



# MAKES IT EASY

Cisco ACI Training Course

DAY1 - Concepts Review & ACI Introduction

November 2020



**Gerardo Marco D'Aurelio**



- Maticmind - Solution Architect, Consulting group.

Main job activity fields:

- Service Provider,
- Data Center,
- Automation.



- Electronic/Telecommunications engineer.

- Currently attending Ph.D. in Applied Electronics, Università degli Studi Roma Tre.

Research interests:

- Machine Learning/Deep Learning,
- Artificial Intelligence,
- Game Theory,
- Multi-Objective Optimization.



## Domenico De Prophetis



- Maticmind - Solution Architect, Consulting group.

Main job activity fields:

- Data Center,
- Campus Networking,
- Service Provider.



- Computer Science diploma
- 2 year Networking Specialization Course
- CCNP Routing & Switching
- 20 years on field expertise

# Course Objectives



*Upon completion of this course, you should be able to:*

**Describe ACI architectural components**

**Describe ACI configuration objects and their interactions**

**Configure basic tasks on the ACI fabric with Cisco APIC**

**Automate the configuration of ACI fabric**



# Course Modules & Schedule



## DAY 1

9:30 – 11:00

- Course Introduction
- Leaf-Spine Topology

11:00 – 11:30

*Break!*

11:30 – 13:00

- DC Underlay Evolution
- A New Overlay: VxLAN

13:00 – 14:00

*Lunch Time*

14:00 – 15:30

- VxLAN Fabric Details

11:00 – 11:30

*Break!*

16:00 – 17:30

- APIC Controller
- Q&A

## DAY 2

- Tenant Config pt. 1

*Break!*

- Tenant Config pt. 2 & 3

*Lunch Time*

- Fabric Access: Interface Policies

*Break!*

- AAEP-EPG Deployment
- Q&A

## DAY 3

- ACI Advanced Features

*Break!*

- ACI Advanced Features

*Lunch Time*

- ACI APIs & Automation
- Q&A

*Course Conclusions!*

# AGENDA - DAY 1

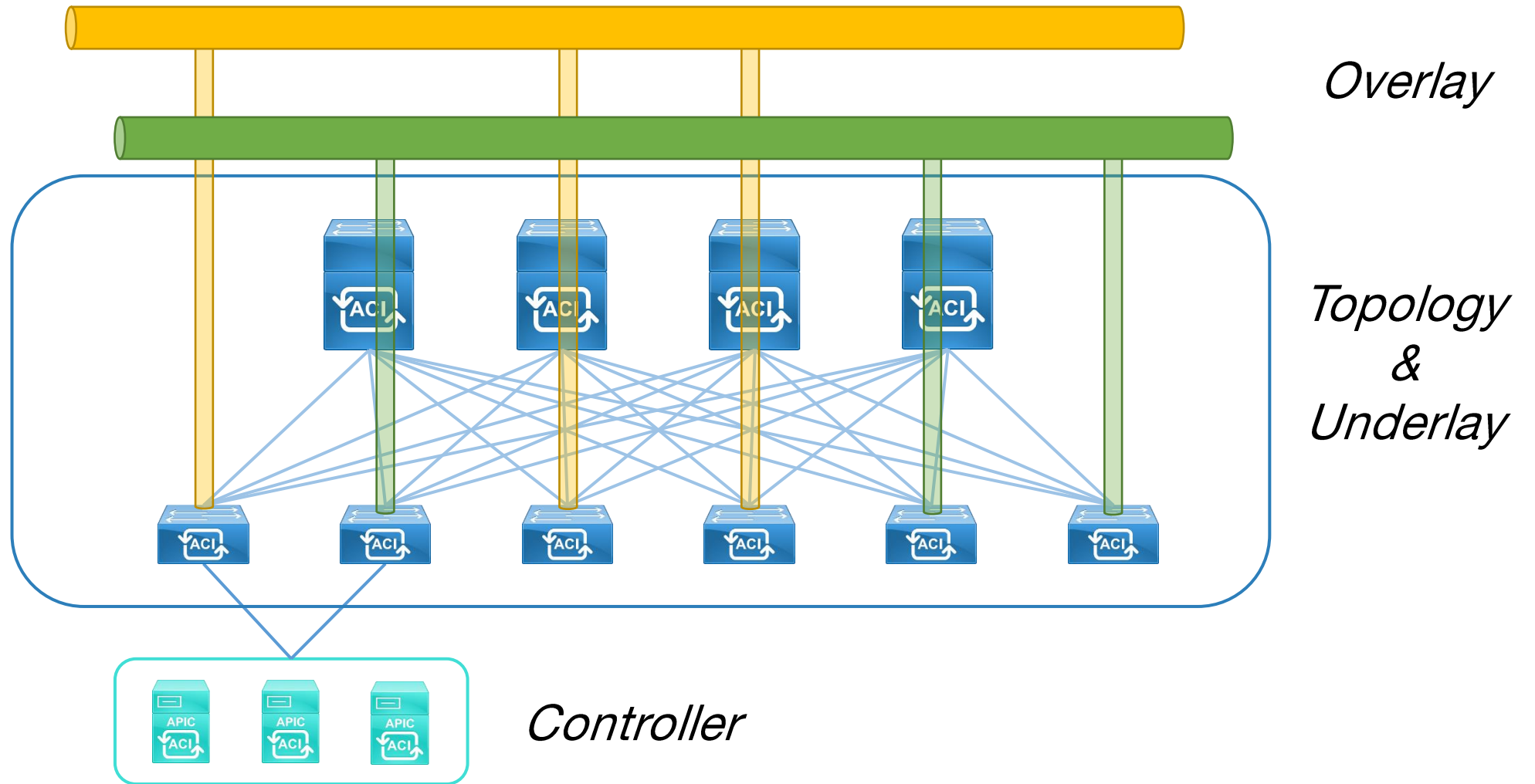


1. Cisco ACI Architectural Components
2. Fabric Architecture – Topology
  1. Clos Network
  2. Leaf and Spine... Why?
3. Fabric Architecture – Underlay
  1. Layer2 vs Layer3
4. Fabric Architecture – Overlay
  1. Virtual eXtensible LAN – VXLAN
    1. Acronyms & Definitions
    2. Frame Format
    3. Distributed Anycast Gateway
    4. L2VNI & L3VNI
    5. Flood & Learn
    6. Inter-VLAN Routing
    7. DEMO LAB0
5. Application Policy Infrastructure Controller
  1. APIC What is?
  2. APIC Clustering
  3. Hands-On LAB1

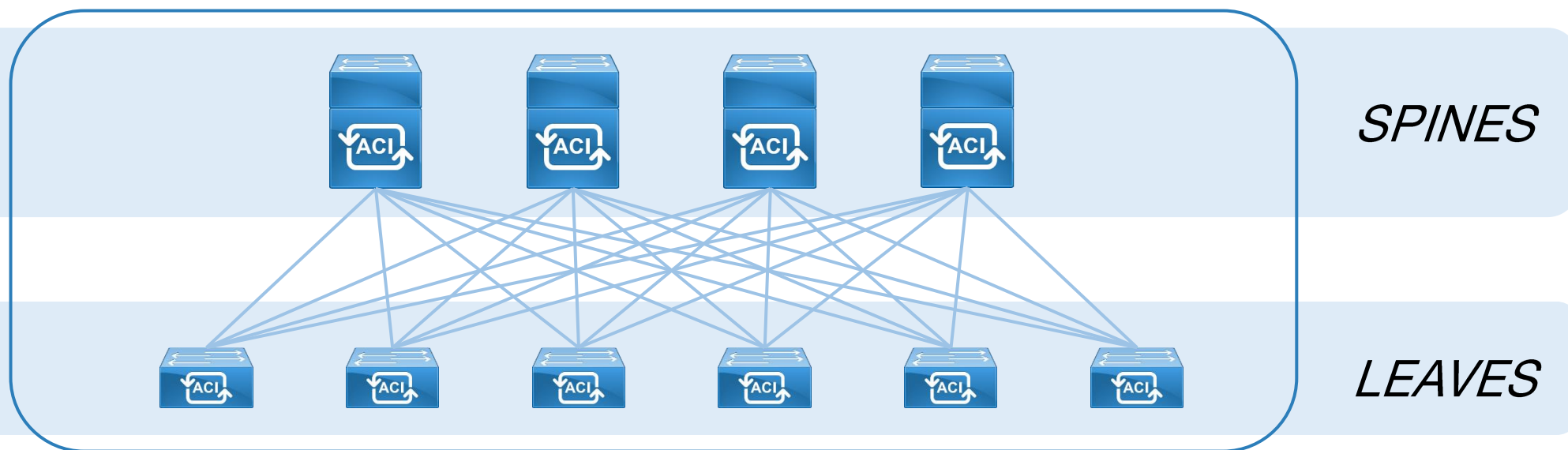




# Cisco ACI Architectural Components



# Fabric Architecture - Topology



## Leaf-Spine Topology

*(a.k.a. Folded-Clos Network, Complete Bi-partite Graph, ...)*

- Every leaf is connected to all and only spines.
- Every spine is connected to all and only leaves.
- No interconnections between leaves, nor between spines.

