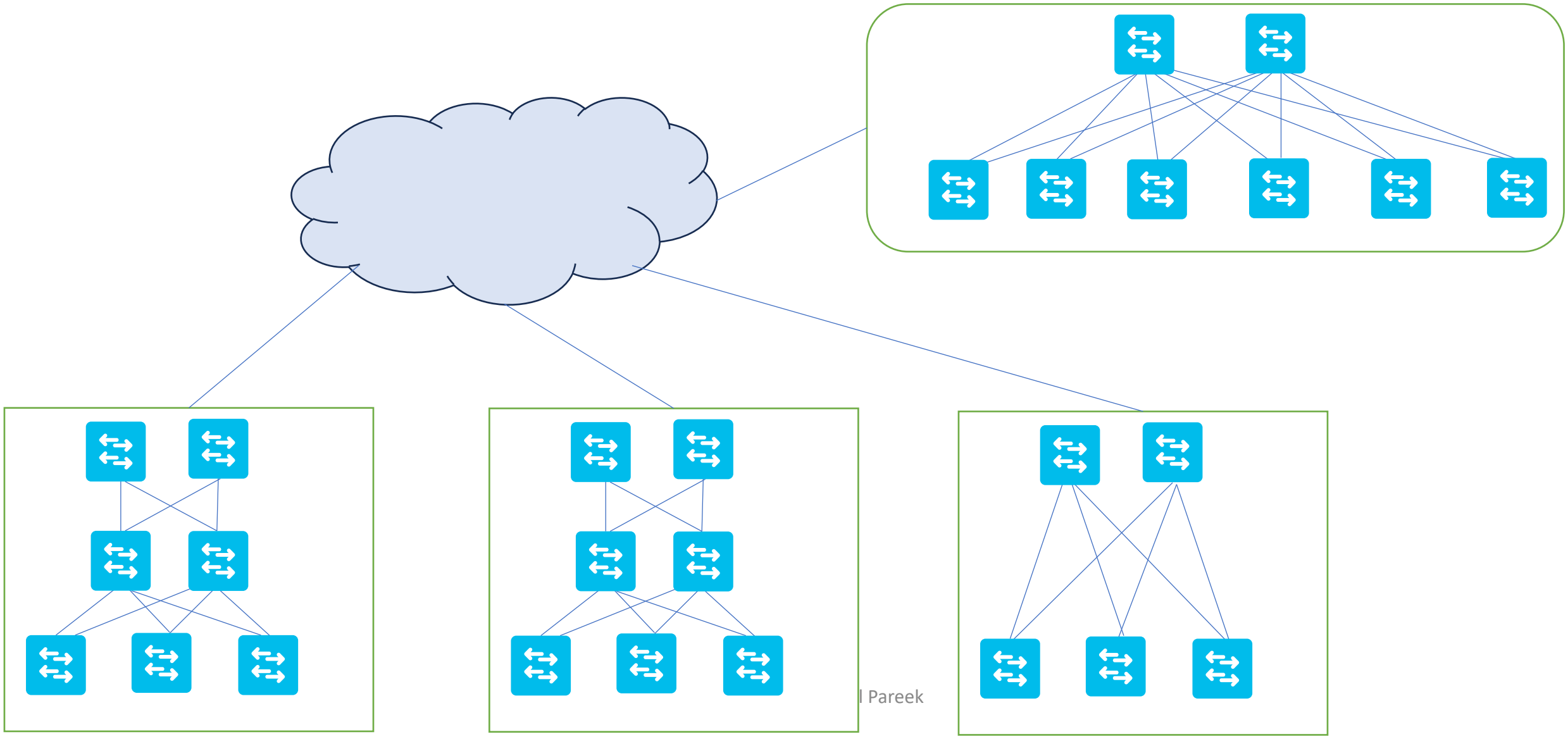


VXLAN with BGP EVPN

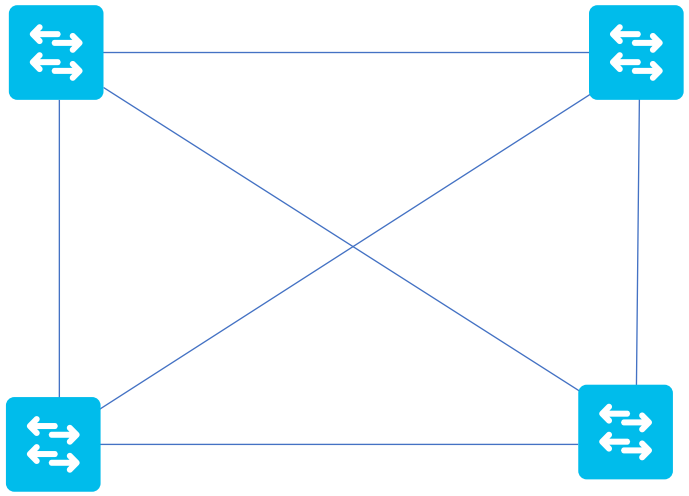
- Layer 2 MAC and Layer 3 IP information distribution by Control plane (BGP)
- Having BGP as Control Plane minimize flooding
- Multi-Tenancy at Scale
- Mobility is being handled by a robust control plane

Why ENTERPRISE CAMPUS NETWORKS Need EVPN

Campus Network Design



Campus Topology



Getting RID of Spanning Tree

- Stacking
- Virtual chassis – VSS/SVL
- vPC/MC-LAG

What about Segmentation, Policies, Mobility

VXLAN with BGP EVPN

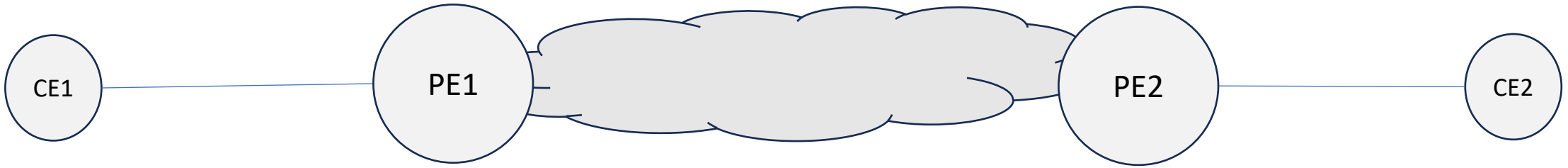
- Layer 2 MAC and Layer 3 IP information distribution by Control plane (BGP)
- Having BGP as Control Plane minimize flooding
- Multi-Tenancy at Scale
- Mobility is being handled by a robust control plane

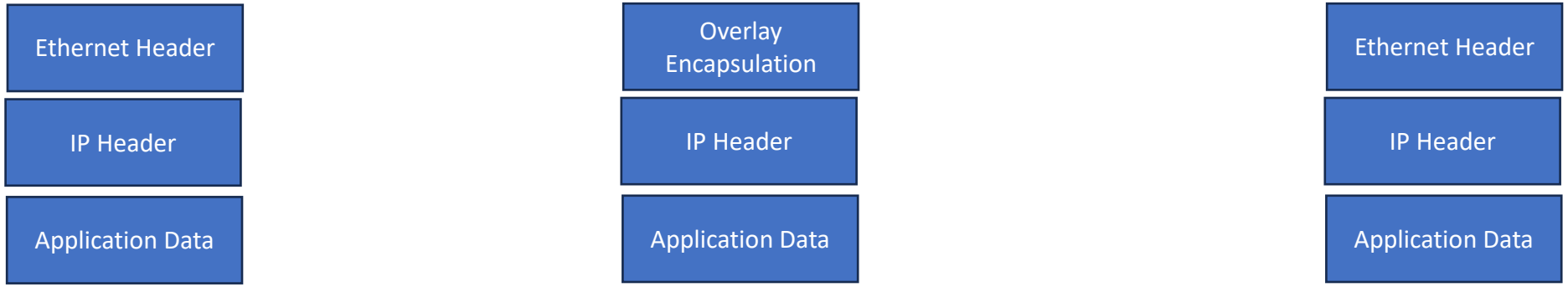
EVPN Drivers for Enterprise

- Industry Standard
- One Fabric Architecture
- Scalable Solution – built on proven BGP
- Flexible design for Overlay networking

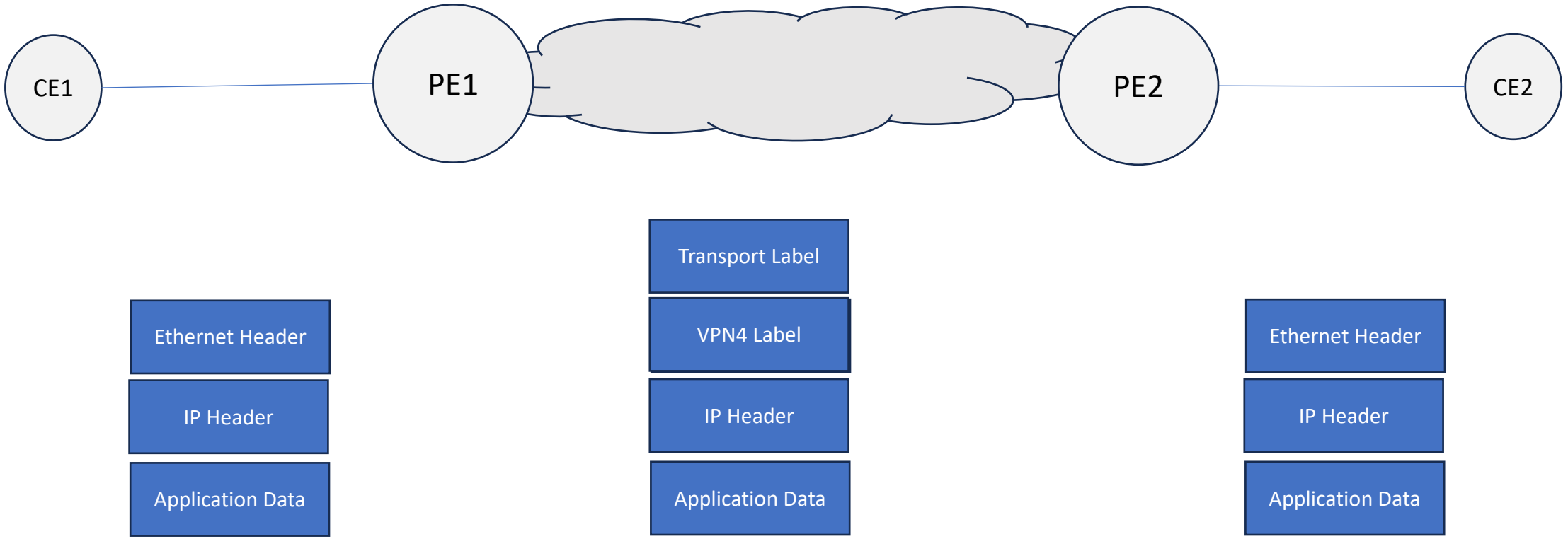
Why SERVICE PROVIDER NETWORKS Need EVPN

Service Overlay for Service Providers

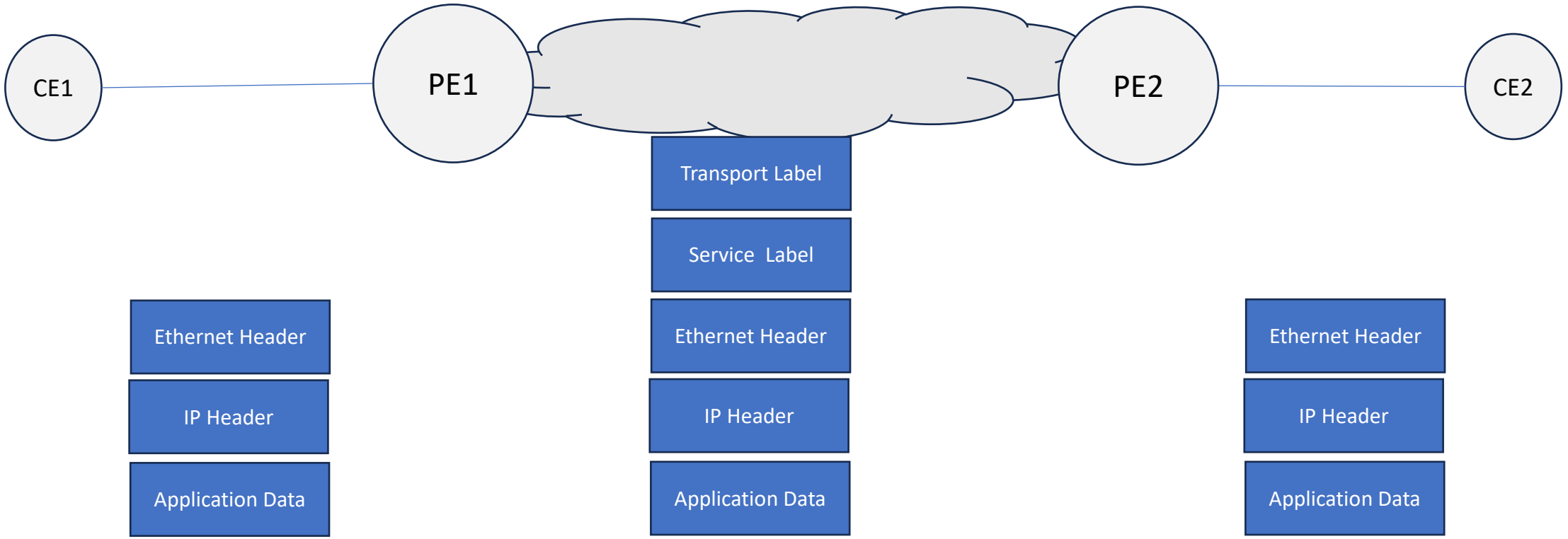




Service Overlay for Service Providers



Service Overlay for Service Providers



Breakdown of Overlay Technologies

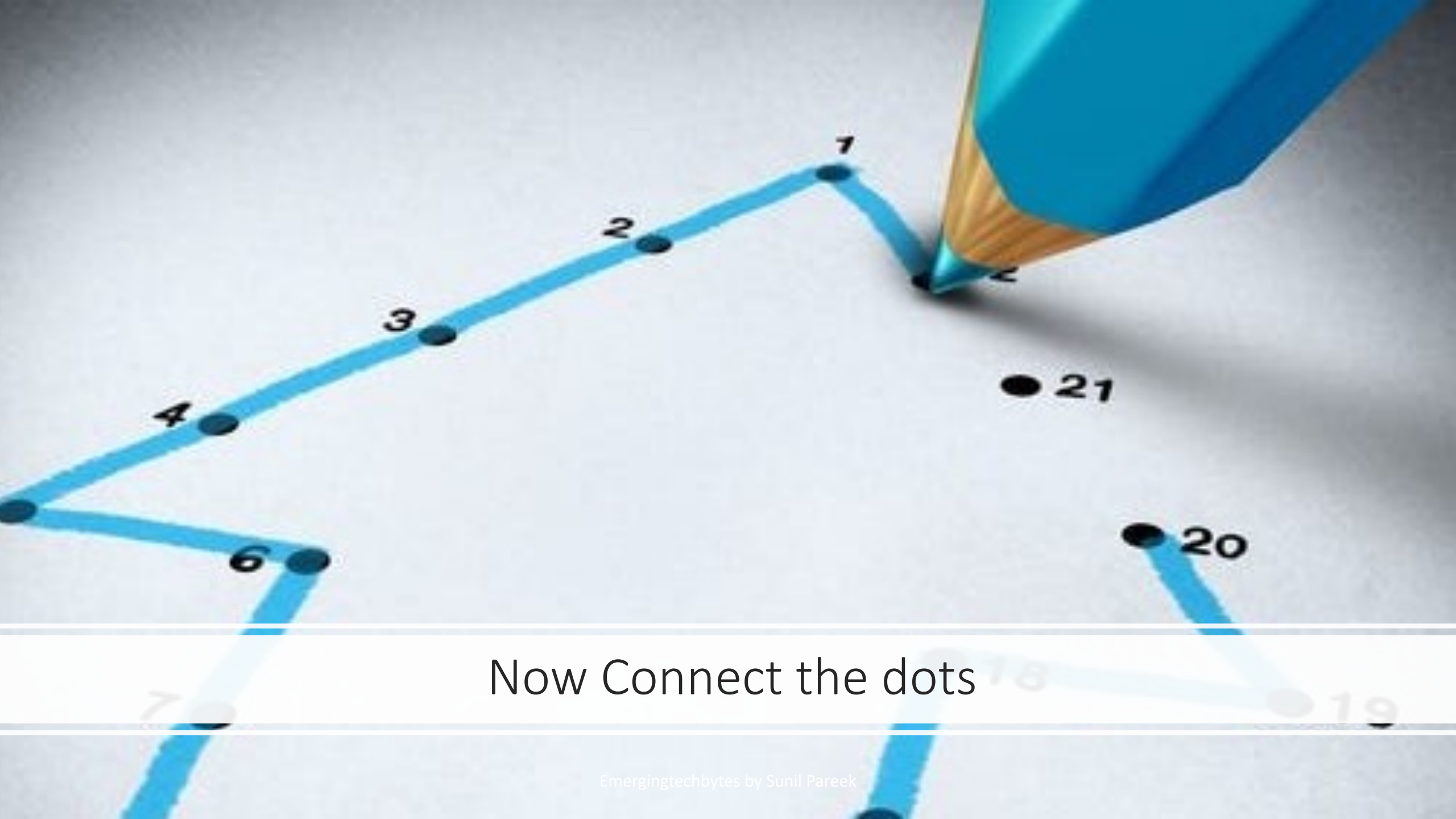
Overlay Services
- Layer 2
- Layer 3

Encapsulation

Underlay Network Transport

Control Plane
- Peer Discovery
- Route Learning and Distribution
  - Local Learning
  - Remote Learning

Data Plane
- Overlay Unicast Traffic
- Overlay BUM Traffic
  - Ingress Replication
  - Multicast
- Multicast Traffic