***Where does it come from?***



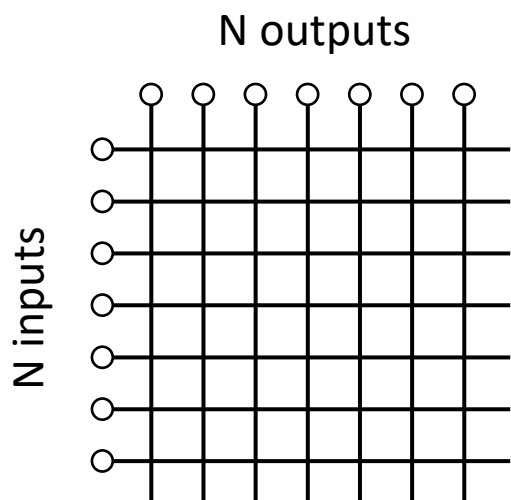


# Clos Network

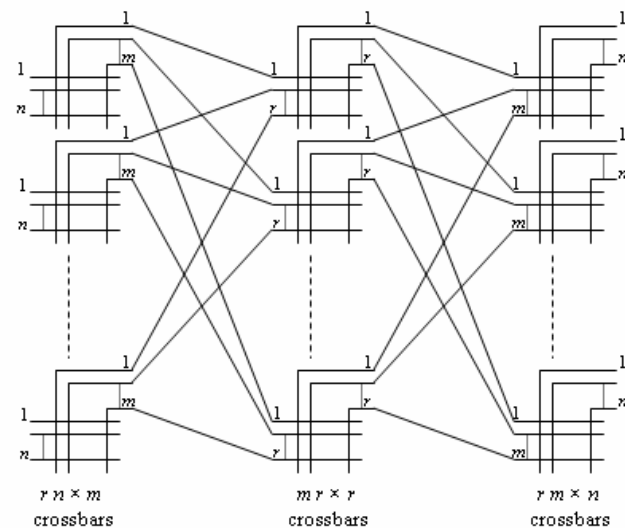


Charles Clos, "A study of Non-Blocking Switching Networks" (1953)

<https://archive.org/details/bstj32-2-406/page/n1/mode/2up>



Crosspoints =  $N^2$



3 Stages -- Crosspoints =  $6N^{3/2} - 3N$

5 Stages -- Crosspoints =  $16N^{4/3} - 14N + 3N^{2/3}$

7 Stages ...

# Clos Network – In-Depth Information



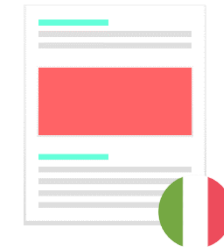
*Looking for...*

*...what is a bi-partite graph?*



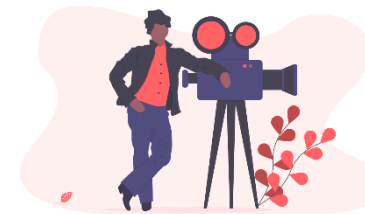
*Wikipedia*

*...a general discussion on the topic?*



*Reiss Romoli*

*...simple explanation and a little bit of formalism?*



*Coursera – Princeton University*

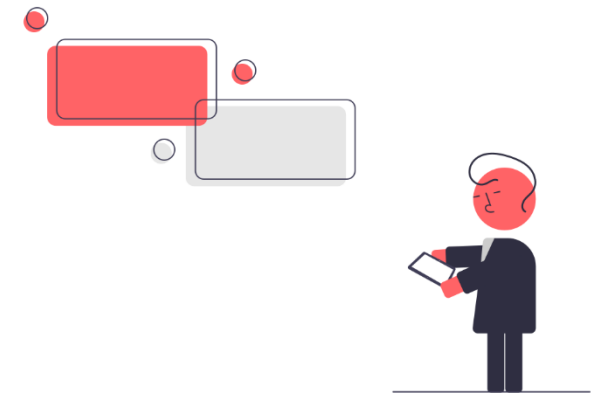
# *Leaf and Spine... Why?*



***New Applications***

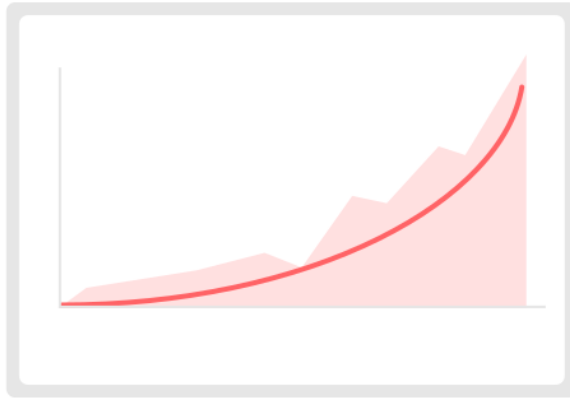


***New Requirements***



***New Designs***

# Leaf and Spine... Why?



## Traffic Growth

Efficient and effective forwarding of traffic.

- ECMP forwarding.

***“Overall, EAST-WEST TRAFFIC (traffic within the data center and traffic between data centers) represents 86 percent of total data center by 2020.”***

*Cisco Global Cloud Index (2015-2020)*

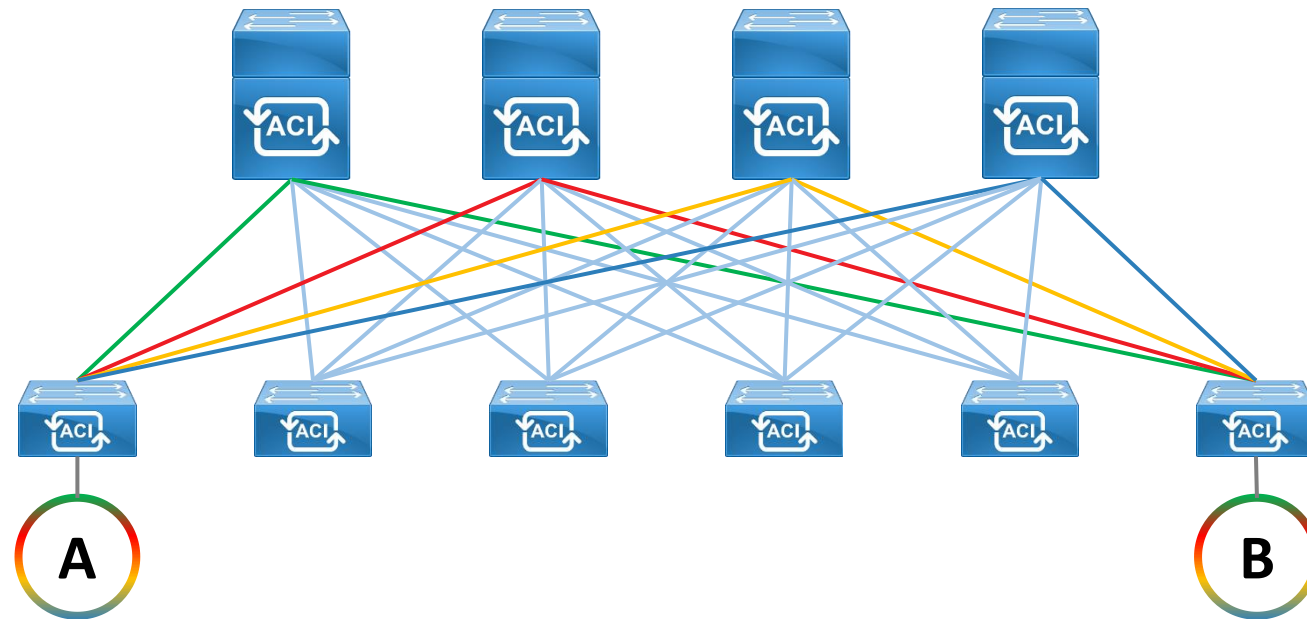
# Leaf and Spine... Why?