Now Connect the dots

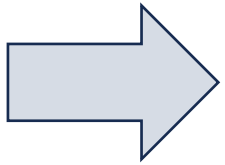
Traditional Network Transition

Layer 2

- Spanning Tree
- IEEE 802.3ad
- VPWS
- VPLS

Layer 3

- Multi-VRF
- Tunneling like GRE
- MPLS VPN



EVPN

From Bridging MAC to Routing MAC

- Integrated Layer 2 and Layer 3 VPN Services
- L3VPN like principles
- All Active Multihoming and load balancing
- Control plane-based learning
- Optimized Broadcast, unknown unicast and multicast traffic delivery
- Choice of data plane
- Industry standard

From Bridging MAC to Routing MAC

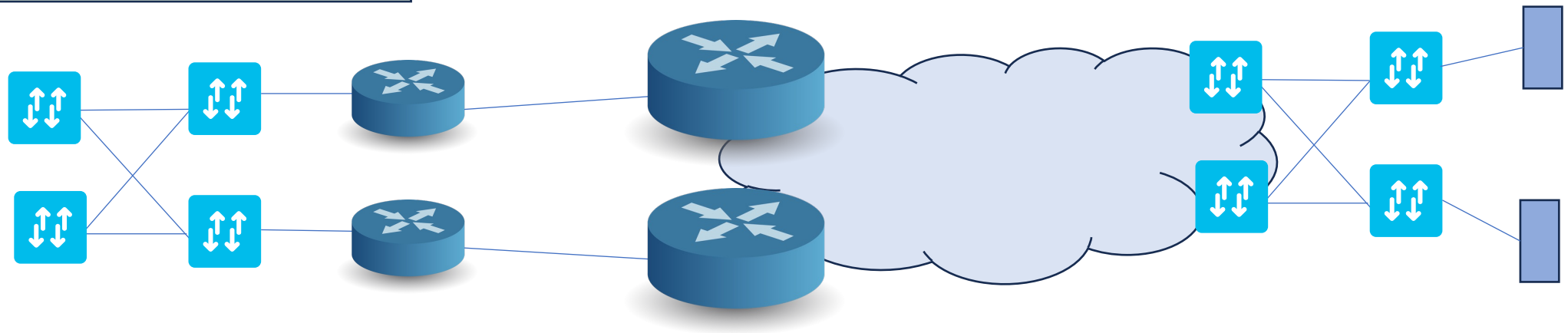
BGP EVPN, SDA

Layer 2, IP, IPv6

Common Control Plane
BGP EVPN, VPNv4/v6

Segment Routing
(MPLS/SRv6)

Segment Routing
(MPLS/SRv6) VXLAN



Hierarchical Network, Routed Access

Layer 2, IP

BGP : VPNv4/v6
LDP: VPLS, PW

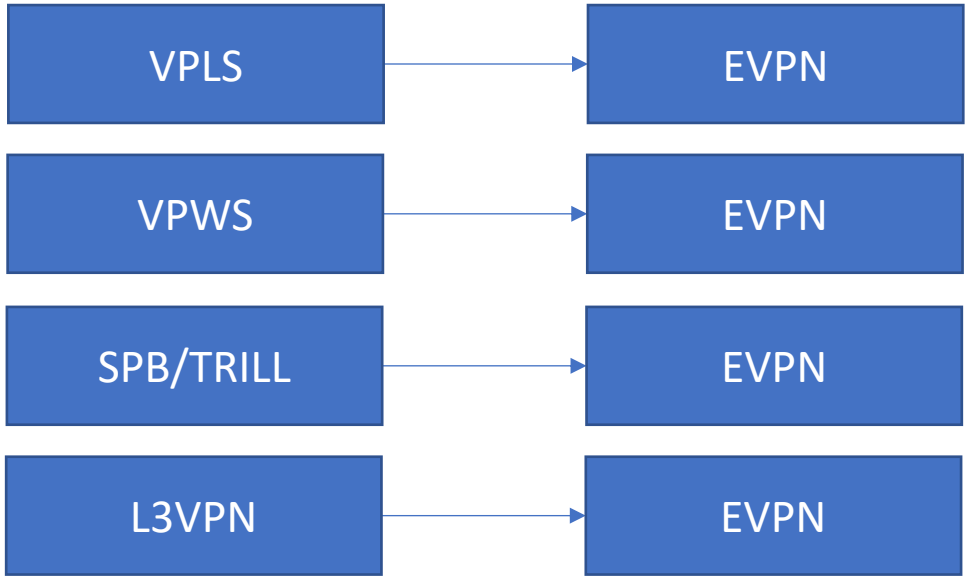
MPLS: LDP, RSVP-TE

Fabric Path,
TRILL

Layer 2, IP

🤔 that is it or can you further simplify

EVPN – What's the Big Deal about this



Key Message here is that **EVPN** not only does the Job of many legacy VPN technologies, but it does It better than each one of them.

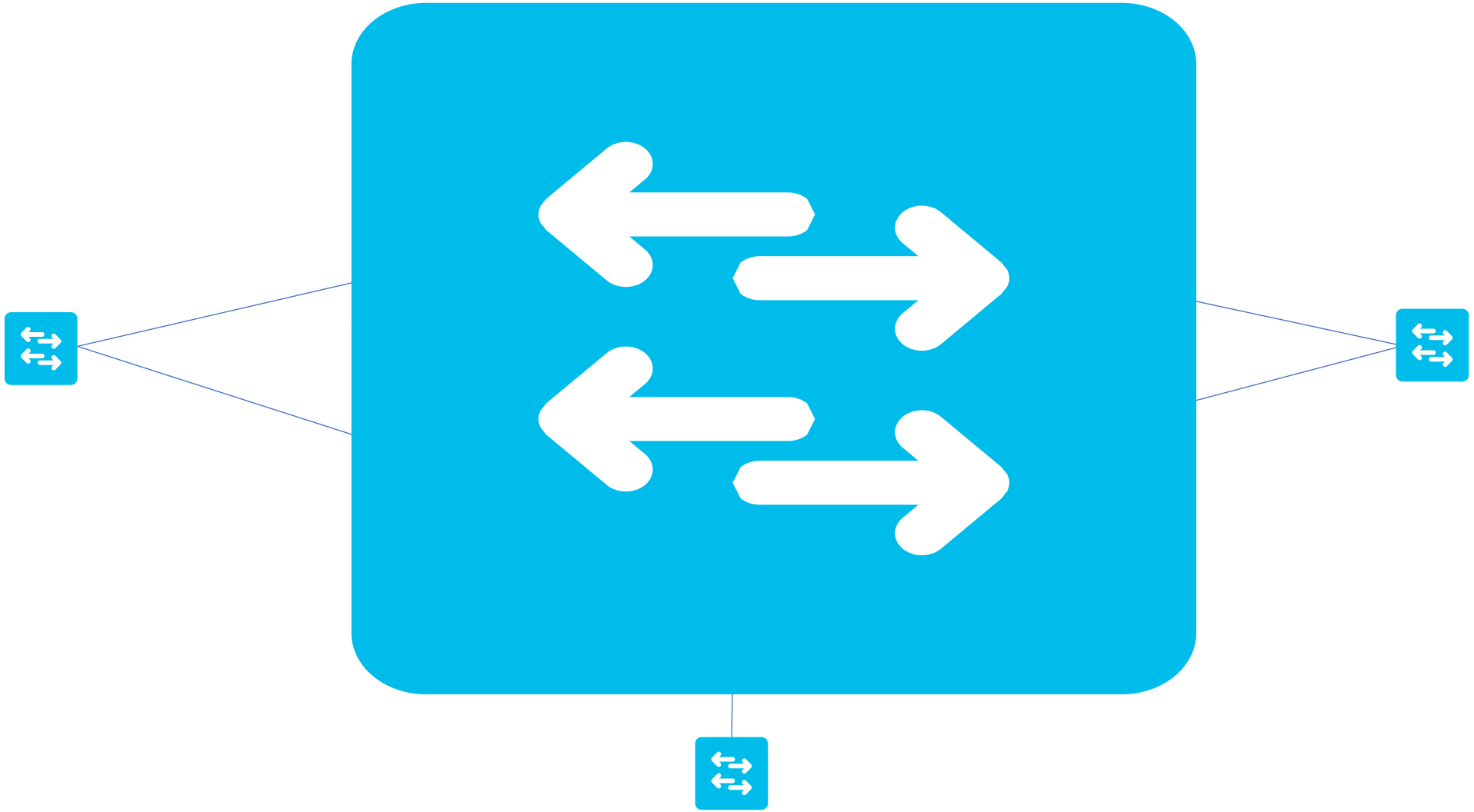
Not to forget – Data Center Interconnect, Data Center Overlay

Let’s Understand VPLS and Issues related to it

Thought Process behind VPLS

- VPLS was the result of obvious evolution of take-anything-over-MPLS idea
  - The process started with P2P transport over MPLS LSPs.
  - LAN Emulation was the next logical step

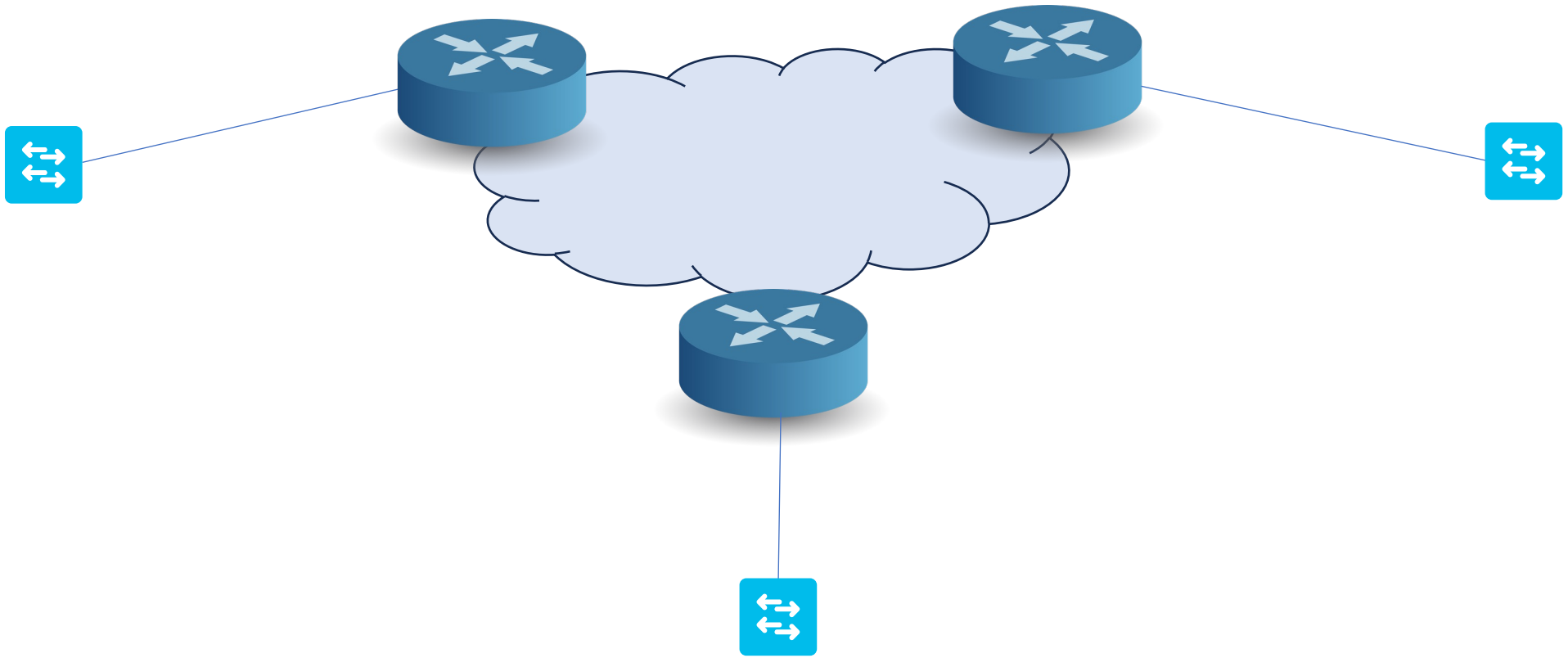
Let’s Understand VPLS First



What is VPLS

- For End Customers, VPLS just looks just like an Ethernet Switch.
  - VPLS creates a big virtualized data switch at the Service Provider which links multiple remote sites together as if they were connected to a same physical switch.
- Hence this solution can suffer from the same issues that a Layer 2 Network is susceptible to.

Let’s Revisit our Understanding on VPLS




Distributing a
MAC Address
Learning a
MAC Address

Learning the Reachability Information

Distribution of Reachability Information

EVPN Does Exactly this

VPLS vs EVPN

- Technically, there's no similarity between EVPN and VPLS
- Apart from the fact that they're trying to solve the same problem.

For me, EVPN is One love and One pain

BGP EVPN Route Types

1. Ethernet Auto-Discovery (A-D) route
2. MAC/IP Advertisement Route
3. Inclusive Multicast Ethernet Tag Route
4. Ethernet Segment Route
5. IP Prefix Route

Thank You

Basics of EVPN – Let’s Learn Network Virtualization and Overlay Networking Fundamentals

Emergingtechbytes by Sunil Pareek

Agenda

- Network Virtualization Journey
- Let's scratch the surface of VXLAN
- Building blocks of EVPN – Optional for Today

Network Virtualization Journey

Server Virtualization vs Network Virtualization

Server virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application. Each virtual server can run its own operating systems independently.

Network Virtualization is carving up a physical network into multiple virtual networks.

Virtualized Tunnels are formed across underlay networks

Overlay Network Services

- Earlier Overlay services are normally offered as layer 2 or as layer 3.
- Modern Overlay provide both layer 2 and layer 3 services.
- Original Packet means a Layer 3 packet or Original Frame means a Layer 2 frame, can be encapsulated into another packet (Layer 3) or another frame (Layer 2).
- In Network overlay, Outer packet can be a layer 2 packet or a layer 3 packet.

Types of Virtual Network

- Virtual Networks can be classified as follow:
  - first is the way in which an ingress node decides to associate a packet with a virtual network.
  - The second is whether transit nodes in a network path are aware of virtual networks.

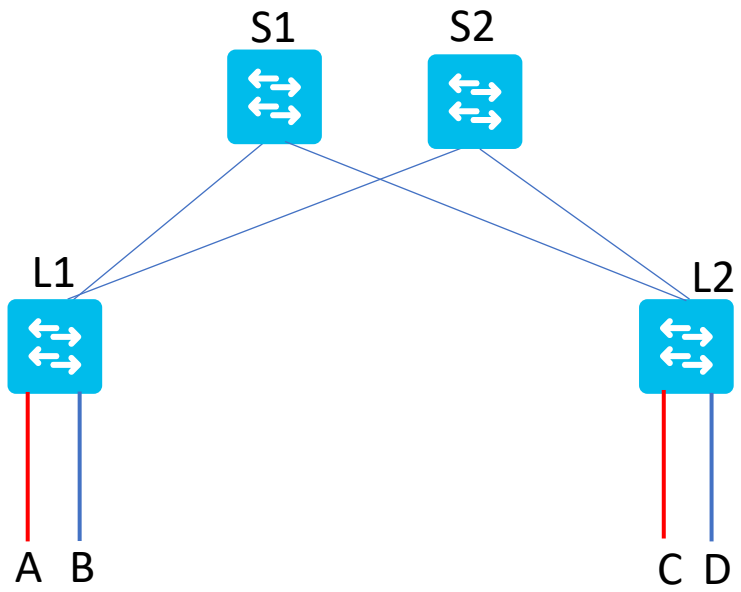
Network Overlay - Definition

- An overlay is a static or dynamic tunnel that runs on top of a physical network infrastructure.
  - MPLS- and GRE-based encapsulations are some well-known examples
  - Some more like IPsec, 6to4, L2tpv3…

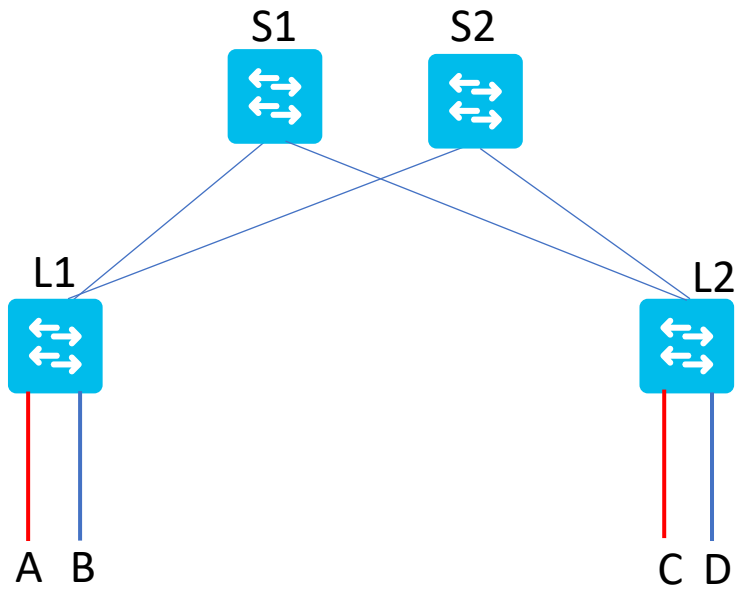
Underlay Networks

- With Overlay Network Services defined, underlying transport network which carries overlay packets or frame, is required
- Provisioning of underlay depends on overlay encapsulation.