## Traffic Growth

Efficient and effective forwarding of traffic.

- ECMP forwarding.



# Leaf and Spine... Why?



## Performance

Consistent and deterministic latency for all traffic.

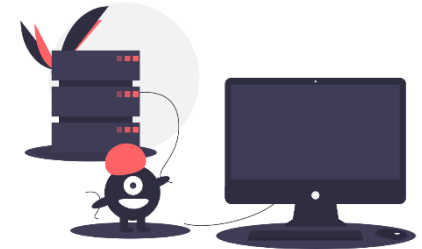
- Fixed number of hop between any couple of leaves.



## Resiliency

High availability and protection against link/node failure.

- Dense and redundant topology.



## Flexible Scaling

Flexibility as regards to subscription ratio.

- No need to re-design the network when scaling.





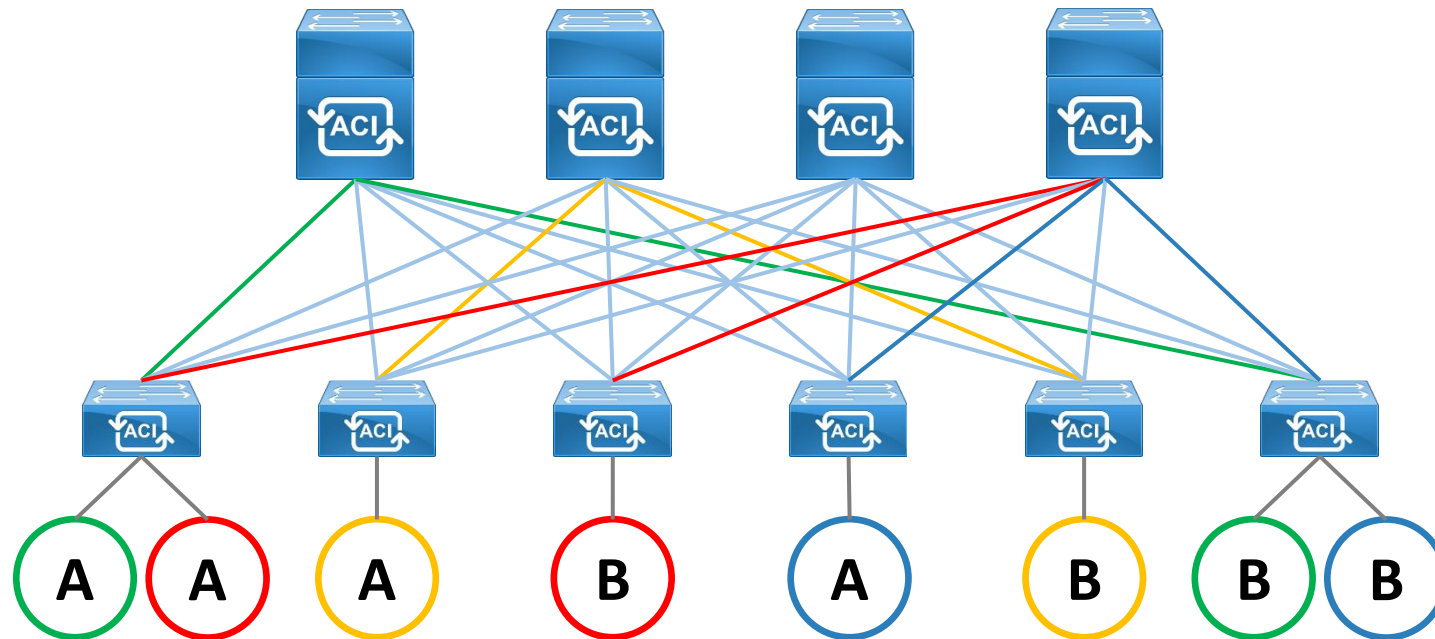
# Leaf and Spine... Why?



## Performance

Consistent and deterministic latency for all traffic.

- Fixed number of hop between any couple of leaves.



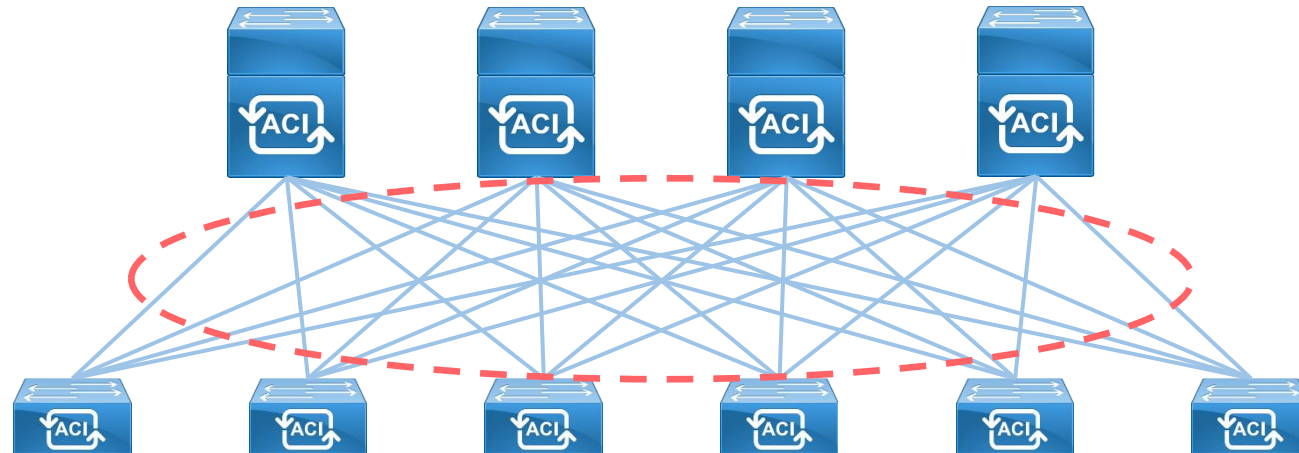
# Leaf and Spine... Why?



## Resiliency

High availability and protection against link/node failure.

- Dense and redundant topology.



# Leaf and Spine... Why?

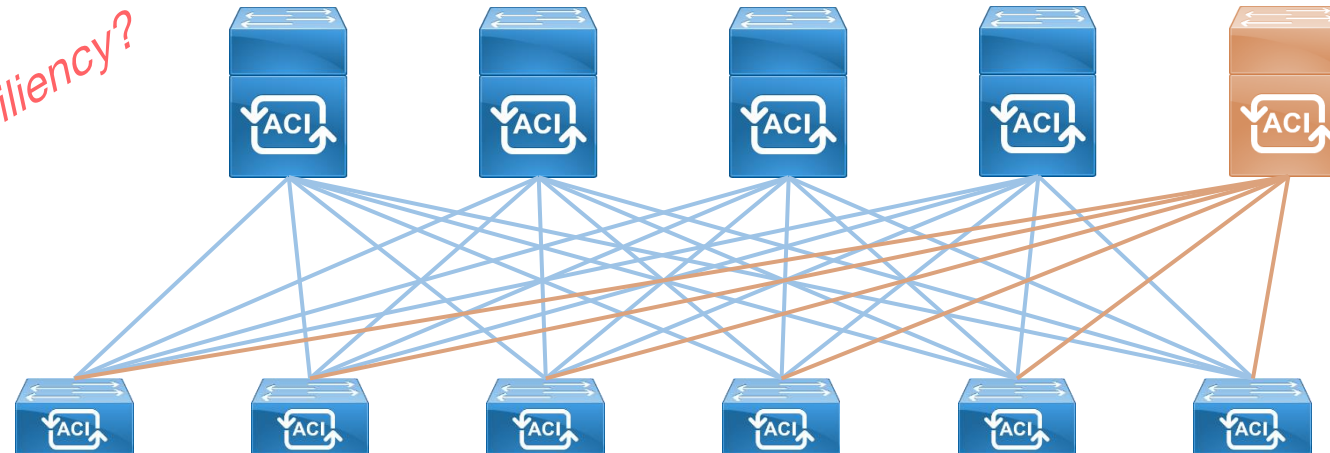


## Flexible Scaling

Flexibility as regards to subscription ratio.

- No need to re-design the network when scaling.