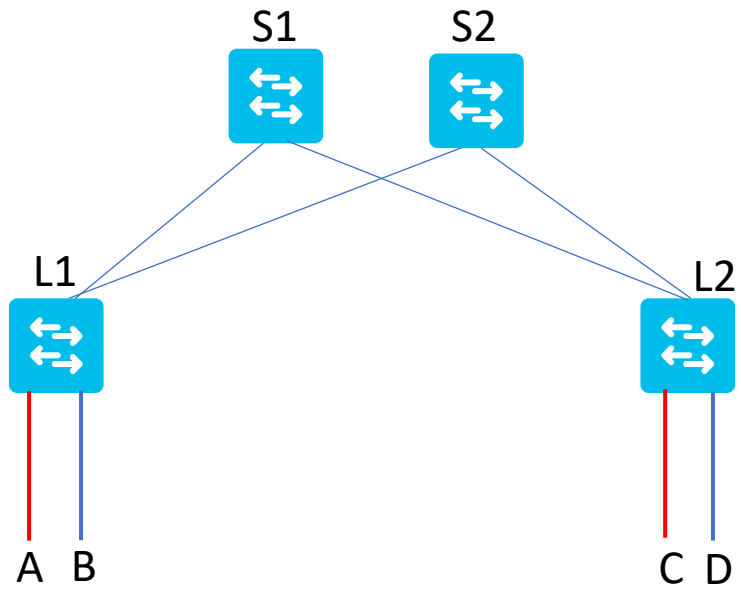
Different Network Overlay Topology



Network Overlay

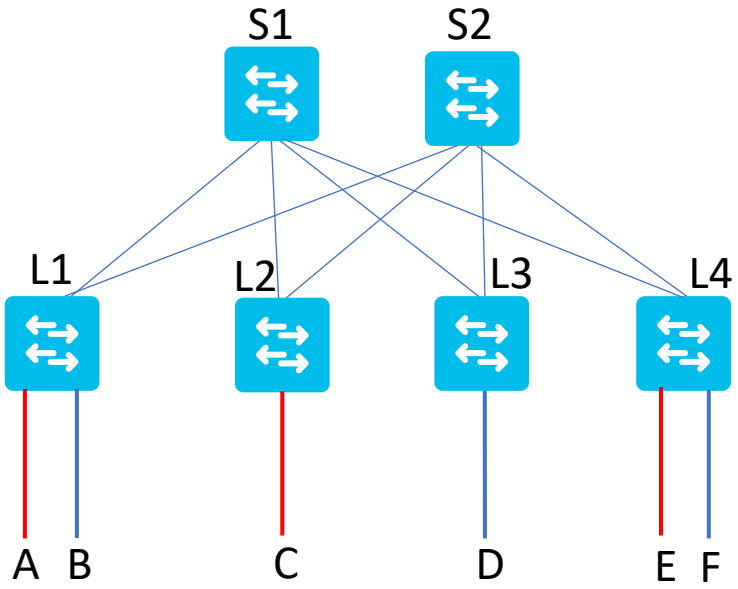


Host Overlay



Hybrid Overlay

Overlay Networking Features

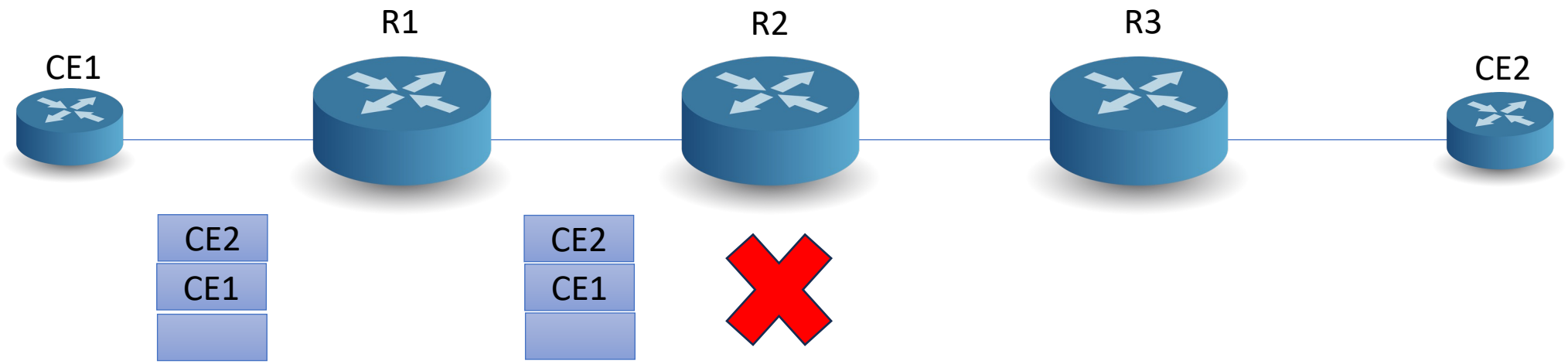


Too Much Overlay

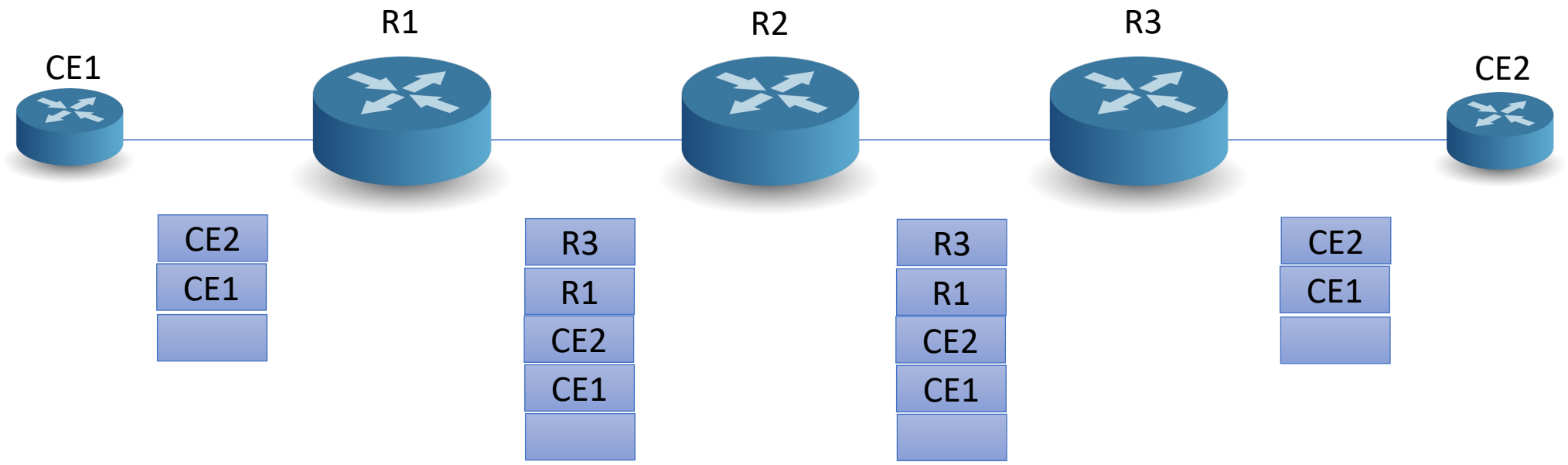
Overlay Networking Features

- A Control plane method is needed to know which end hosts are behind which overlay edge devices.
- Mapping of end-points to overlay edge devices is maintained and known as location identity mapping data base.

Overlay Network Forwarding



Overlay Network Forwarding



Network Virtualization - Role of EVPN

- Ethernet VPN (EVPN) is a technology for connecting Layer 2 network segments which are separated by a Layer 3 network.
- This is done by constructing a virtual L2 network over the underlying L3 network.

How do virtual networks cope up with overlapping address spaces?

- Network addresses must be unique only in a connected network. Consider postal addressing. A common model for a postal address is to use street address, the city, the state, and maybe the country.
  - Within a city there can be only a single location that is addressed as 133 Heritage County. Similarly, within a state, you can have only one city called Bengaluru, and within a country there is one state called as Karnataka.
  - The uniqueness of an address is specific to the container it is in.

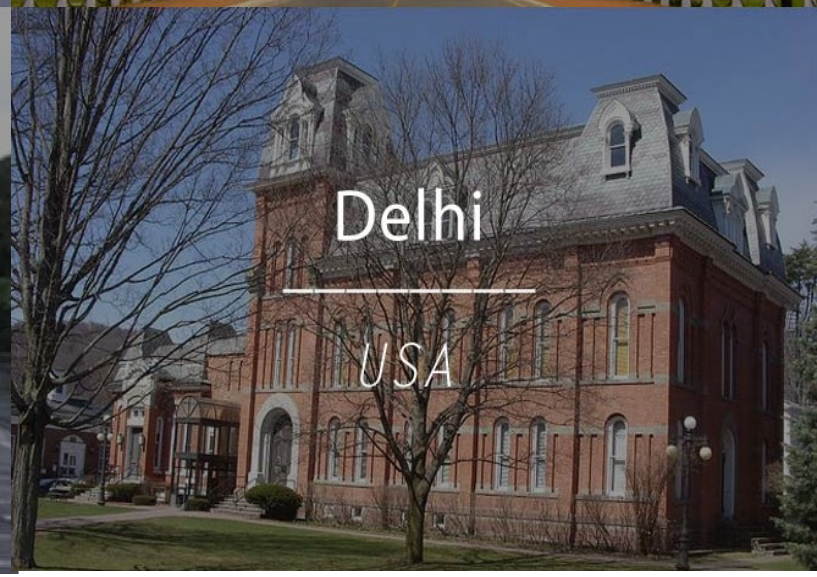

Kochi
Kerala


पटना जंक्शन
PATNA JUNCTION
Patna
Bihar


Delhi
India


Kochi
Japan


East Ayrshire
PATNA
Please Drive Carefully
Patna
Scotland


Delhi
USA

How do virtual networks cope up with overlapping address spaces?

- On the same lines, a MAC address needs to be unique only in a connected L2 network, typically one customer environment.
- Same way, An IP address needs to be unique only within a Layer 3 network.

Benefits of Overlay Virtual Network

- The primary benefit of virtual network overlays over non-overlays is that they scale much better. Because the network core does not have to store forwarding table state for the virtual networks, it operates with much less state.
- The second benefit of overlay networks is they allow for rapid provisioning of virtual networks. Rapid provisioning is possible because you configure only the affected edges, not the entire network.

Payload for Virtual Networks

- Virtual Networks are provisioned in some form of tunnels
- The tunnel header can be constructed using an L2 header or an L3 header.
  - L2 tunnels
    - double VLAN tag (Q-in-Q or double-Q),
    - TRILL,
    - Mac-in-Mac (IEEE 802.1ah).
  - L3 tunnel
    - VXLAN,
    - IP Generic Routing Encapsulation (GRE)
    - Multiprotocol Label Switching (MPLS)

The Consequences of Tunnelling

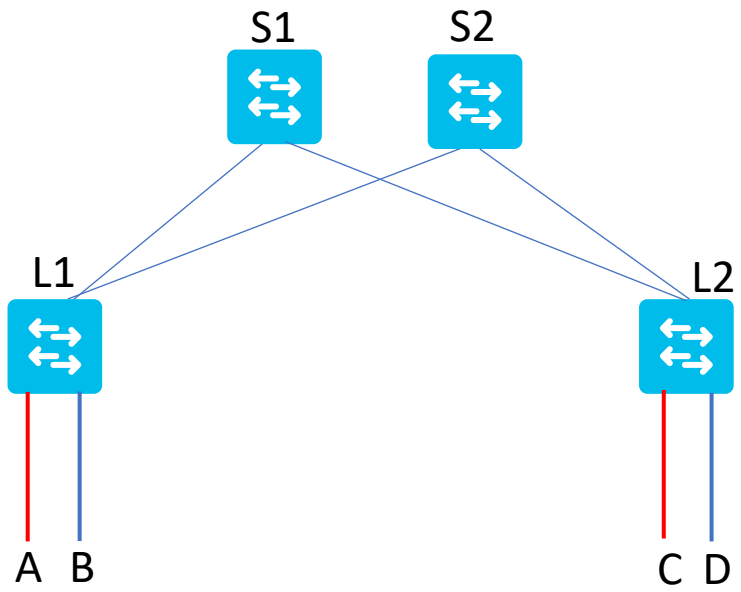
- Load Balancing
- Server NIC issues
- MTU issues
- Lack of Visibility

Let’s Understand VXLan

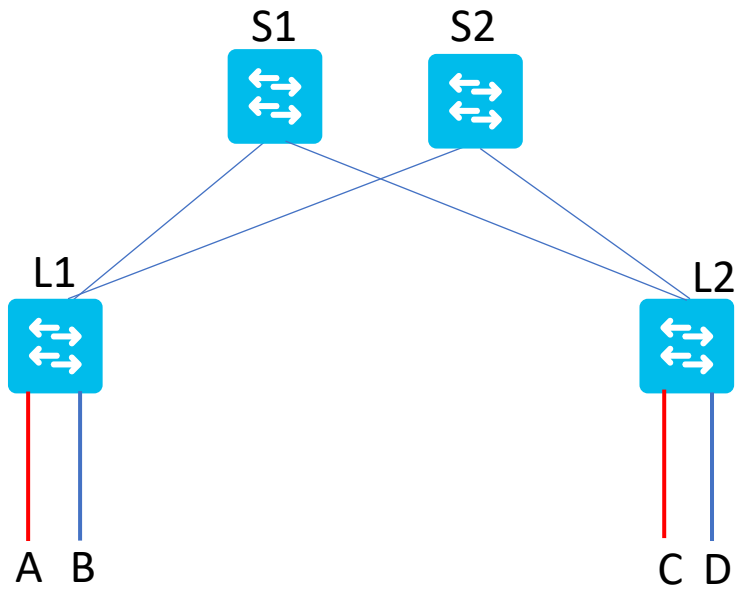
Let’s Introduce VXLAN

- VXLAN is a relatively new tunnelling technology designed to run over IP networks while providing mainly L2 connectivity to the connected endpoints.

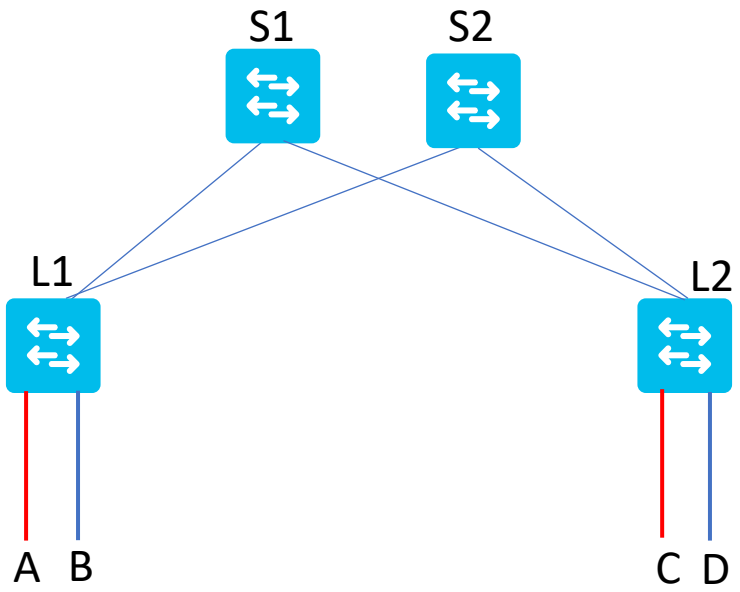
Let’s Revisit Overlay Topology



Network Overlay



Host Overlay



Hybrid Overlay

Thought Process behind VXLAN

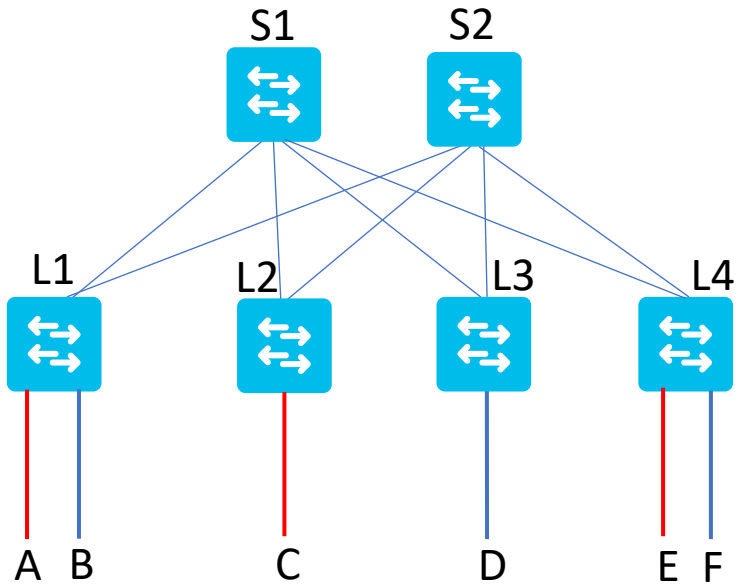
- VXLAN was designed to allow compute nodes to be the NVEs, with Network being a simple IP based forwarder.
- Initially, Multiple software vendors signed up to provide such a solution. You may recall such solutions include VMWare's NSX, Nuage Networks.
- In fact, Originally Networks running VXLAN were proposed as Software-Defined Network (SDN)

Thought Process behind VXLAN

- An alternate approach to this SDN solution was to rely on traditional networking protocols such as Border Gateway Protocol (BGP)

Ideal Ask from the Control Plane

- Some mapping mechanism for the destination address of inner payload to the correct egress NVE's address.
- A mechanism to allow NVE's to convey the virtual networks it is interested in, to allow point-to-multipoint communication such as broadcast.



Building Blocks of BGP EVPN

BGP EVPN Building Blocks

- Border Gateway Protocol (BGP) is the **control plane** that drives Ethernet VPN (EVPN). Enhancement were introduced as a part of this:
  - BGP Peering Model,
  - Address-family for exchanging routing information

BGP Address Family Indicator/Subsequent Address Family Indicator

- The AFI/SAFI list that is configured on a BGP speaker will be advertised using BGP Capabilities in the BGP OPEN message.
- Two BGP peers will exchange information about a network address only if both sides advertise an interest in its AFI/SAFI.
  - EVPN is designed as a SAFI family of the L2VPN AFI.

Route Distinguisher

- When exchanging VPN addresses, BGP prepends an 8-byte RD to every address. This combination of RD + address makes the address globally unique.
- As we have seen, Virtual networks allow the reuse of an address. By appending the RD, we are making addresses unique.

Route Target

- A mechanism to allow NVE’s to convey the virtual networks it is interested in

Route Types

- In BGP, UPDATE messages carry reachability information for configured address-family
- This reachability information is encoded in Network Layer Reachability Information aka NLRI.


BGP
Any Encapsulation
Multicast
Network Virtualization
Switching Fundamentals
E
V
P
N

Basics of EVPN – Let’s Learn VXLAN Concepts and Packet Forwarding

Emergingtechbytes by Sunil Pareek

Agenda

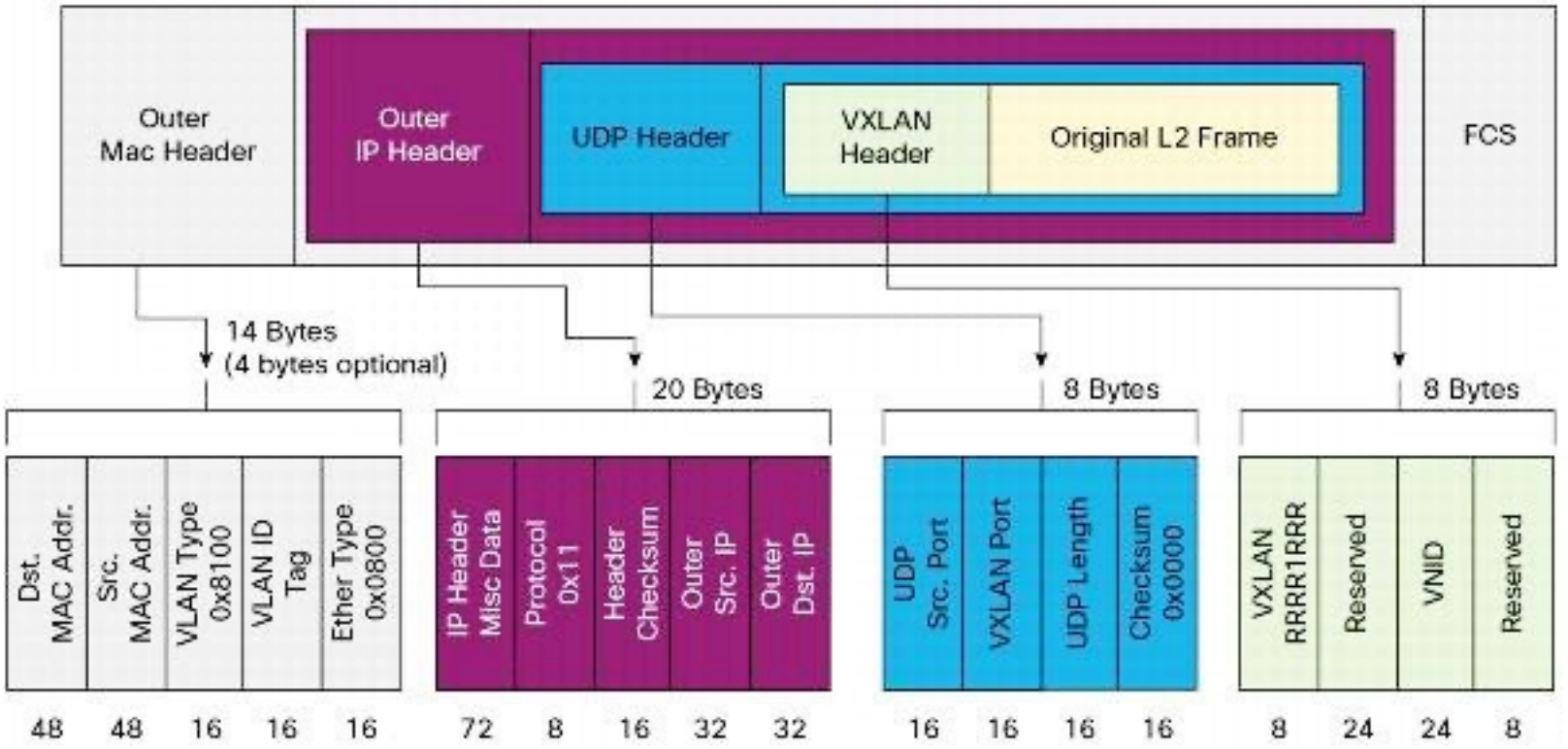
- VXLan Packet Format
- Packet Walk in an Ethernet VPN

Let’s scratch the surface of VXLan

VXLan Introduction

- EVPN’s main function is to support virtual Layer 2 (L2) network overlays.
- VXLAN is a MAC in IP/UDP(MAC-in-UDP) encapsulation with a 24-bit segment identifier in the form of a VXLAN ID.
- Because it is IP/UDP encapsulation, it allows each LAN segment to be extended across existing Layer 3 networks.

VXLan Packet Format



VXLAN Tunnel Endpoint

- VXLAN uses VXLAN tunnel endpoint (VTEP) devices
  - This basically map tenants' end devices to VXLAN segments.
- Perform VXLAN encapsulation and de-encapsulation.
- Each VTEP function has two interfaces
  - One is a switch interface on the local LAN segment to support local endpoint communication
  - Other is an IP interface to the transport IP network.

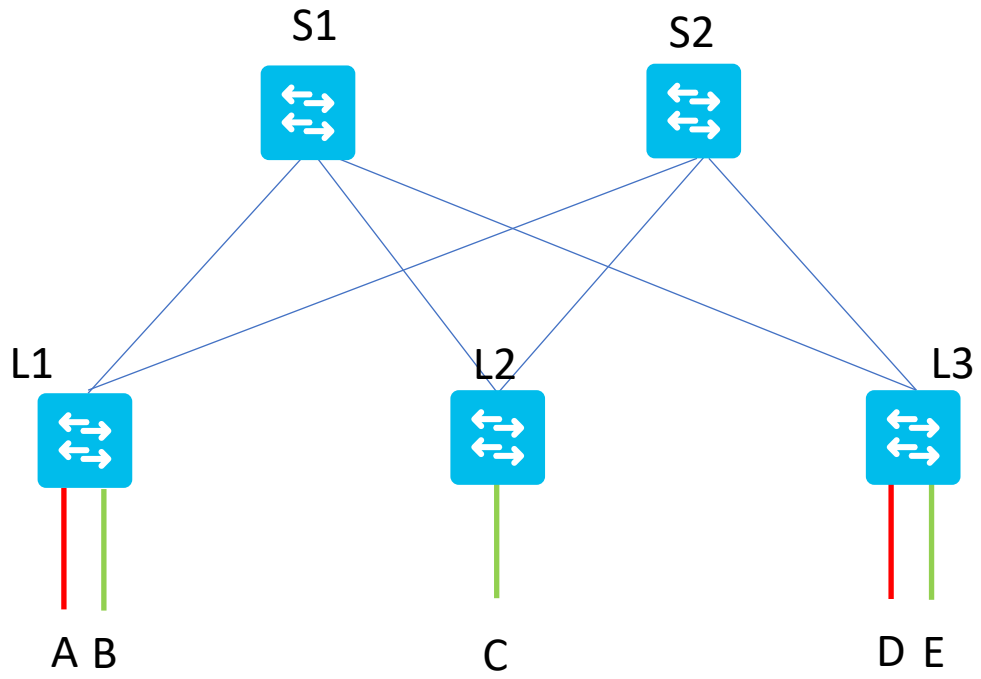
Virtual Network Identifier (VNI)

- A VNI is a value that can identify a specific virtual network in the data plane.
  - It is typically a 24- bit value which can support up to 16 million individual network segments

Let’s look at Bridging in Traditional Environment

- An 802.1Q bridge forwards a packet based on the VLAN and the destination MAC address of the packet.
- 802.1Q bridges uses “flood-and-learn” mechanism to populate the MAC forwarding table

Let’s look at Bridging in Traditional Environment

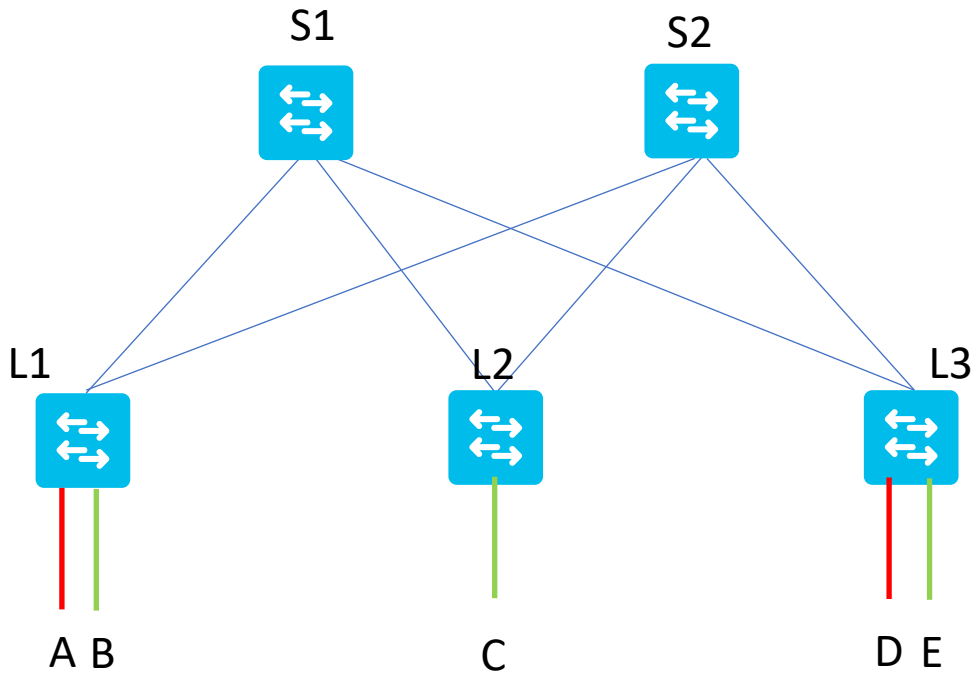


Red VNI has subnet 10.1.1.0/24, Green VNI has subnet 10.1.2.0/24.
For our discussion, A's IP is 10.1.1.A, D's IP is 10.1.1.D etc.

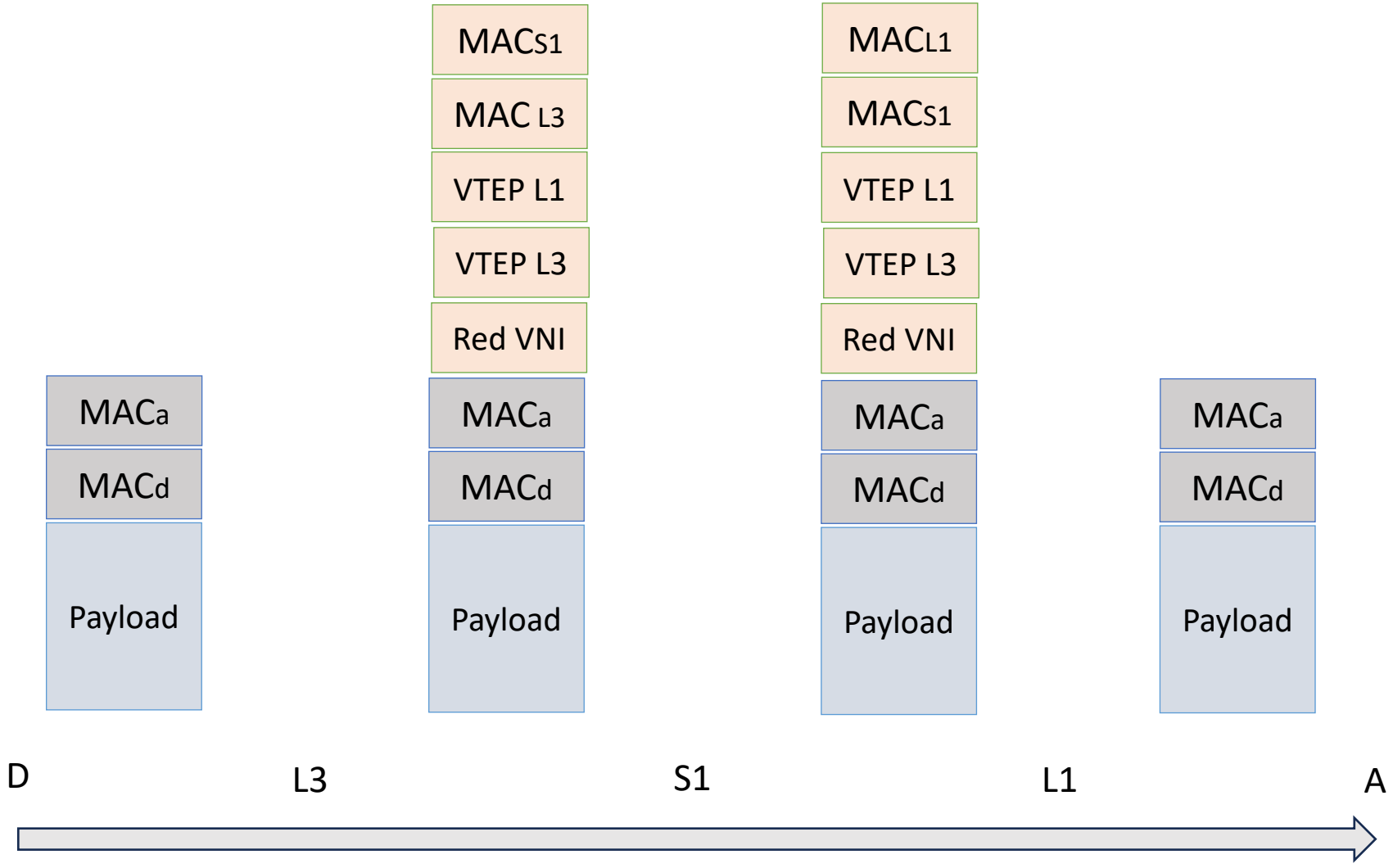
Let’s look at Bridging with EVPN

- First thing first, Packet forwarding between the leaves and spines happens via Routing.
- Leaf switches act as Network Virtualization Edges (NVEs).

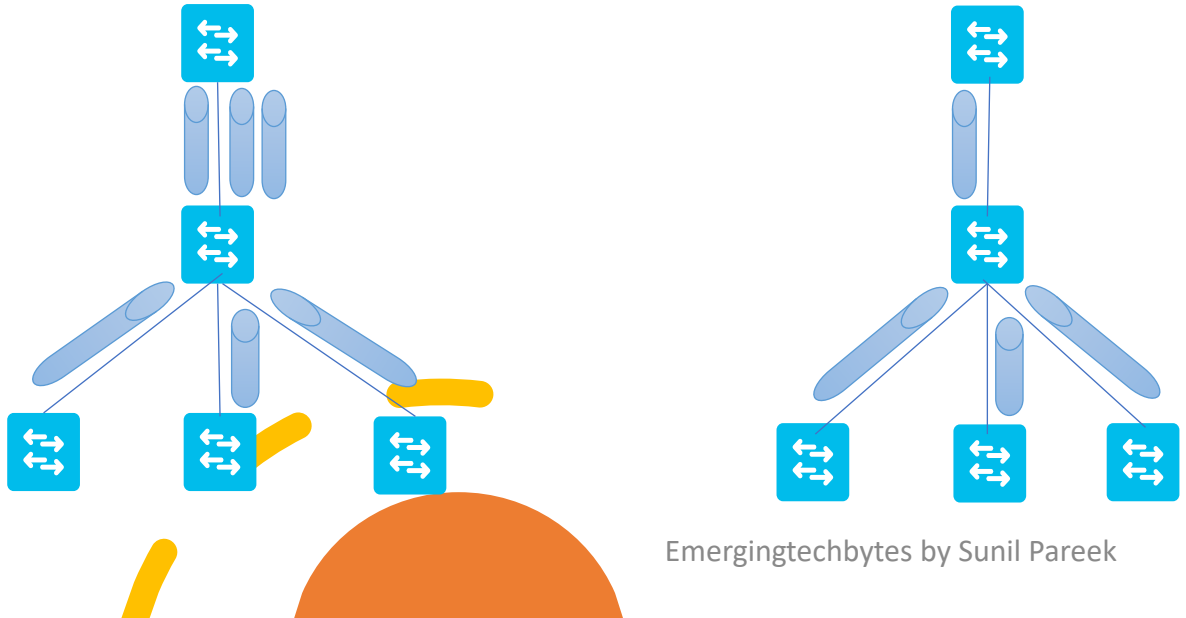
Let’s look at Bridging with EVPN



VXLan Encapsulation



Basics of EVPN – Let’s Learn BUM Traffic Forwarding in EVPN



Emergingtechbytes by Sunil Pareek

Agenda

- Handling BUM Packets

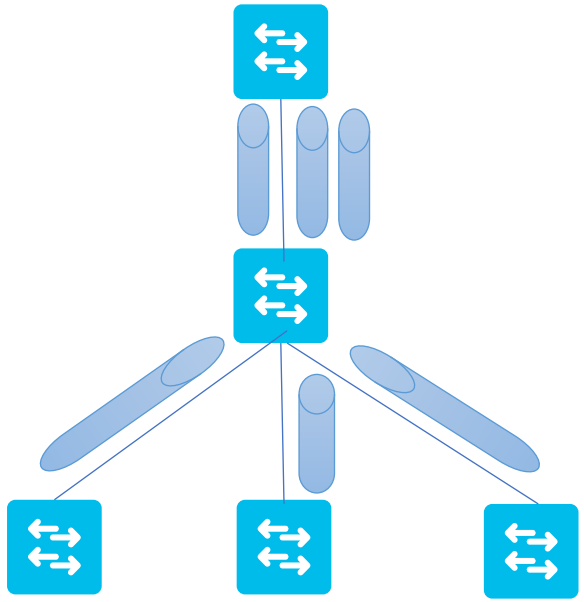
Two Choices that Exist

- Ingress Replication
- Layer 3 Multicast – Its in underlay
- Any third choice ??