*Need more bandwidth & resiliency?*



**ADD SPINES**

# Leaf and Spine... Why?

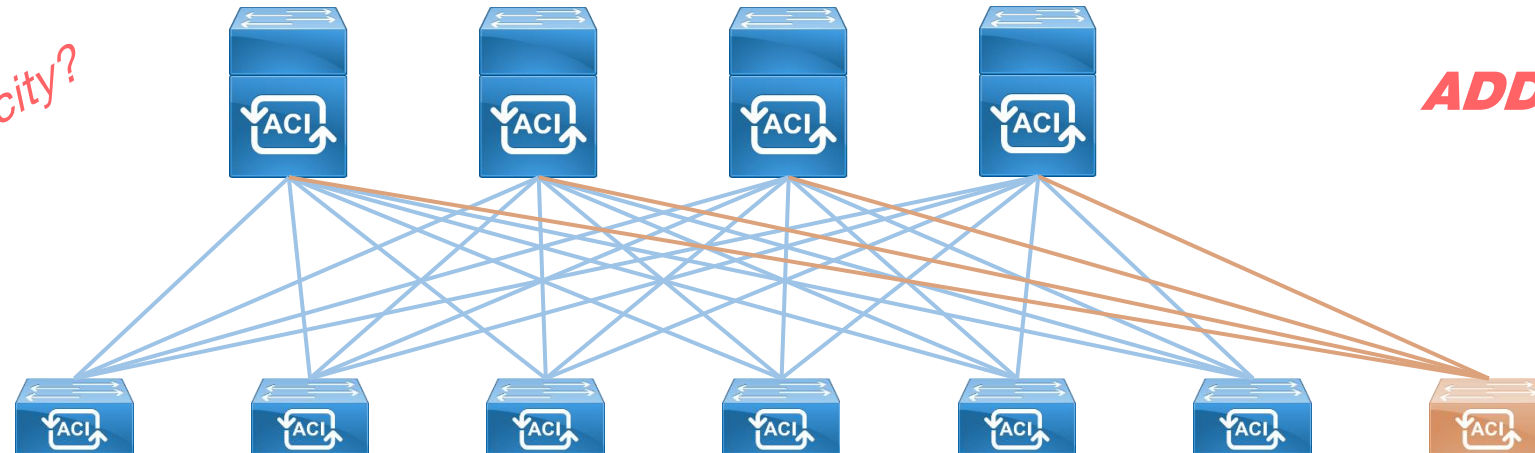


## Flexible Scaling

Flexibility as regards to subscription ratio.

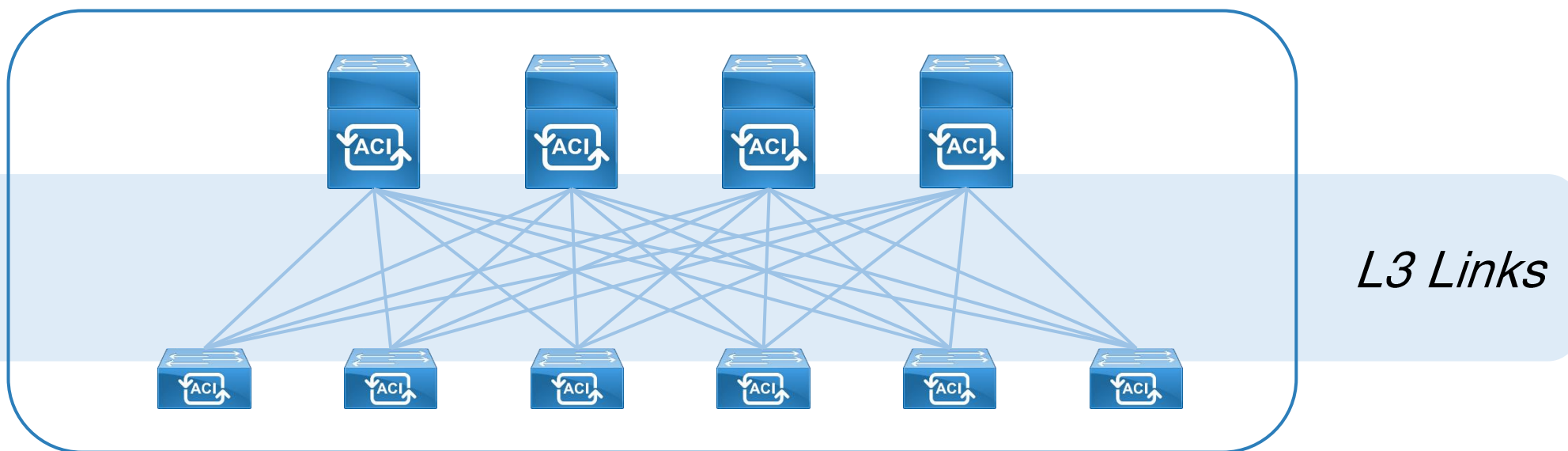
- No need to re-design the network when scaling.

*Need more ports & capacity?*



**ADD LEAVES**

# Fabric Architecture - Underlay



## Layer 3 Core

- All the links in the fabric are routed.
- IP unnumbered is used to save IP addresses.
- Link-State IGP: IS-IS.