Ingress Replication

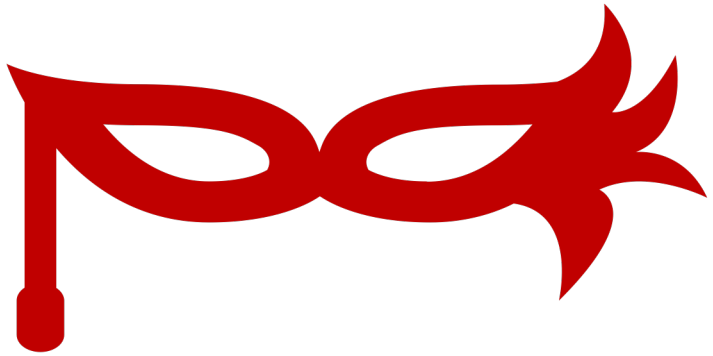
Ingress Replication

- Ingress VTEP sends multiple copies of a packet, one for each egress VTEP **who so ever is interested** in the virtual network



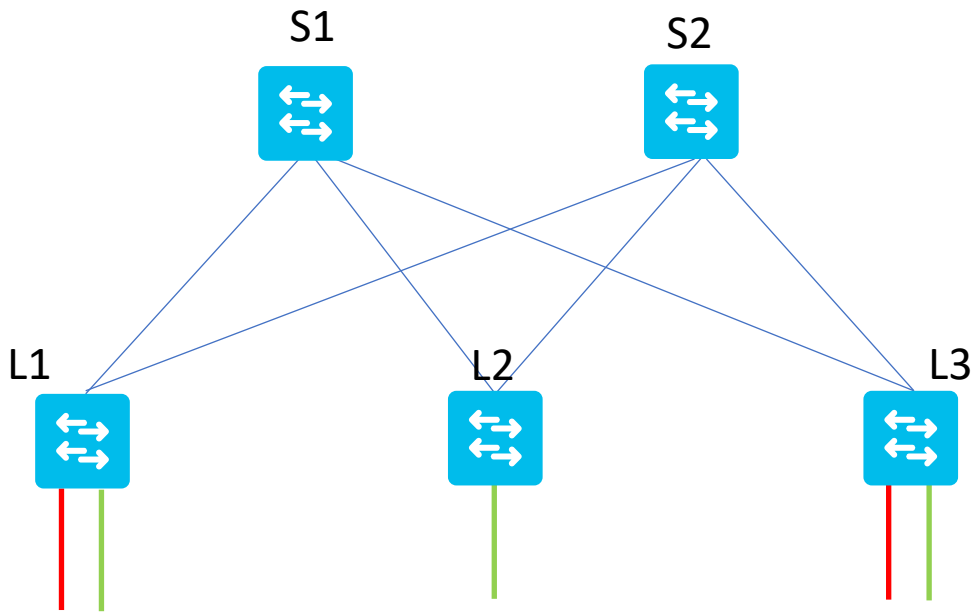
Why Ingress Replication

- Major benefit of this model is that it keeps the underlay networks very simple
  - No fancy features like Multicast, Period!!!



Fundamental Question

- The replication list is automatically formed from the BGP EVPN Route Type -3 messages without any intervention from the user.
  - Basically Route-type 3 carries the Virtual Network Identifiers (VNIs) of interest to a VTEP.



BGP Route type 3

- EVPN Type 3 routes are used by VTEPs to advertise L2VNIs and VTEP IP addresses to each other for creating an ingress replication list.
- In other words, Type 3 routes are used for automatic VTEP discovery and dynamic VXLAN tunnel establishment.
- This provides a way to replicate multi destination traffic in a unicast way.

When BGP Route type 3 is Generated

- Route type 3 is generated immediately and sent to all ingress replication–participating VTEPs as soon as a **VNI is configured at the VTEP and is operational**.
  - This is different from Route type 2, which is only sent with MAC/IP information, once end hosts have been learned.
- Because of RT-3, every VTEP is aware of all the other remote VTEPs that need to be sent a copy of a BUM packet in a given VNI.
- Route type 3 is called “Inclusive Multicast Ethernet Tag route”

How Does BGP Route type 3 looks like

- The NLRI of Type 3 routes consists of a prefix and a PMSI attribute
- The Originating Router's IP Address field of the NLRI contains VTEP IP address information
- MPLS Label field of the PMSI attribute contains L2VNI information.

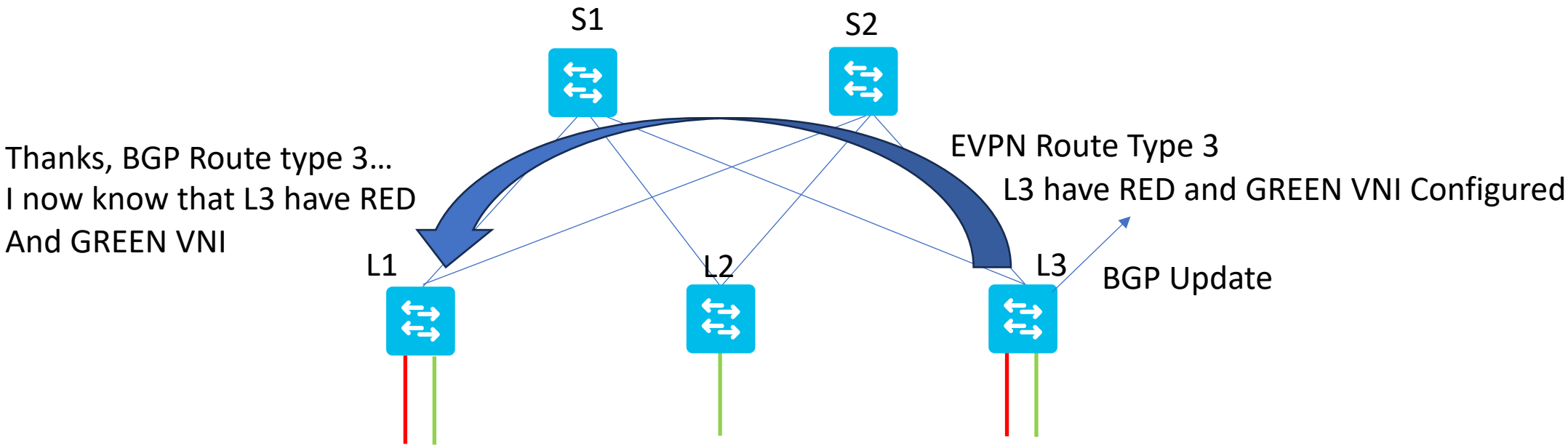
Prefix

Route Distinguisher (8 bytes)
Ethernet Tag ID (4 bytes)
IP Address Length (1 byte)
Originating Router's IP Address (4 or 16 bytes)

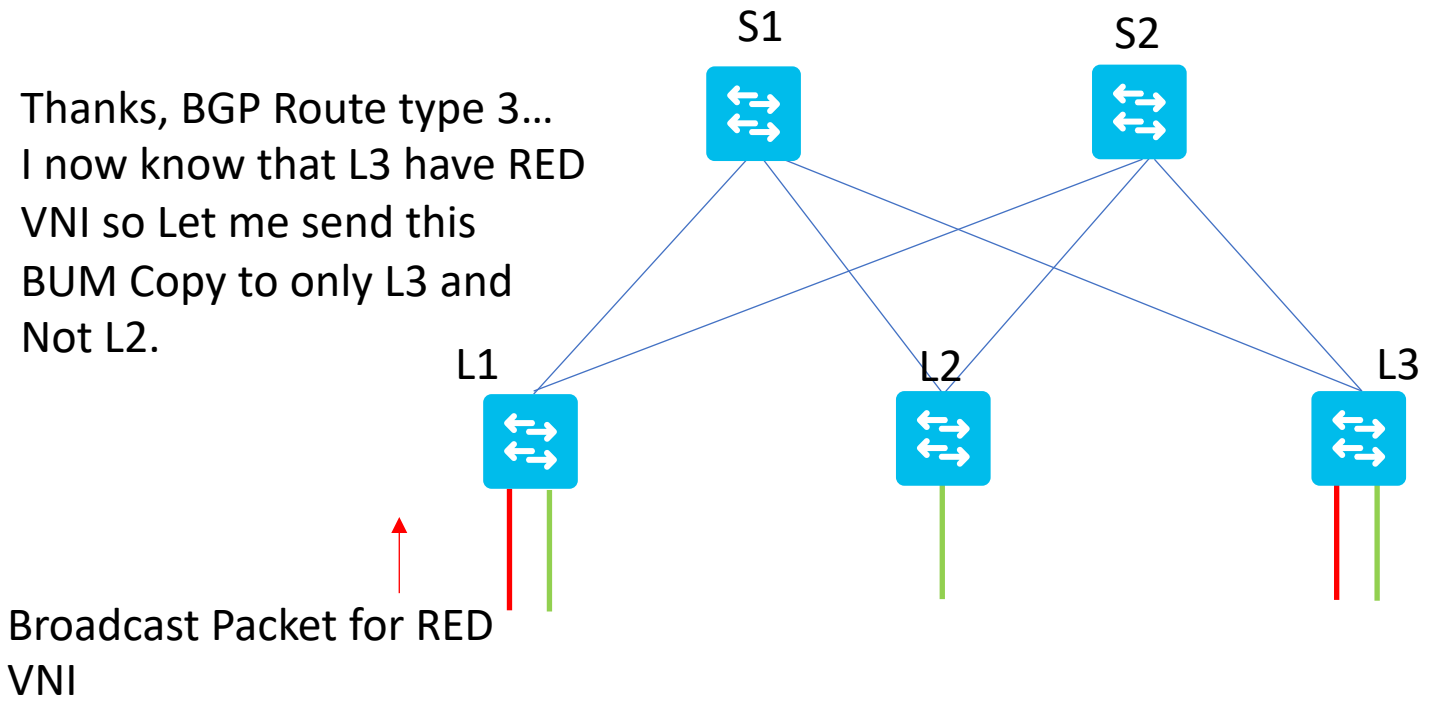
PMSI attribute

Flags (1 byte)
Tunnel Type (1 byte)
MPLS Label (3 bytes)
Tunnel Identifier (variable)

BGP Route type 3 – Simple Analogy for Ingress Replication



BGP Route type 3 – Simple Analogy for Ingress Replication



BGP Route type 3

- Dynamic replication list stores all the remote destination peers which are discovered on a BGP Route type 3 in the same Layer 2 VNI.
- The replication list gets updated every time you configure the Layer 2 VNI at a remote peer.

VTEP Show command

```
Leaf-01#sh l2route evpn imet topology 102
EVI ETAG Prod   Router IP Addr    Type Label   Tunnel ID Multicast Proxy
----- ---------- ------ --------------- ----- -------- -------------- ---
102  0    BGP    10.16.254.4        6    10102  10.16.254.4           No
102  0    BGP    10.16.254.5        6    10102  10.16.254.5           No
102  0    L2VPN  10.16.254.3        6    10102  10.16.254.3           No
```

IMET - Inclusive Multicast Ethernet Tag Route

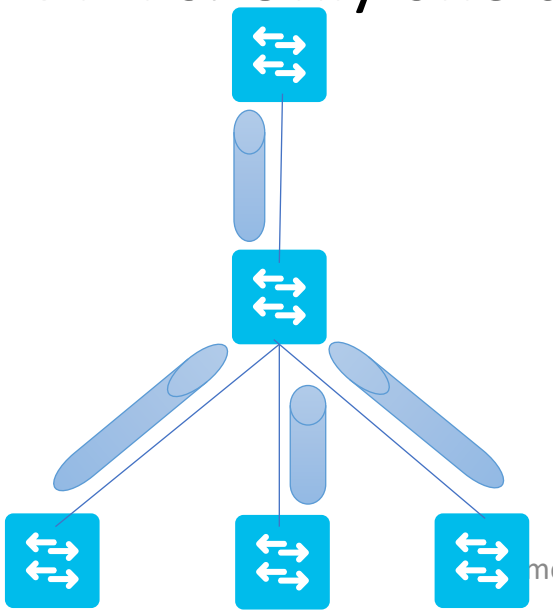
Any Downside

- Downside of this approach
  - Replication bandwidth needed from the underlay can be high

Layer 3 Multicast in Underlay

Layer 3 Multicast in the Underlay Network

- Second approach to handling BUM packets is to use Layer 3 multicast in the underlay network
- The main advantage of this approach is that it is possible to handle a large volume of BUM packets as packets are not replicated per interested VTEPs. Only one copy is sent from ingress.



Layer 3 Multicast in the Underlay Network

- In this model, besides providing unicast routing support, the underlay must also provide multicast routing support.
- Protocol Independent Multicast (PIM).

Any Downside

- Layer 3 Multicast is a configuration Intensive feature.
- To make sure that for every virtual network only, the associated VTEPs get the packet, each virtual network must be in its own multicast group.

Any Downside

```
l2vpn evpn instance 101 vlan-based
encapsulation vxlan
!
l2vpn evpn instance 102 vlan-based
encapsulation vxlan
!
vlan configuration 101 member
evpn-instance 101 vni 10101
vlan configuration 102 member
evpn-instance 102 vni 10102
vlan configuration 901
member vni 50901
!
```

```
interface nve1
no ip address
source-interface Loopback1
host-reachability protocol bgp
member vni 10101 mcast-group 225.0.0.101
member vni 10102 mcast-group 225.0.0.102
```

Dropping BUM packets

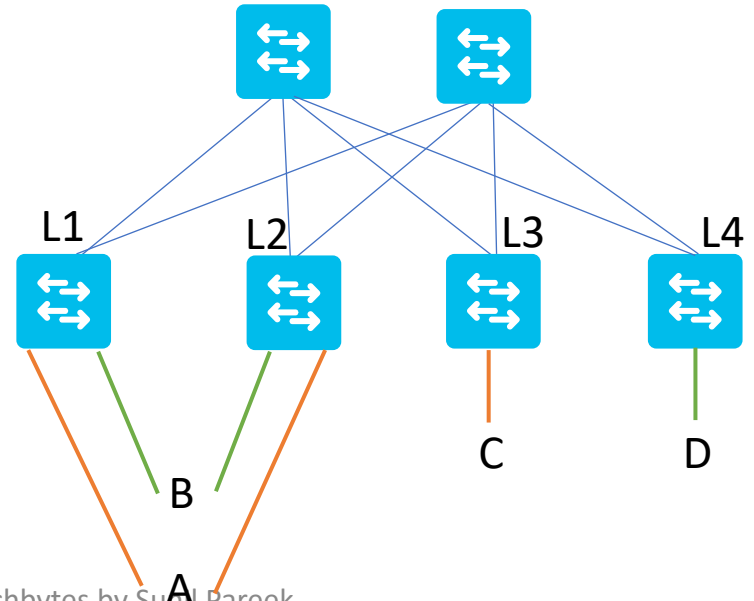
- BUM packets can be considered as a DDoS attack on the network
- ARP/ND suppression can help here

Signaling which approach is deployed

- Because there are choices, each VTEP must inform the other VTEPs of what it can support.
- RT-3 EVPN messages carry a BGP attribute called Provider Multicast Service Interface (PMSI), which identifies the kind of BUM packet handling supported by this device.

  + 0 - No tunnel information present
  + 1 - RSVP-TE P2MP LSP
  + 2 - mLDP P2MP LSP
  + 3 - PIM-SSM Tree
  + 4 - PIM-SM Tree
  + 5 - BIDIR-PIM Tree
  + 6 - Ingress Replication
  + 7 - mLDP MP2MP LSP

Basics of EVPN – Let’s Learn Multi-homing in EVPN



Agenda

- Dual Attached Hosts in EVPN

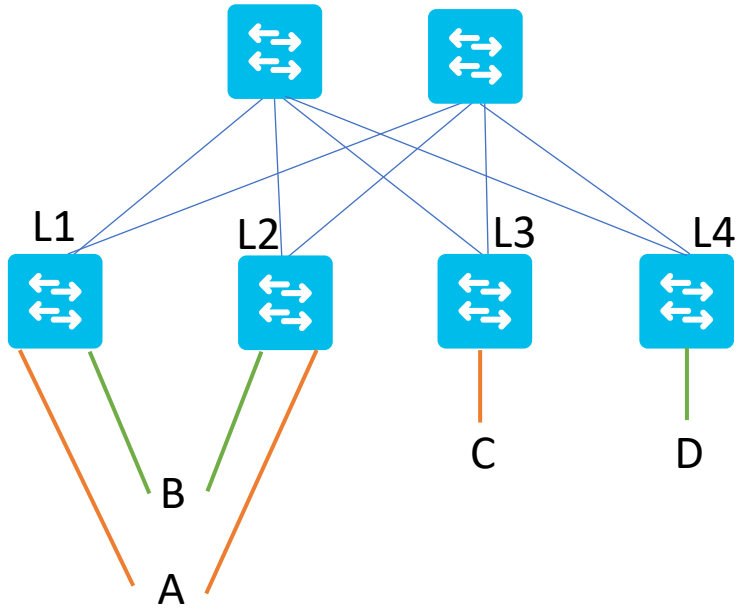
Dual Attached Hosts

- In Data Center, Enterprise Network or while connecting a CE node to a service provider, it’s a very common thing that end-point nodes are connected to more than one upstream network node.
- This is primarily done to ensure that a single link or a single node failure doesn’t leave the end-point node disconnected.

Dual Attached Hosts

- EVPN multihoming (EVPN-MH) provides support for all-active redundancy. It is a standards-based replacement for MC-LAG in Data Centers. Replacing MC-LAG:
  - Eliminates the need for peer links or inter-switch links between the top of rack switches
  - Allows more than two TOR switches to participate in a redundancy group
  - Provides a single BGP-EVPN control plane
  - Allows multi-vendor interoperability

Dual Attached Hosts



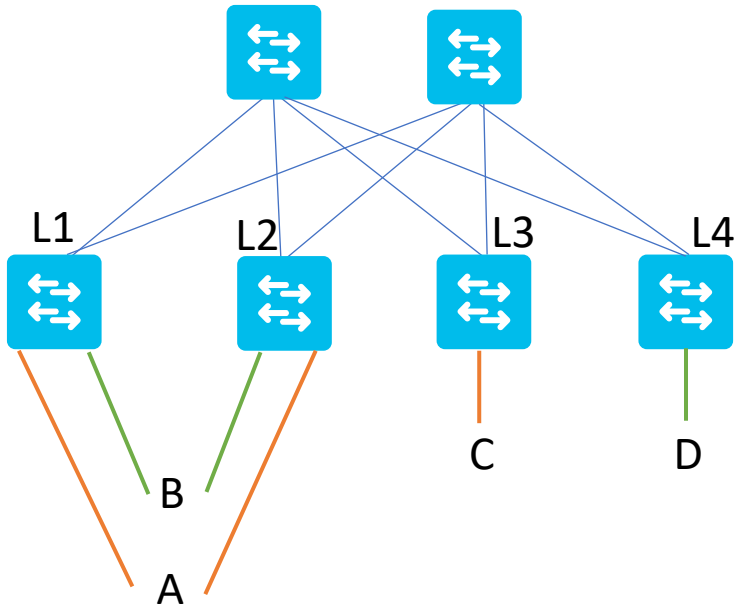
- What are the available way for a compute to be dual homed
- In Network, how dual attached host is seen by other remote vteps/nodes
- How BUM packets get delivered to a Host which is multi-homed
- How network redundancy is maintained when one link fail for dual homed endpoint

Two Choices that Exist

- MC-LAG or MLAG
- EVPN ESI

MLAG

- Most Commonly, two links from end-point node deployed in a port-channel aka bond interface.
  - Active/Active or Active standby load balancing
  - Single IP address is used



EVPN Dual Connected Hosts

- EVPN supports dual-attached devices natively.
- Primarily, EVPN uses Route Type 1 (RT-1) and Route Type 4 (RT-4) to handle multihomed nodes.

EVPN Multihoming Mode of Operation

- Single
  - Does not require Ethernet segment values to be configured.
- Dual Home
  - Active-Standby
  - Active Active

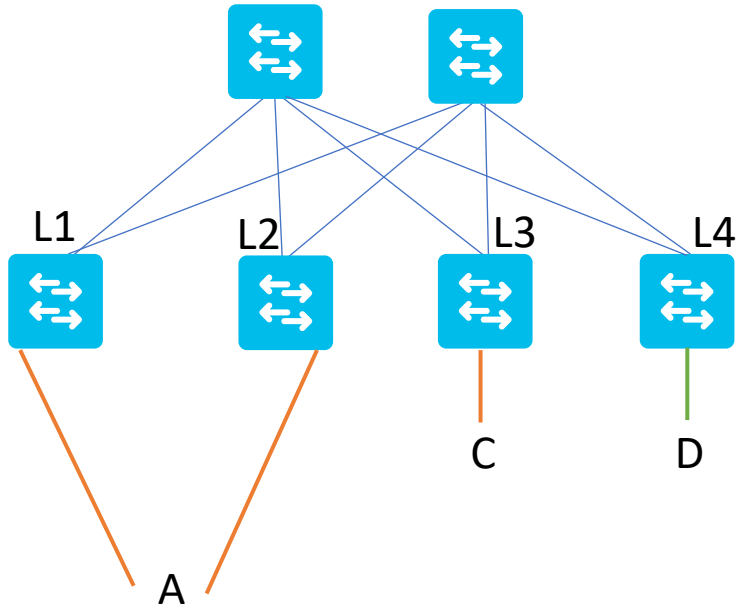
EVPN Operation

At start up, PEs exchange EVPN routes to advertise the following:

- **VPN Membership**: The PE discovers all remote PE members of a given EVI.
- **Ethernet Segment Reachability**: In multihoming scenarios, the PE auto-discovers remote PE and their corresponding redundancy mode (all-active or single-active).

EVPN Multihoming Concept

- **Ethernet Segment** - When a CE device is multihomed to two or more PE routers, the set of Ethernet links constitutes an Ethernet segment. An Ethernet segment appears as a link aggregation group (LAG) to the CE device.
- **Ethernet Segment Identifier (ESI) -** Ethernet segments are assigned a unique non-zero identifier, which is called an Ethernet Segment Identifier (ESI). ESI represents each Ethernet segment uniquely across the network.
- **EVI** - An EVPN instance (EVI) is an EVPN routing and forwarding instance spanning all the PE routers participating in that VPN. An EVI is configured on the PE routers on a per-customer basis. Each EVI has a unique route distinguisher and one or more route targets.
    - EVIs are assigned import/export Route Targets (RTs).



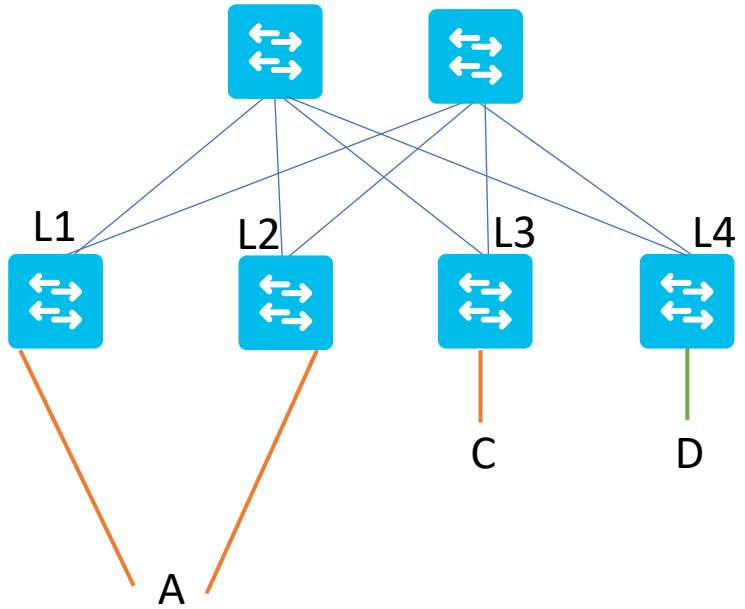
Ethernet Segment Route – Route Type 4

- Type 4 BGP Route
  - Discover other ESI Members
  - Used for DF Election

EVPN Multihoming Concept

Ethernet Segment Route—The PE routers that are connected to a multihomed CE device use BGP Ethernet segment route messages to discover each of the PE routers connected to the same Ethernet segment.

The PE routers advertise the Ethernet segment route, which consists of an ESI and ES-import extended community.



Auto Discovery Route – Route Type 1

- Type 1 Mandatory Route
  - Used for Faster Convergence
  - Mass Withdrawal Route

EVPN Multihoming Concept

- EAD/ES: Ethernet Auto Discovery Route per ES is also referred to as Route Type 1. This route is used to converge the traffic faster during access failure scenarios.
- EAD/EVI: Ethernet Auto Discovery Route per EVI is also referred to as Route Type 1. This route is used for aliasing and load balancing when the traffic only hashes to one of the switches.

When One link Fails in Multihoming

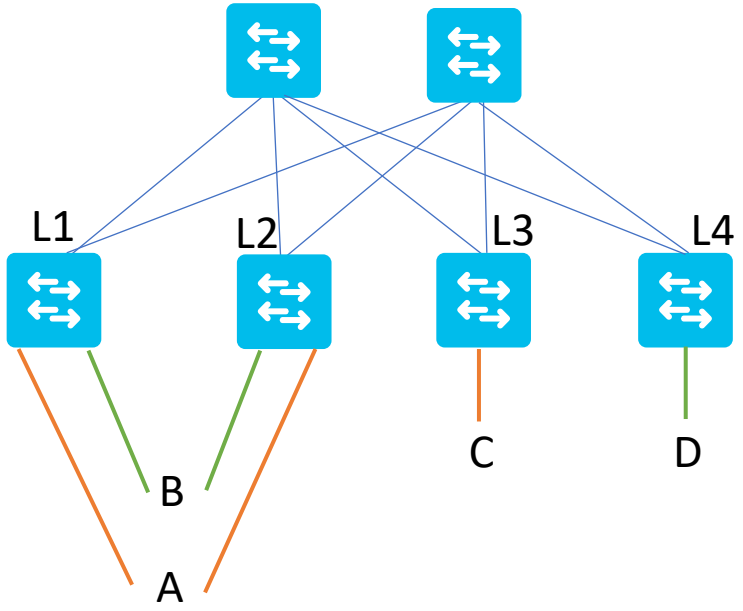
- What happens if one of the hosts—say host A loses a link
  - In the case of MLAG, using the peer link to reach the host via the other switch is the most common implementation.
  - In EVPN multihoming implementations, the switch that lost the connectivity to the host will also withdraw reachability

Traffic Flow

- The traffic flows in EVPN multihoming can be based on the two traffic types:
  - Unicast traffic
    - In active-standby mode
    - In active-active mode
  - BUM traffic
    - In active-standby mode
    - In active-active mode

Basics of EVPN - Let's Learn EVPN Concepts

Multihoming Advance



Agenda

- Advance Scenarios and Questions

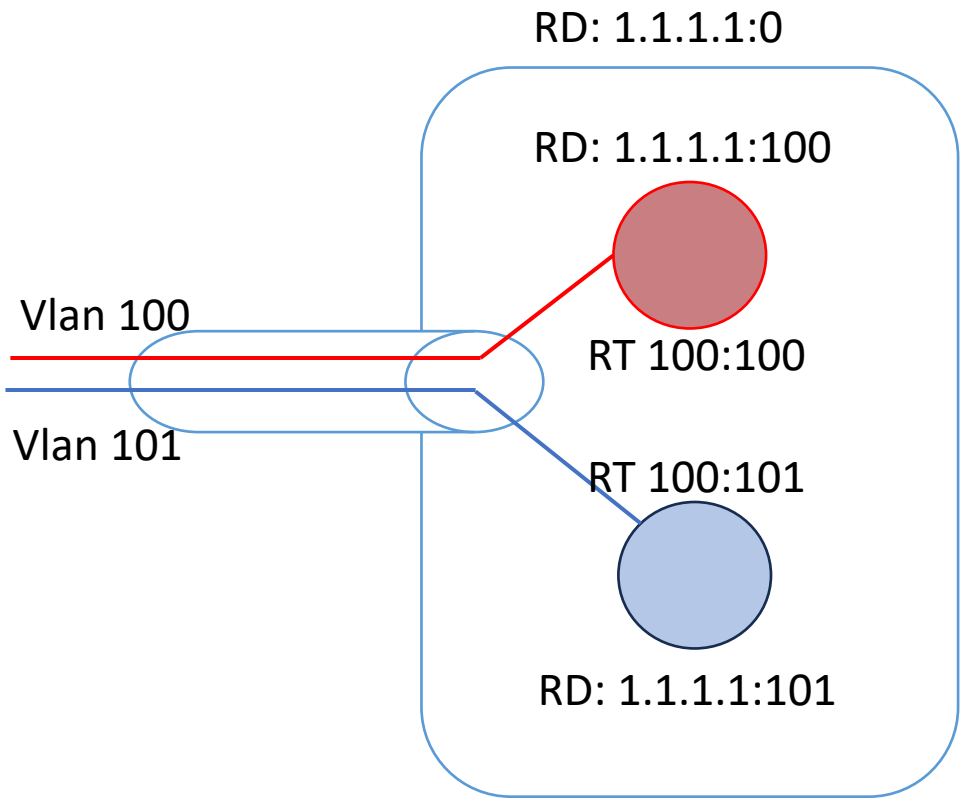
How EVPN RD and RT Allocation works

- Normally when you configure EVPN, you don’t need to configure RD and RT values. There is a process to auto-generate.
- RD and RT values are generated using BGP:
  - Per-node/Per-EVI RD - [BGP Router-ID]:[EVI-ID]
    - Similar to VRF RD in L3VPN
  - Per-node/Per-EVI RT – [BGP-AS]:EVI-ID]
  - Per-node RD – [BGP Router-ID]:1,2,3…
    - DF Election and Mass Withdraw for EVPN RT1, RT4

Give me some example

For Example – BGP Router id – 1.1.1.1, BGP AS 100, EVI 101

- Per node RD : 1.1.1.1:0,1,2…
- Per node/Per-EVI RD : 1.1.1.1:101
- Per node/Per EVI RT: 100:101



How does a PE discover other multi-homed PE Devices

EVPN Configuration

```
lacp system mac 1010.1010.1010

Interface Bundle-Ether100
 l2transport
 !
!

evpn
 evi 100
 advertise-mac
!

Interface Bundle-Ether100
ethernet-segment
 identifier type 0 10.10.00.00.00.00.00.11.00
!
```

```
l2vpn
 bridge group 100
 bridge-domain 100
  interface Bundle-Ether100
  !
 !
 evi 100
  !
  !
```

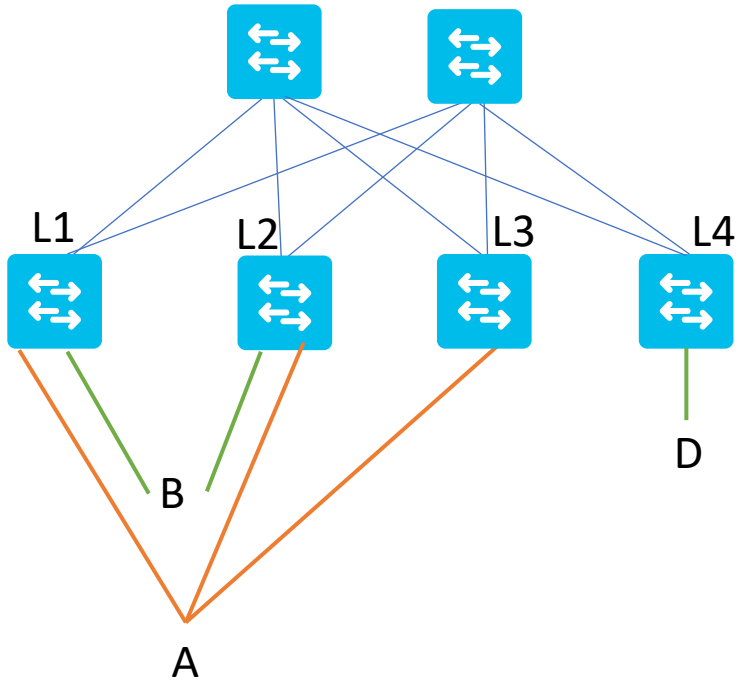
EVPN Configuration

```
router bgp 100
 bgp router-id 1.1.1.1
 address-family l2vpn evpn
  !

 neighbor-group rr
 remote-as 100
 update-source Loopback0
 address-family l2vpn evpn
 !
 neighbor 2.2.2.2
 use neighbor-group rr
```

How does a PE discover other multi-homed PE Devices

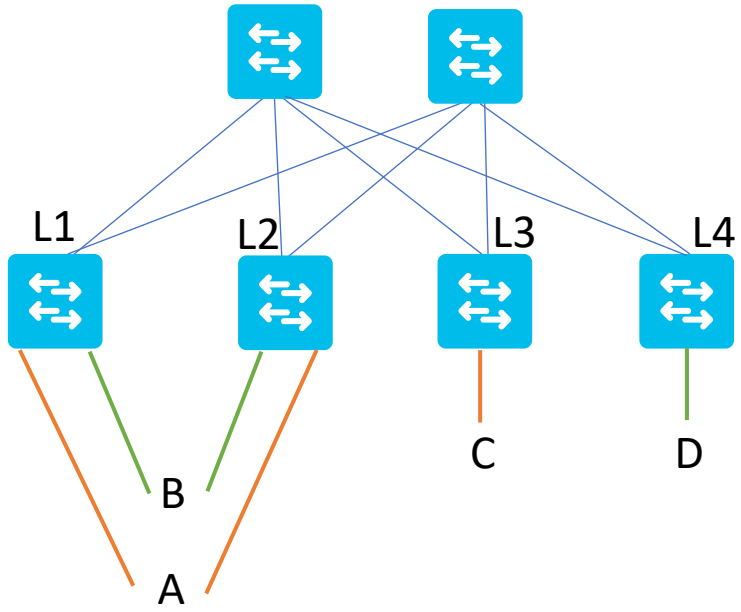
- Unique 10-byte global identifier per ethernet segment
- Bundle on the leaf's connecting to a CE should have identical ethernet segment identifier.
- Another important thing here is You **typically** configure Ethernet segment per physical interface.



Ethernet Segment Route - Summary

- In EVPN context, this is Type 4 route.
  - Purpose of this route is to enable the **PE routers connected to the same Ethernet segment to automatically discover** each other.
- This route will carry an **ES-import extended community** which is **derived from the ESI** value only.
  - Hence this route is **advertised and imported only by PE routers that are multihomed** on the advertising Ethernet segment.