# Layer 2 (STP) vs Layer 3 (IP) Underlay



## **Spanning Tree Protocol**

**BLK ports = Wasted Resources**

*Redundancy causes loops!*

**ECMP**



**1 Shortest Path Spanning Tree per LAN**



## **IP + Link-State IGP**

**All links are used!**

*...potentially, it depends on topology and configuration.*

**ECMP**

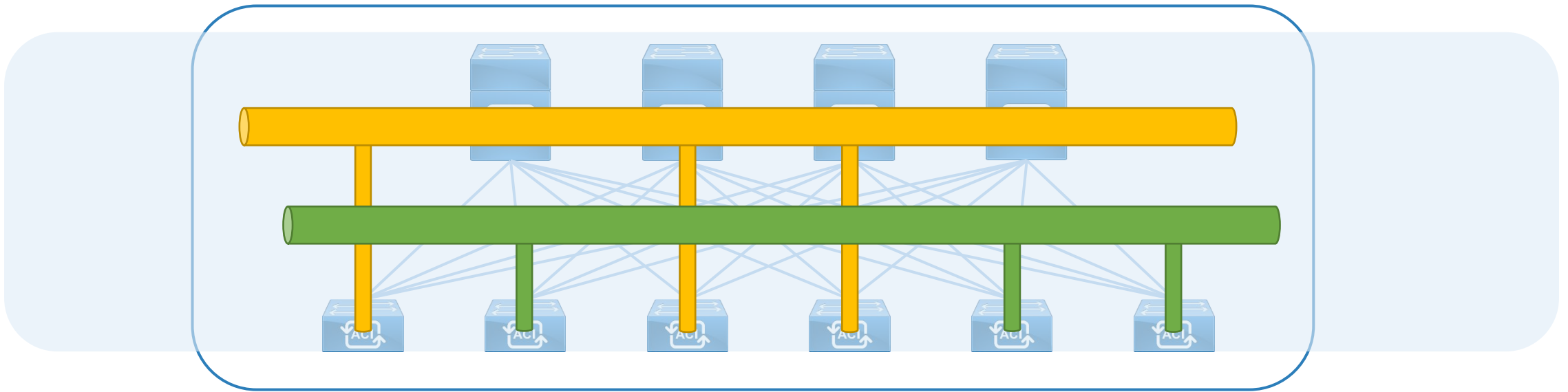


**1 Shortest Path Spanning Tree per node**

*Dijkstra guaranteed!*

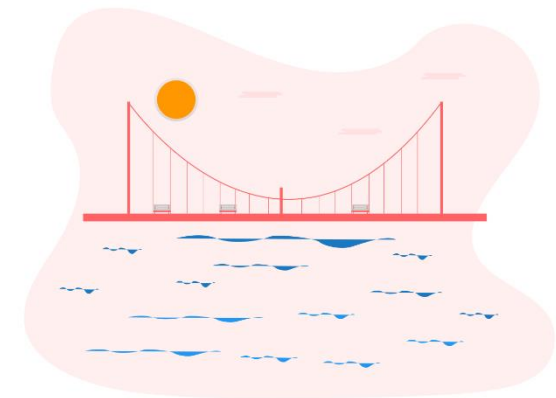


# Fabric Architecture - Overlay



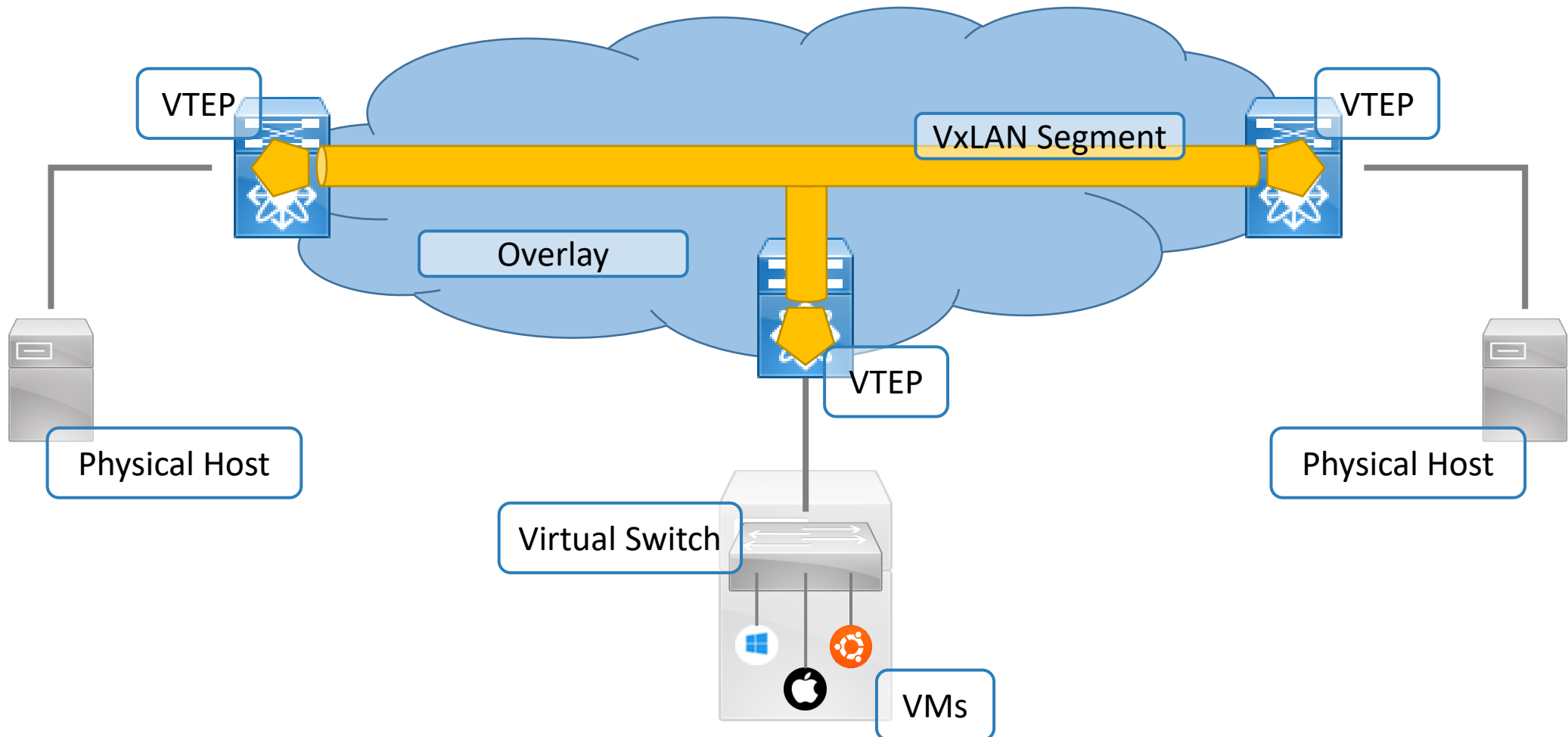
## Overlay: Virtual eXtensible LAN (VXLAN)

- Standard: IETF RFC 7348 (2014)
- Layer 2 overlay scheme on a Layer 3 network.
- Tunneling scheme.



## Virtual eXtensible LAN – VXLAN

*View from 20.000 feet*



# Virtual eXtensible LAN – VXLAN



## Acronyms & Definitions



*IETF RFC7348, “Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks” (2014)*

<https://tools.ietf.org/html/rfc7348>

### VTEP: Virtual Tunnel End Point

An entity that originates and/or terminate VXLAN tunnels.

### VXLAN Segment

VXLAN Layer 2 overlay over which VMs communicate.

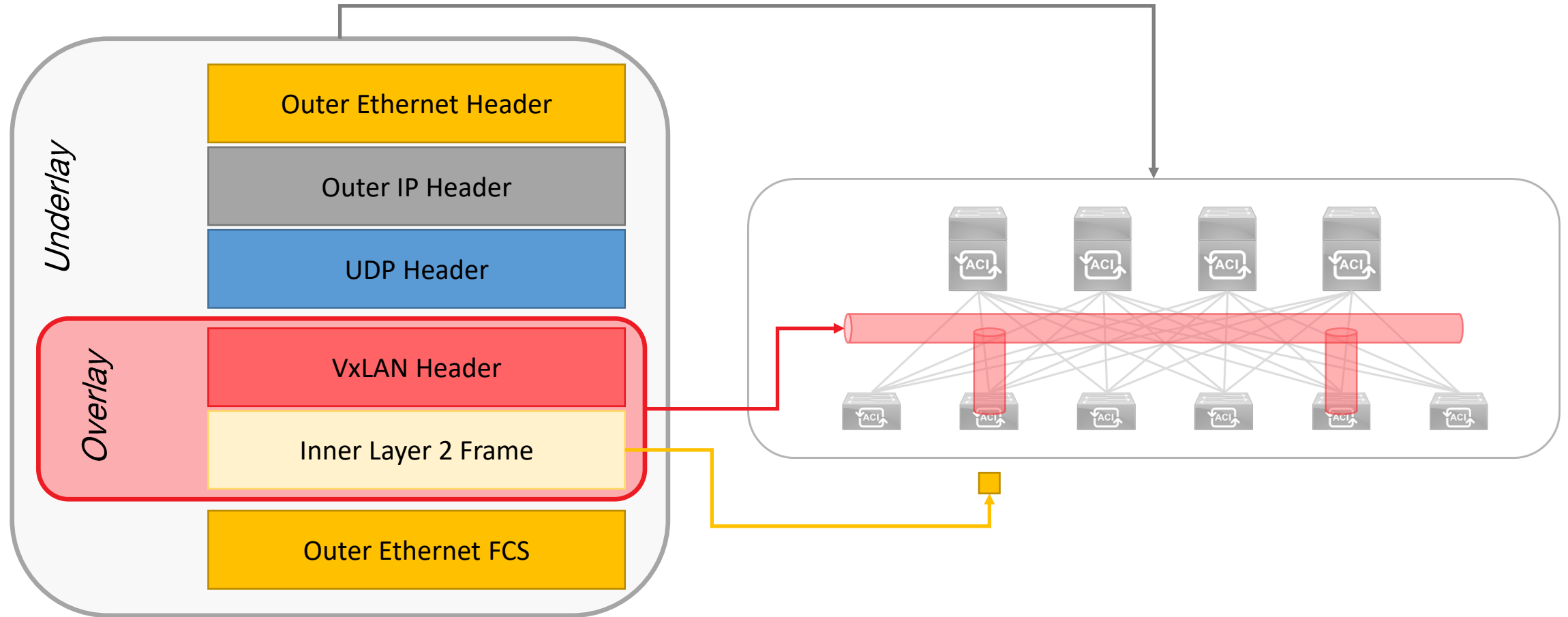
### VNI: VXLAN Network Identifier (or VXLAN Segment ID)



# Virtual eXtensible LAN - VXLAN



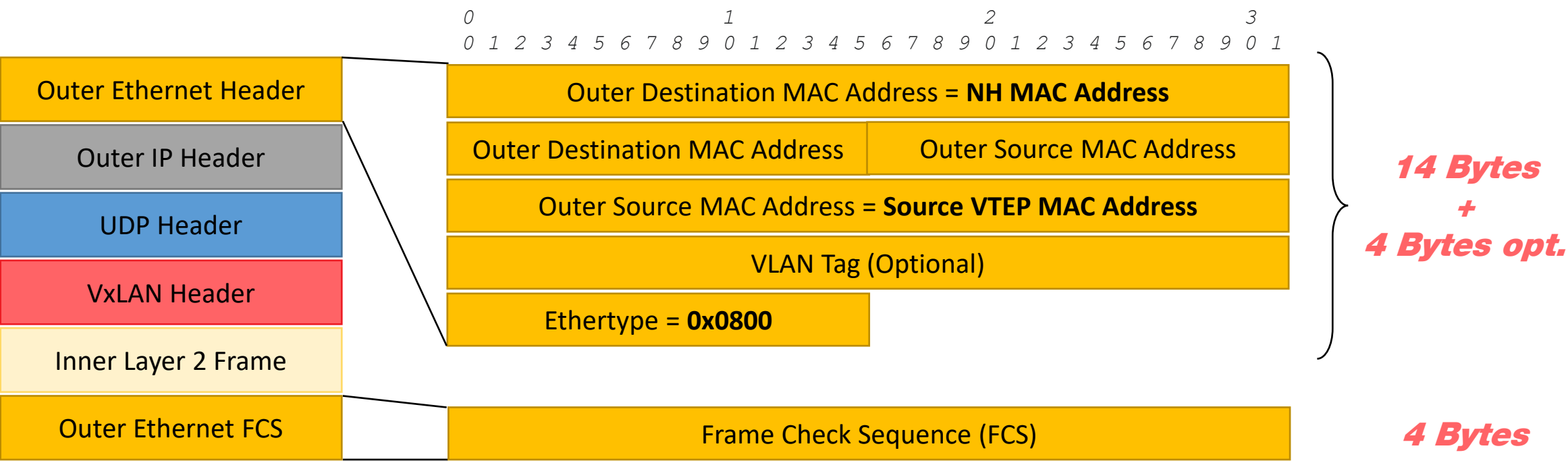
## Frame Format





# Virtual eXtensible LAN - VXLAN

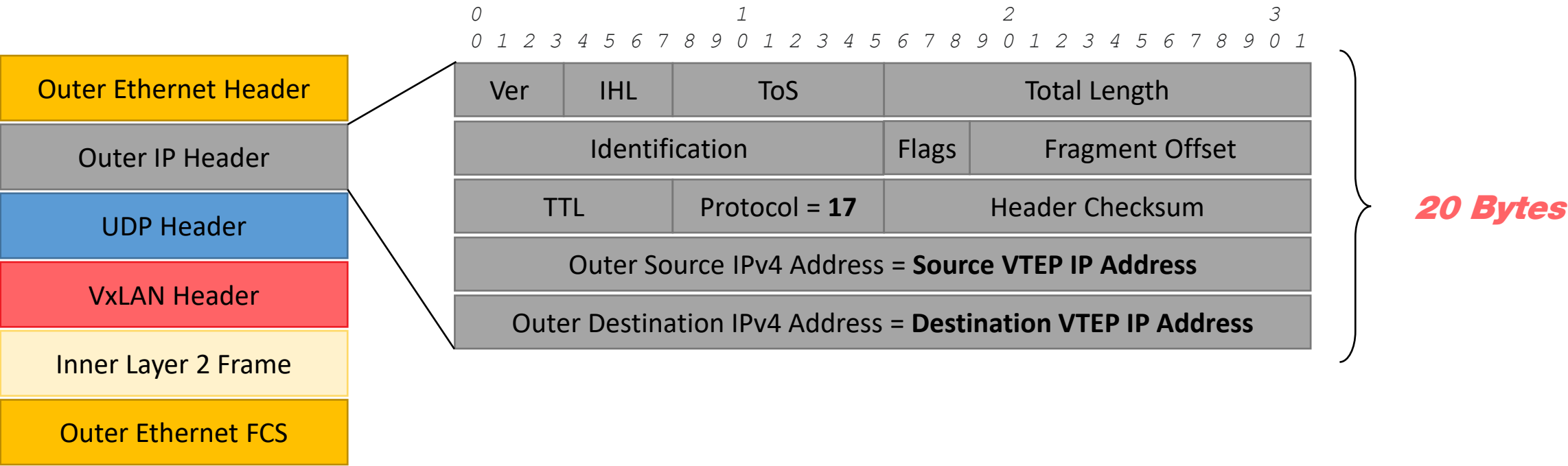
## Frame Format





# Virtual eXtensible LAN - VXLAN

## Frame Format

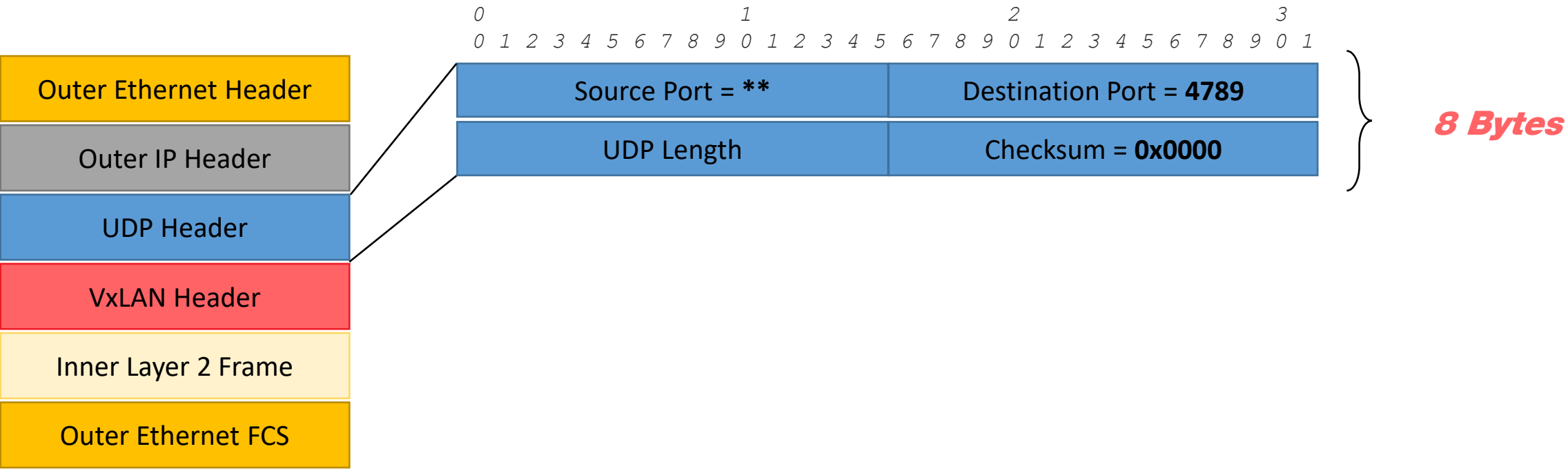






# Virtual eXtensible LAN - VXLAN

## Frame Format

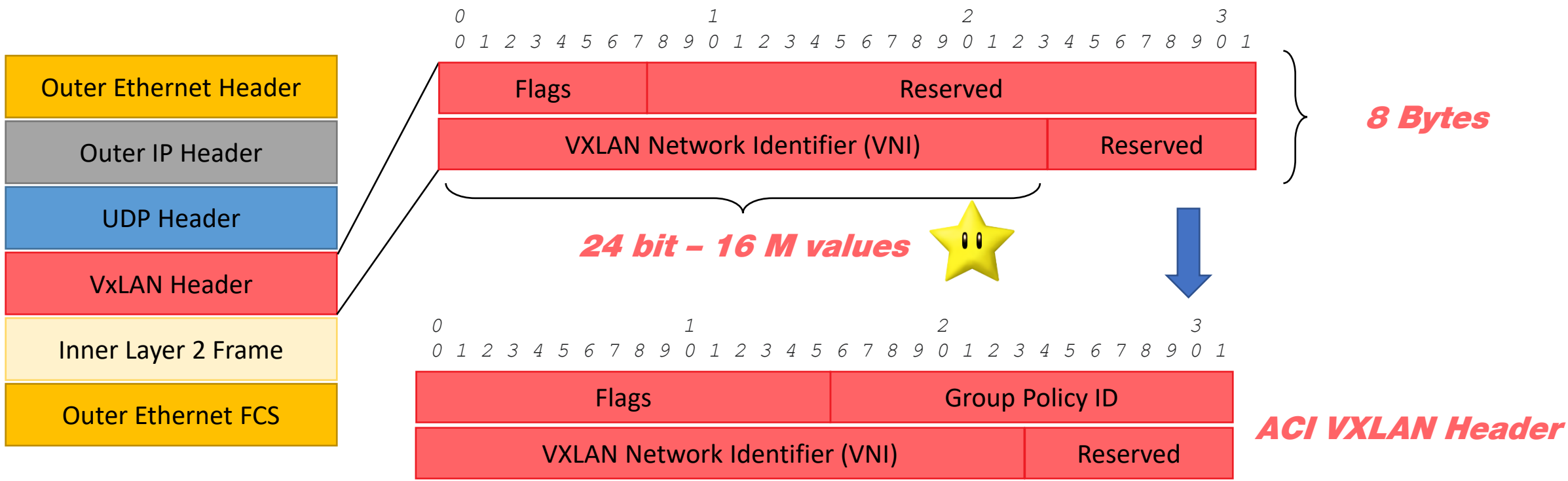


**\*\*** *It is recommended that UDP Source Port value be calculated using a hash of fields from the inner packet (e.g. L2/L3/L4 headers of Inner Layer 2 Frame). This enables entropy for the ECMP/load-balancing of the traffic across the VxLAN overlay.*