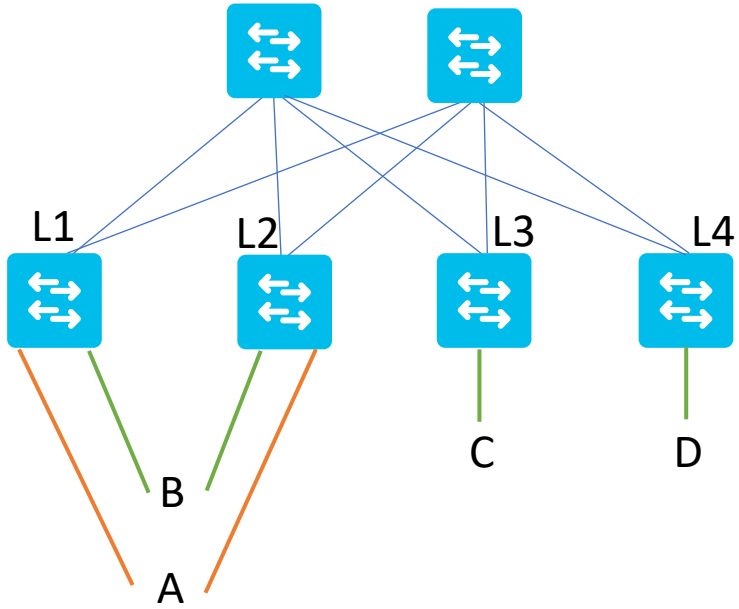
Dual Attached Hosts



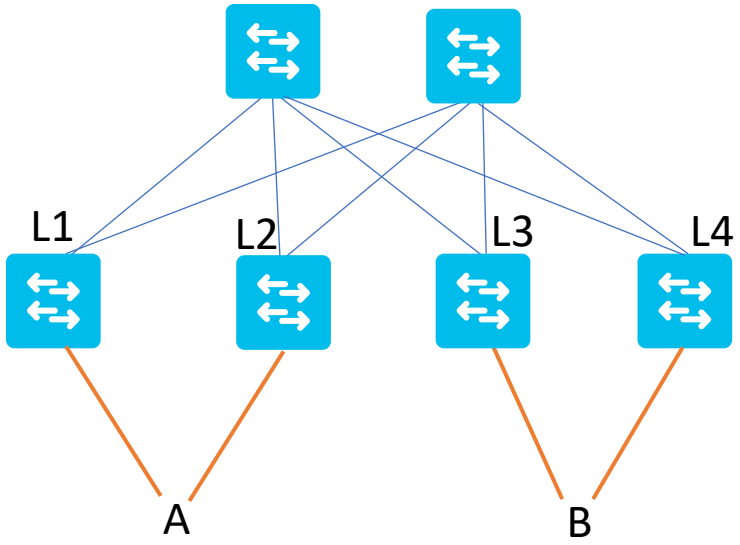
- What are the available way for a compute to be dual homed
- In Network, how dual attached host is seen by other remote vteps/nodes
- How BUM packets get delivered to a Host which is multi-homed
- How network redundancy is maintained when one link fail for dual homed endpoint

Traffic Flow

- The traffic flows in EVPN multihoming can be based on the two traffic types:
  - Unicast traffic
    - In active-standby mode
    - In active-active mode
  - BUM traffic
    - In active-standby mode
    - In active-active mode



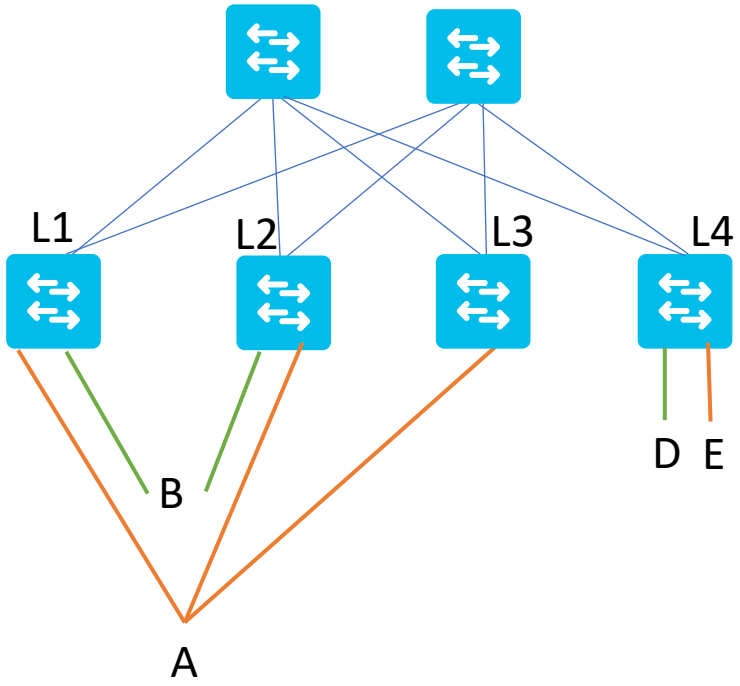
How BUM Replications works in EVPN



EVPN Multihoming Concept – Part 1 covered

- EAD/ES: Ethernet Auto Discovery Route per ES is also referred to as Route Type 1. This route is used to converge the traffic faster during access failure scenarios.
- EAD/EVI: Ethernet Auto Discovery Route per EVI is also referred to as Route Type 1. This route is used for aliasing and load balancing when the traffic only hashes to one of the switches.

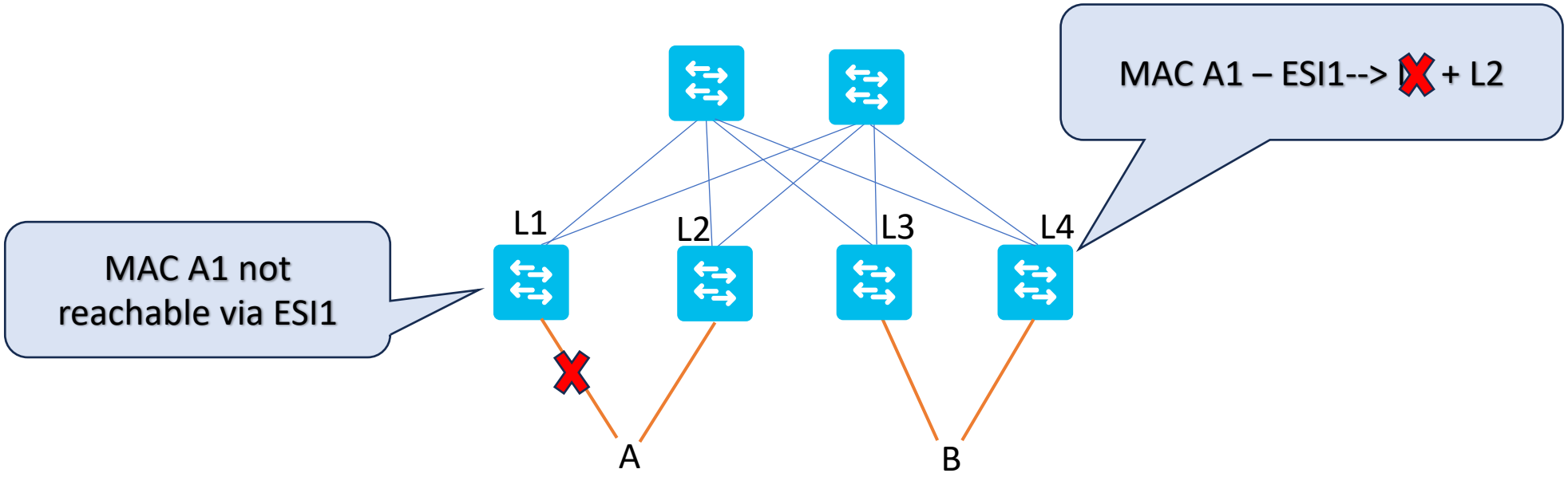
How Load Balancing works in EVPN



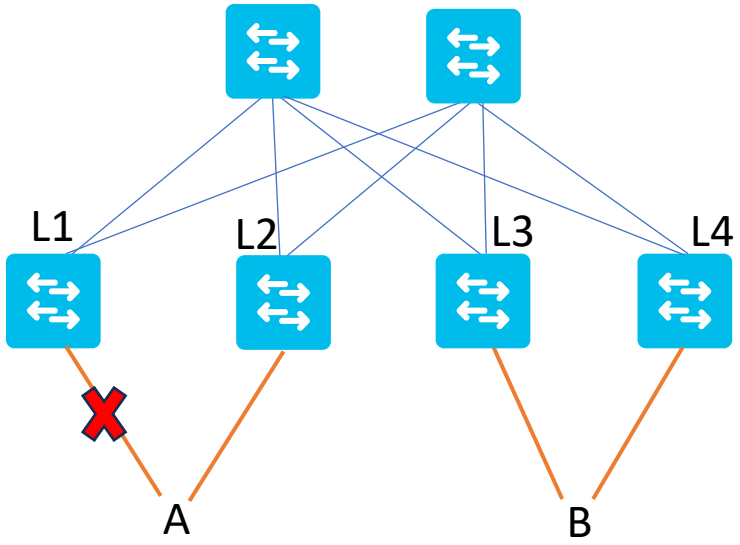
Aliasing

- Aliasing is the ability of a remote PE device to load balance Layer 2 unicast traffic on all the Multi-homed PE devices that share same Ethernet segment.
- Each of the multihomed PE device advertise an auto discovery route per EVPN instance (EVI).
  - This route is imported by the remote PE devices.

How does Route Type 1 help in convergence from Remote PE side

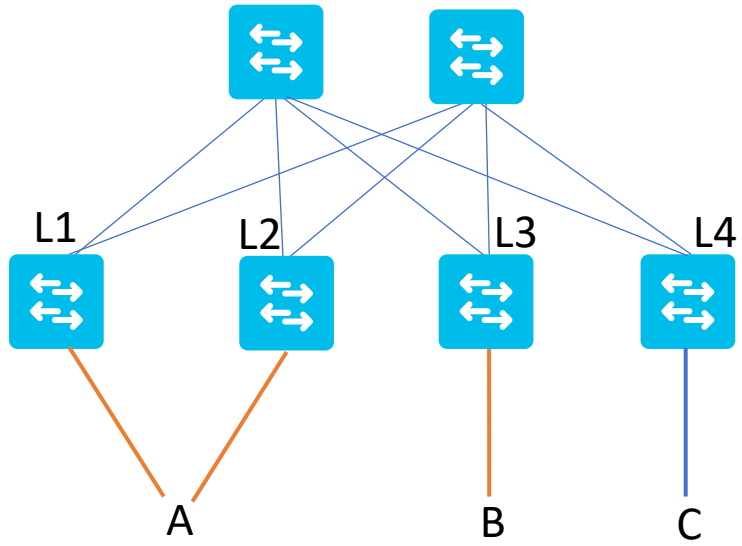


How does Route Type 1 help in convergence from Local Multi-homed PE side



Auto discovery Route per Ethernet Segment Feature

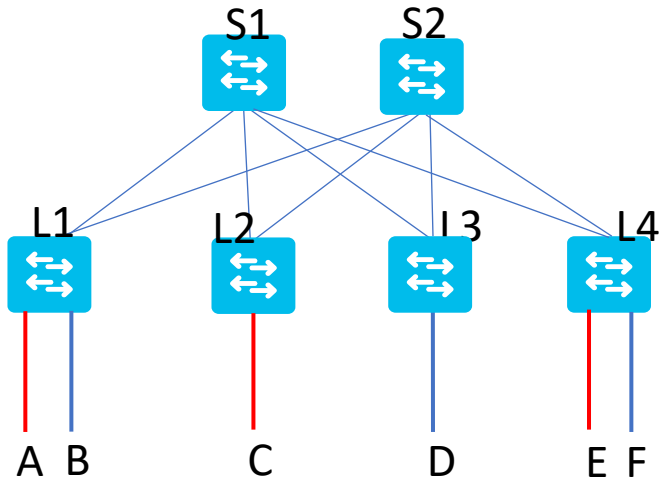
- This is a Type 1 route, used for fast convergence and for advertising the split horizon label.
- This route is advertised and imported by all multihomed and remote PE routers that share the same EVI on the advertising ESI.



EMERGING TECHBYTES PRESENTS

Let’s Learn Why we need

Routing in EVPN Advance Session



Agenda

- Why Routing in the EVPN Network
- How does this work
- Questions

Routing in EVPN

- Layer 2 VPN
  - VPWS
  - VPLS

- Layer 3 VPN
  - MPLS Based Layer 3 VPN

EVPN

Integrated Routing & Bridging

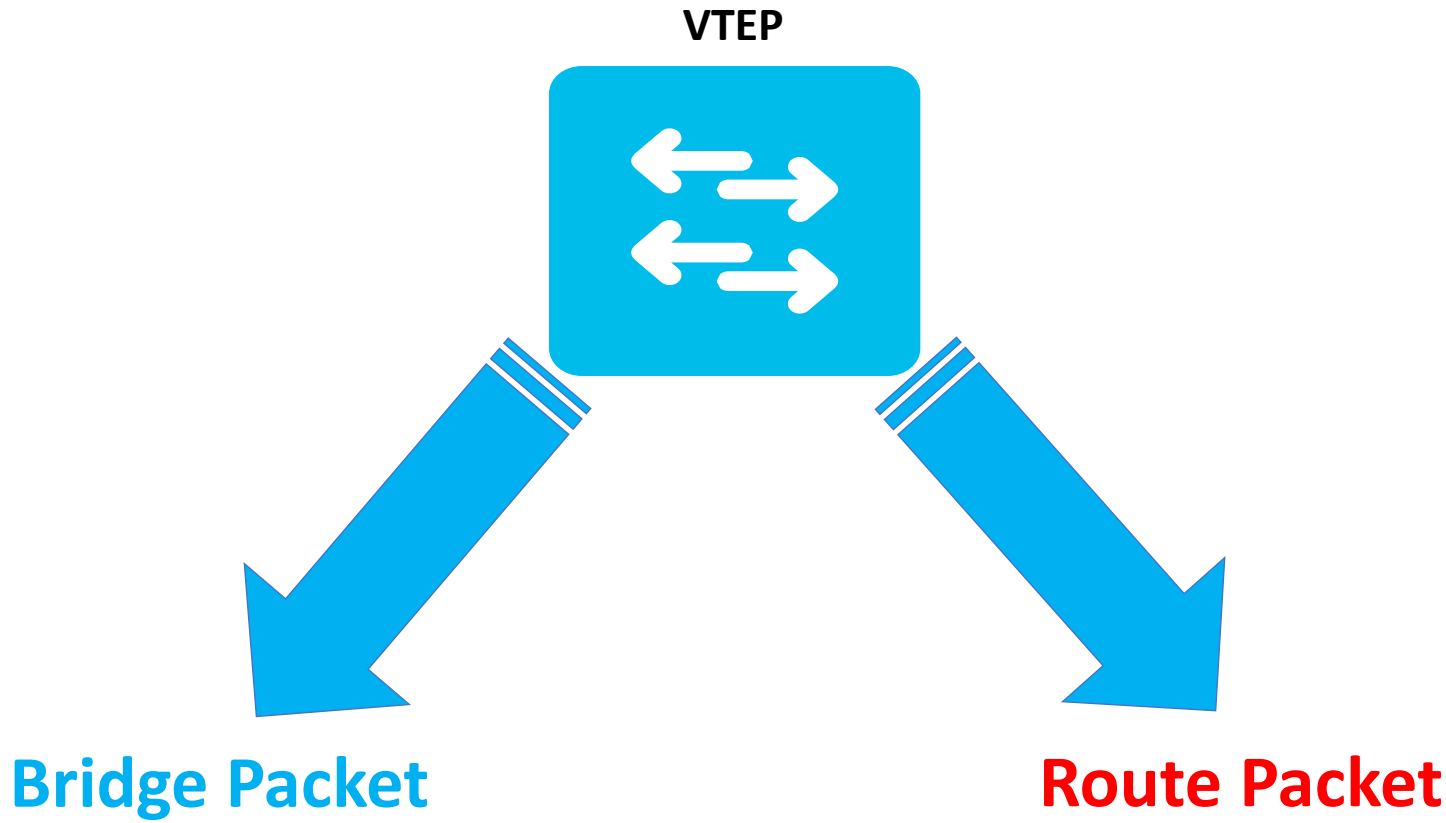
Why Routing in EVPN

- So, what exactly the use cases that drive the need for a routing solution in EVPN?

Routing Use Cases in the Data Center

- Company Name – ABC Limited

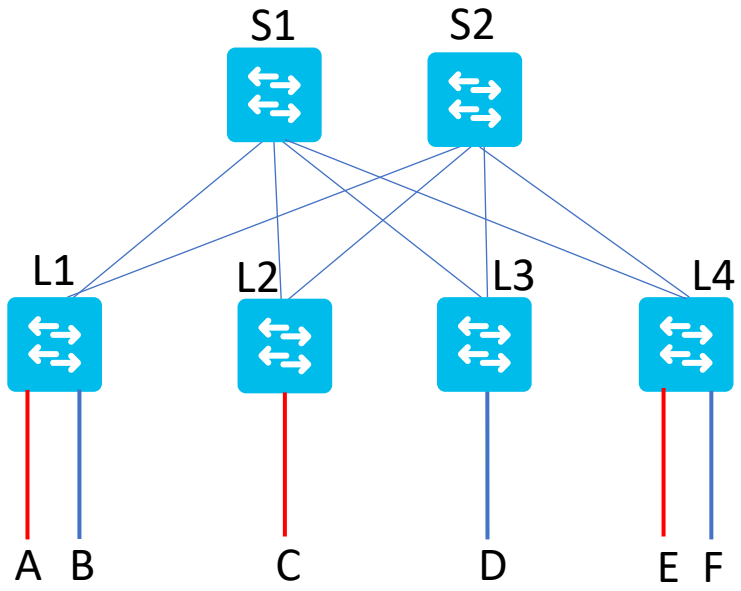
So, what’s the conclusion here



EVPN Routing Dilemma

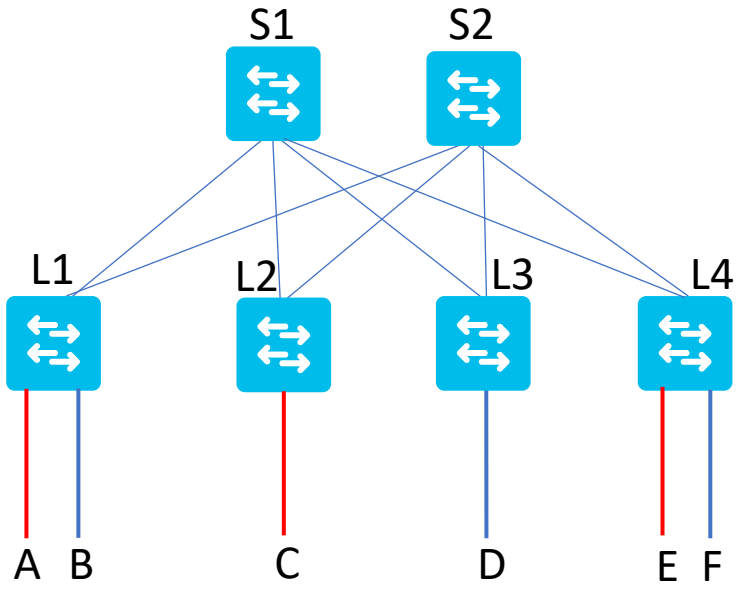
- Wait Sunil, Virtual Extensible LAN (VXLAN) provides a virtual L2 overlay network. So how can it transport routed packets?

Our Topology for the session



One More Question

What happen when C wants to send a packet to D.