# Virtual eXtensible LAN - VXLAN

## Frame Format

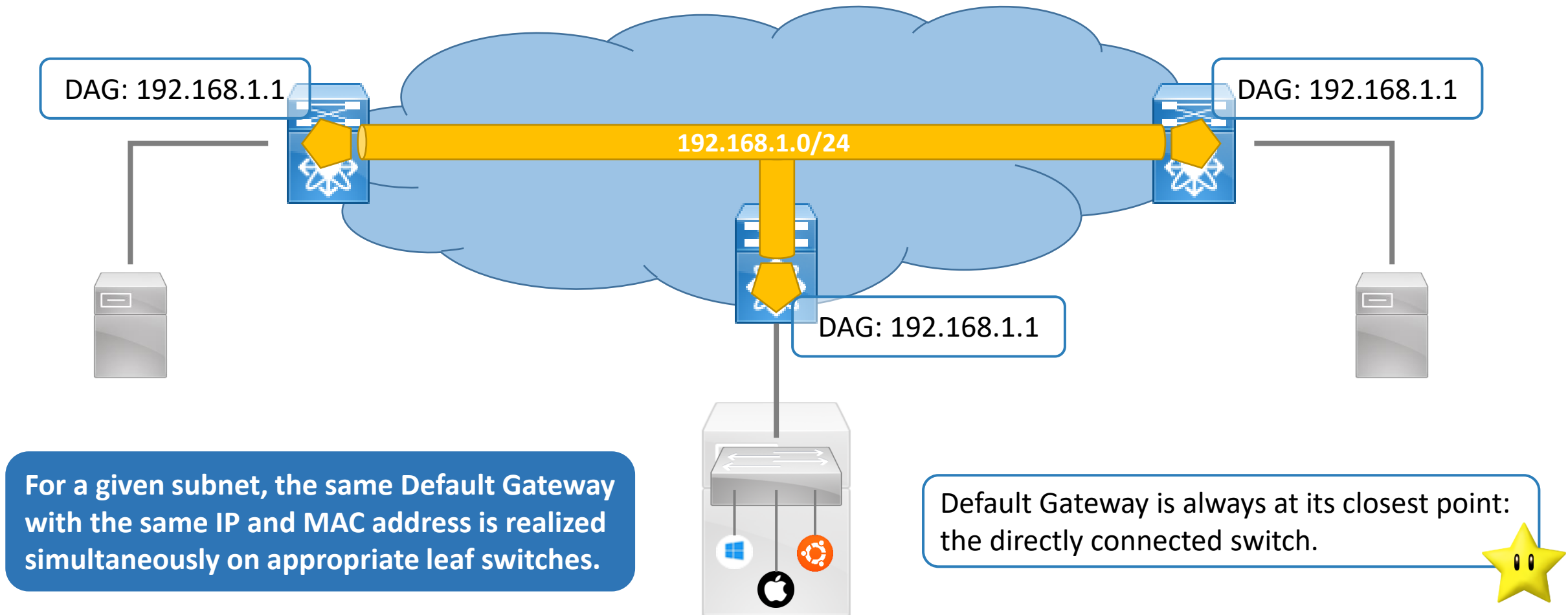


*IETF draft (expired), "VXLAN Group Policy Option" (2019)*  
<https://tools.ietf.org/html/draft-smith-vxlan-group-policy-05>



# Virtual eXtensible LAN - VXLAN

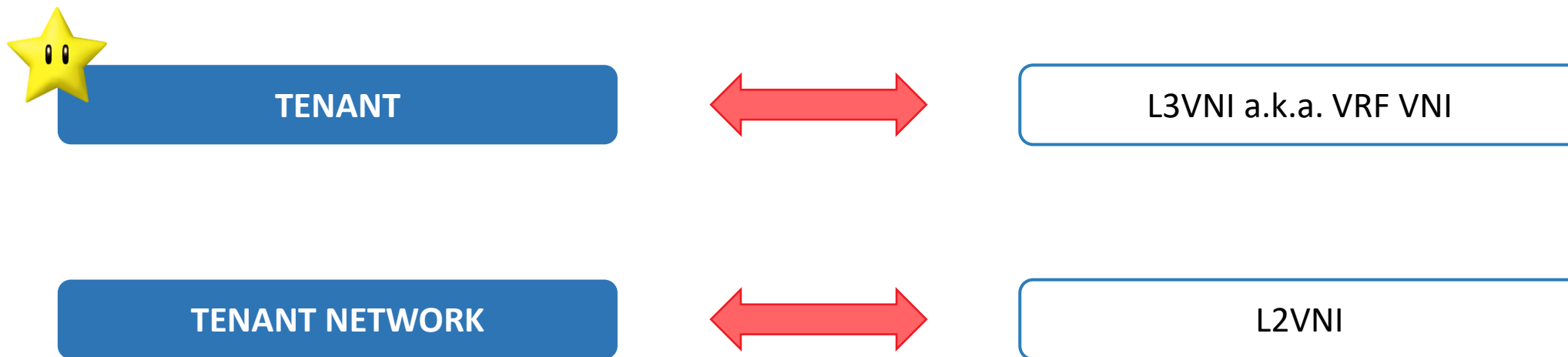
*Distributed Anycast Gateway*



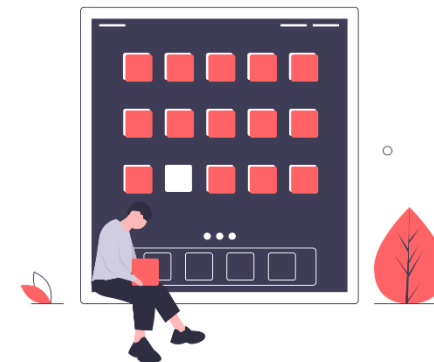


# Virtual eXtensible LAN - VXLAN

*L2VNI & L3VNI*



***The VNIs all come from the same  $2^{24}-1$  pool represented by the 24-bit VNI identifier carried in the VXLAN header.***





# Virtual eXtensible LAN - VXLAN

## Addressed Problems



### Scalability



From 4094 (VLAN) to 16M (VXLAN) possible L2 Domains.

### Multitenancy



Supported → L3VNIs isolate different tenants traffics.