Type of Routing in EVPN

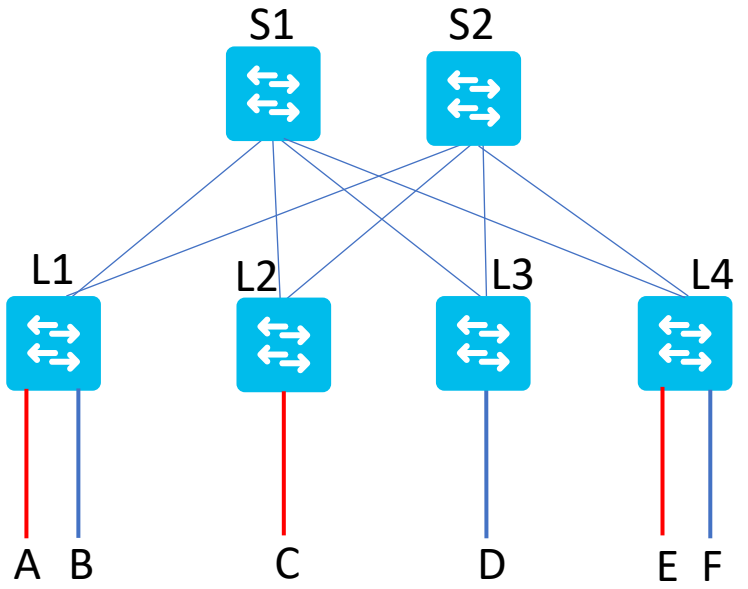
- When a single VTEP (or subset of VTEPs) is the first-hop router for a virtual network, the model is called *centralized routing*.
- If each VTEP is the first-hop router for its local endpoints on a virtual network, the model is called *distributed routing*
  - In distributed routing, every VTEP is the first-hop router for its locally attached networks

Available Routing Options in EVPN

- When L1 bridges the packet to F directly after routing and puts the F's VNI (blue) in that packet, it is called the ***asymmetric model*** of routing.
- When L1 routes the packet to L4 and puts in a new VNI, which represents the VRF and that's neither Red nor Blue, it is called the ***symmetric model*** of routing.

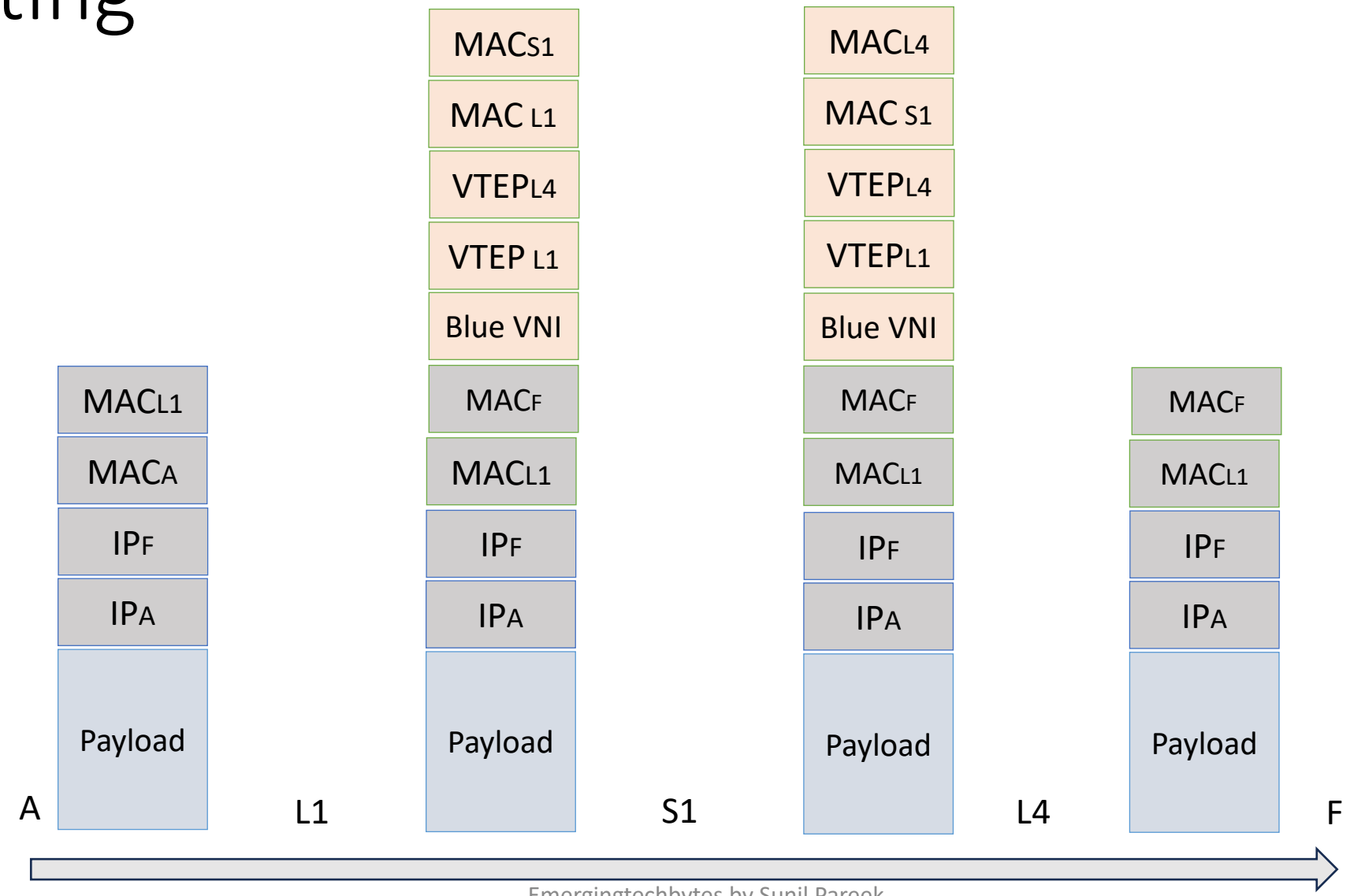
Asymmetric Routing – How it works

- Ingress and Egress VTEPs behave differently.



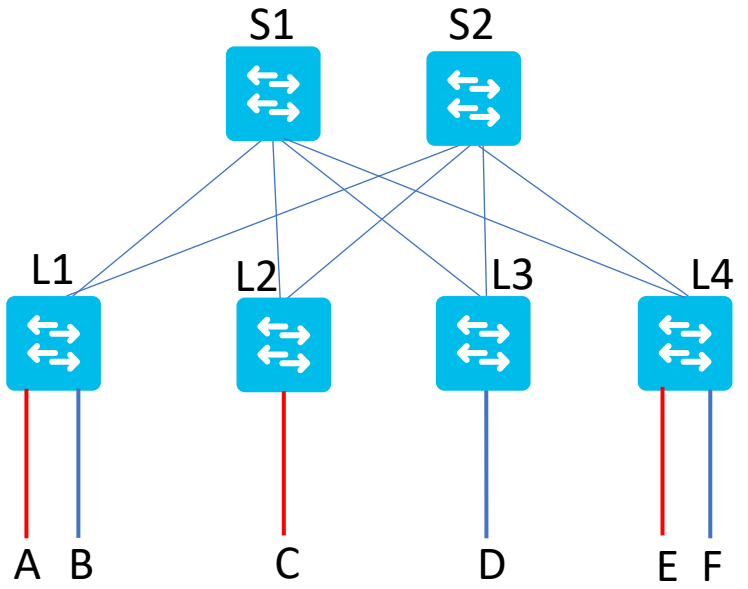
The ingress VTEP routes, whereas the egress VTEP only bridges

Packet Forwarding in Asymmetric Routing



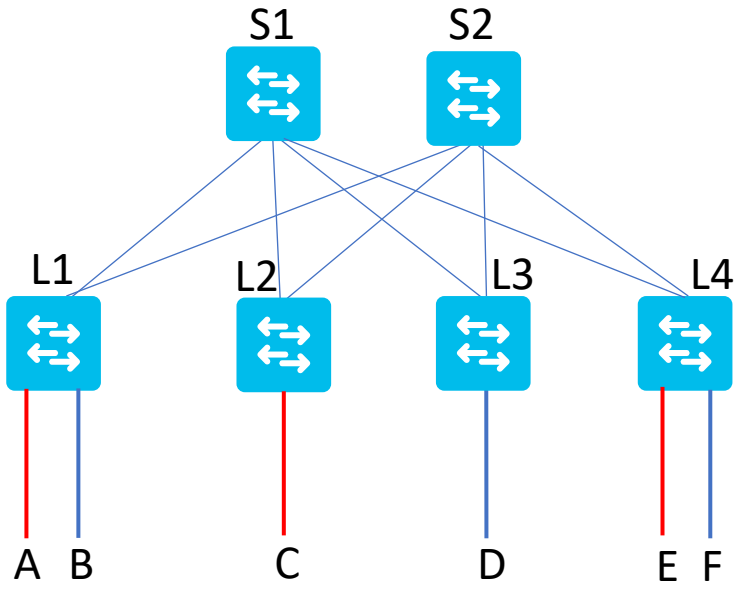
Remember this Question

What happen when C wants to send a packet to D.



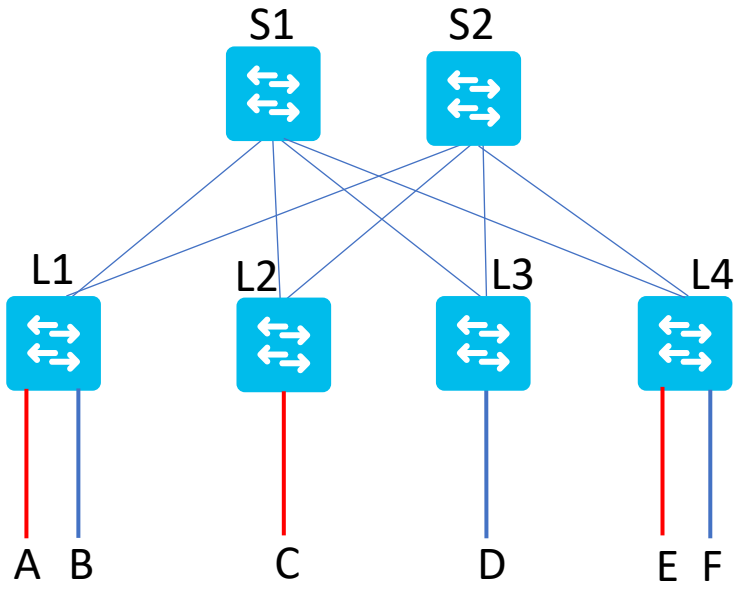
Thoughts on Asymmetric Routing

- Routing happened in at the first hop itself
- Asymmetric routing does not work if the destination subnet is not locally attached to the first-hop router.



Symmetric Routing – How it works

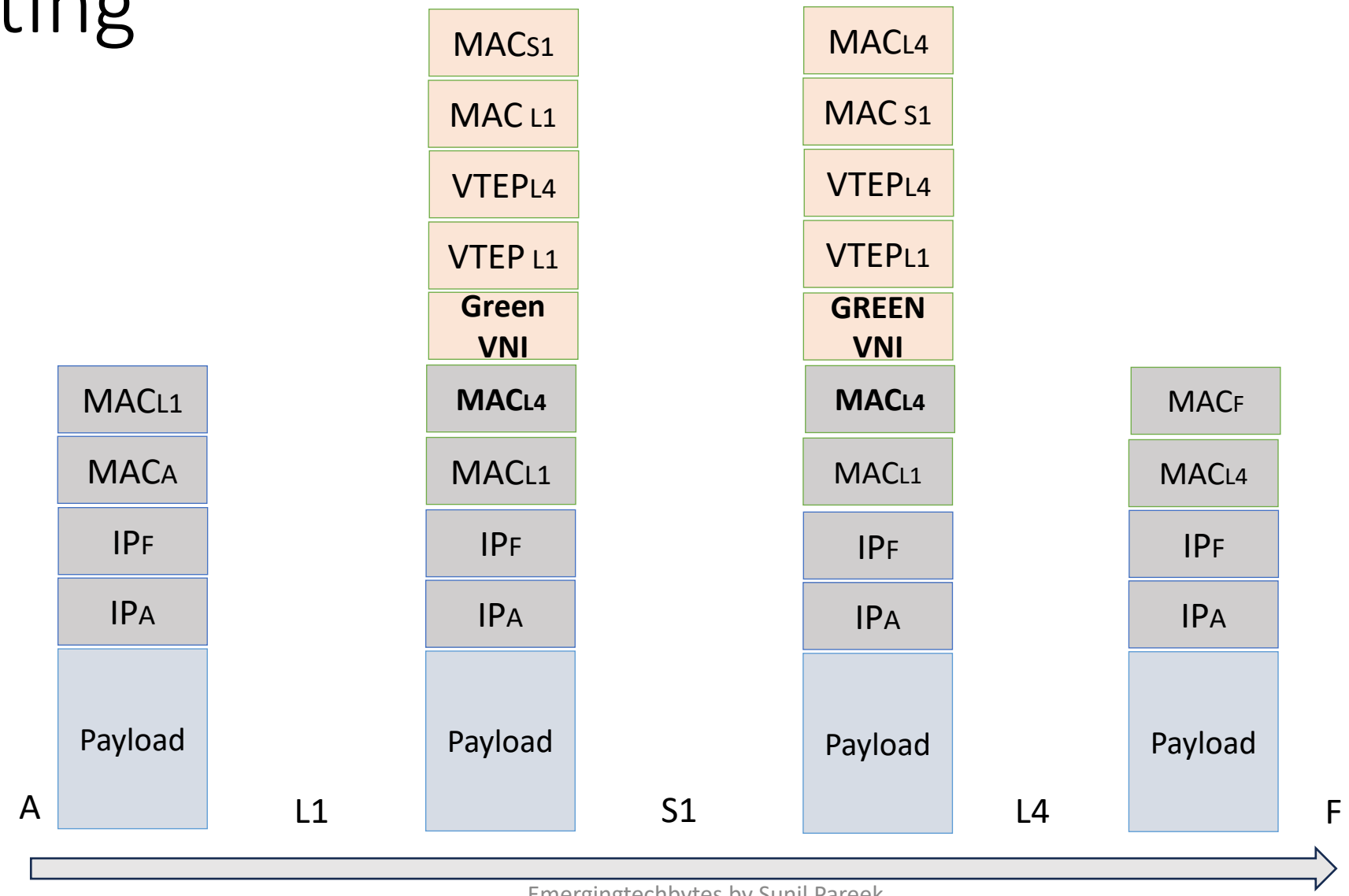
- In symmetric routing, Both the ingress and the egress VTEPs route the packet to its final destination.



Symmetric Routing – How it works

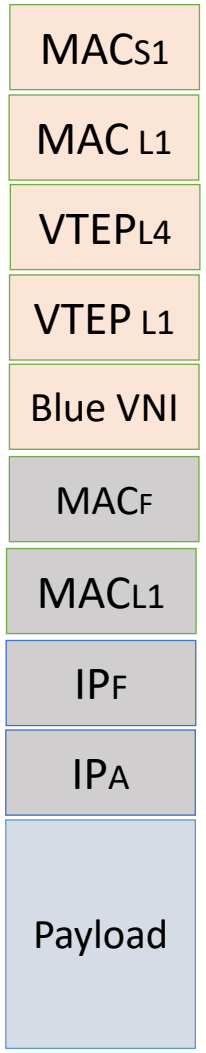
- Ingress VTEP routes the packet to the final destination with the egress VTEP as the next hop.
- Egress VTEP, after decapsulating, does a routing lookup to decide the path to the final destination.
- Third, the VNI used to carry the packet between the ingress and egress VTEPs is a Layer 3 VNI.

Packet Forwarding in Symmetric Routing



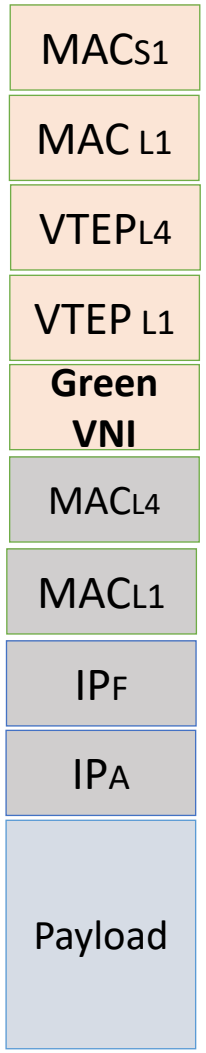
What is the difference here

Asymmetric



L1

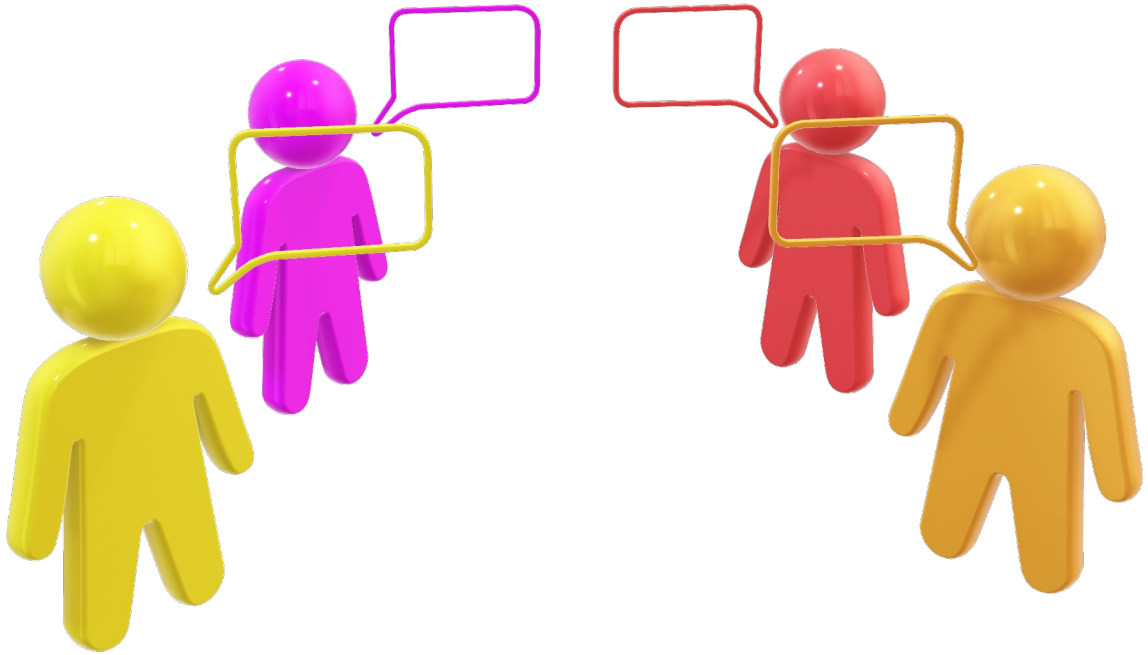
Symmetric



L1

Thoughts on Symmetric Routing


Learn Something



On Behalf of EMERGING TECHBYTES

Thank You