### Forwarding Optimization

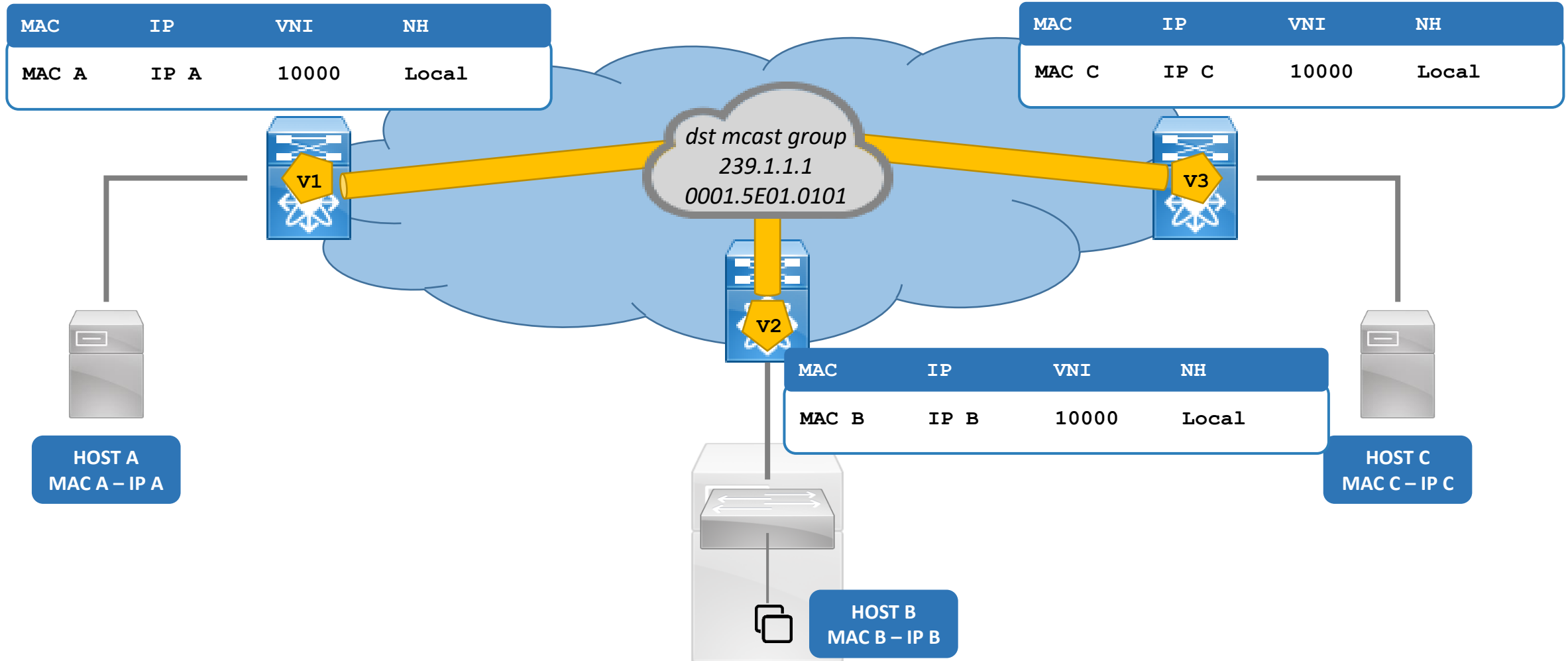


Distributed Anycast Gateway ensures traffic is optimally forwarded within the fabric without going through any tromboning.

# Virtual eXtensible LAN – VXLAN



## Flood & Learn

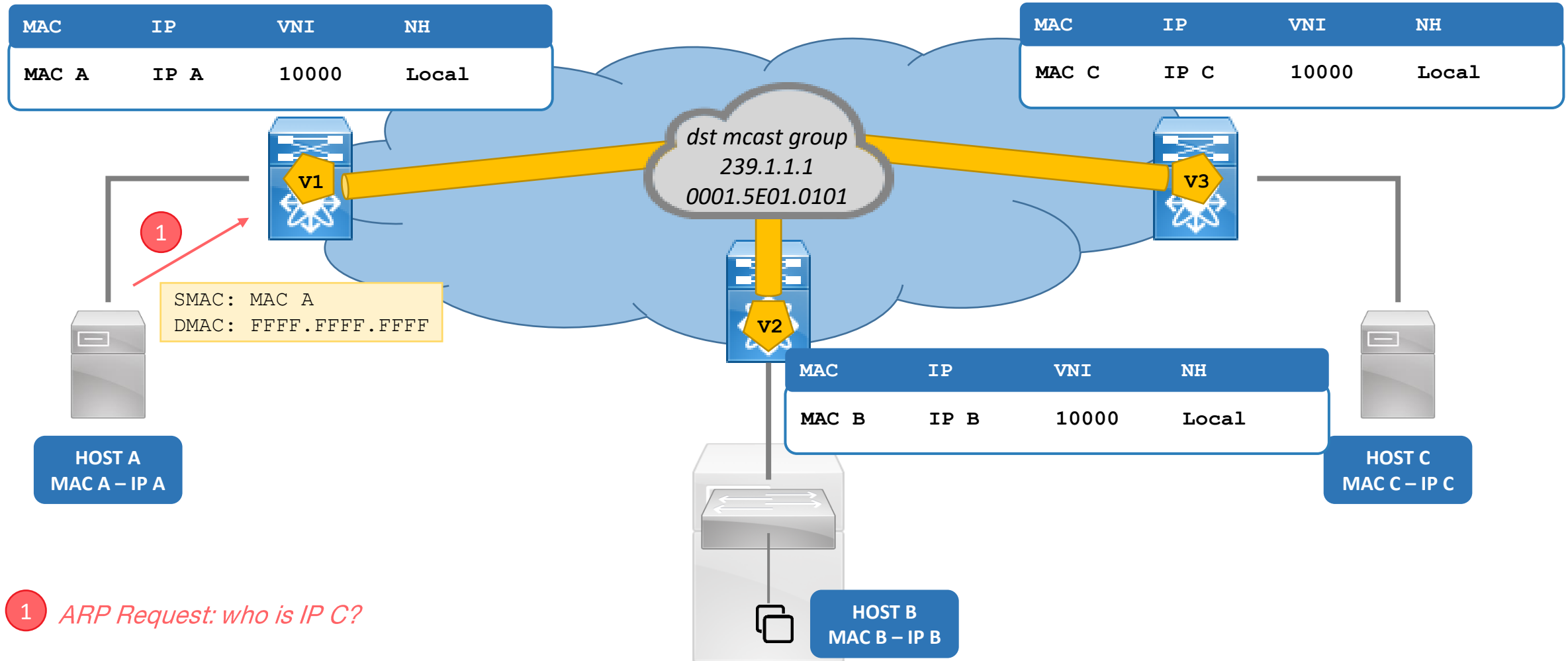




# Virtual eXtensible LAN - VXLAN



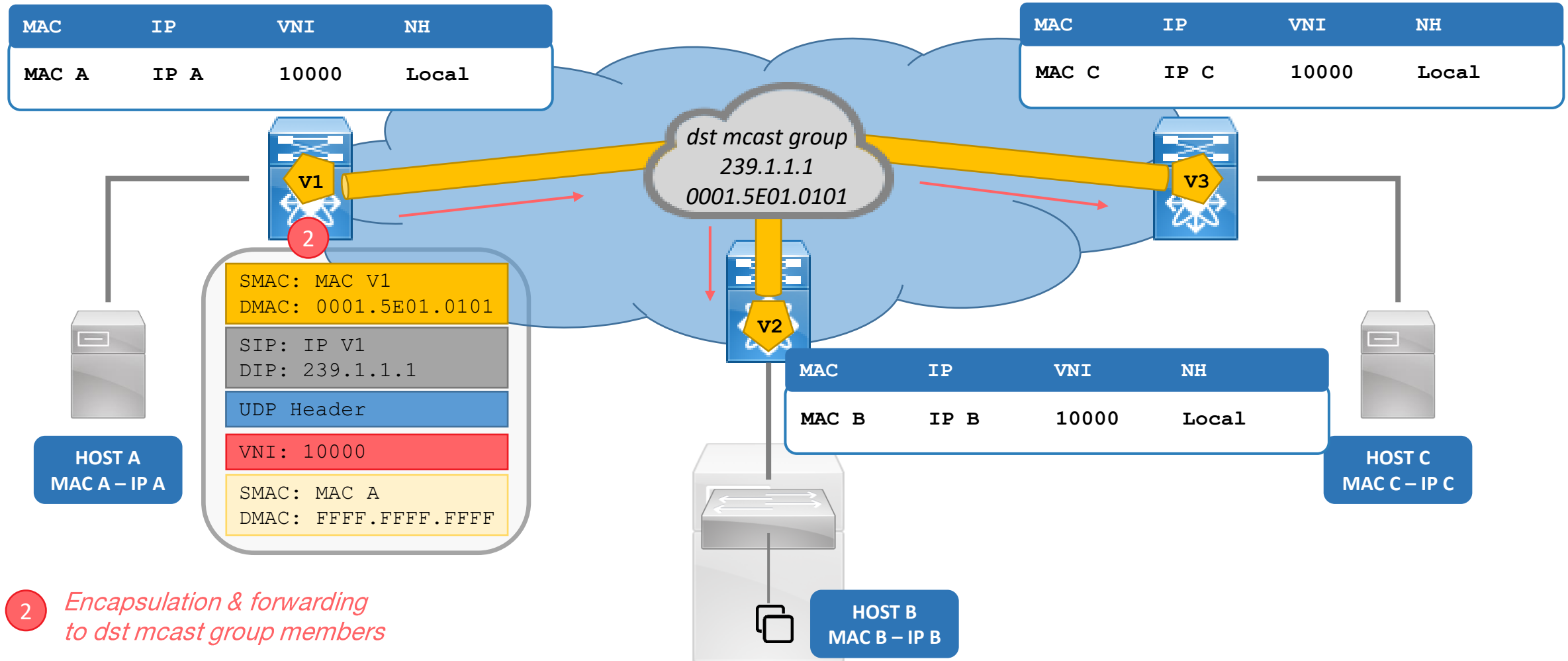
## Flood & Learn



# Virtual eXtensible LAN – VXLAN



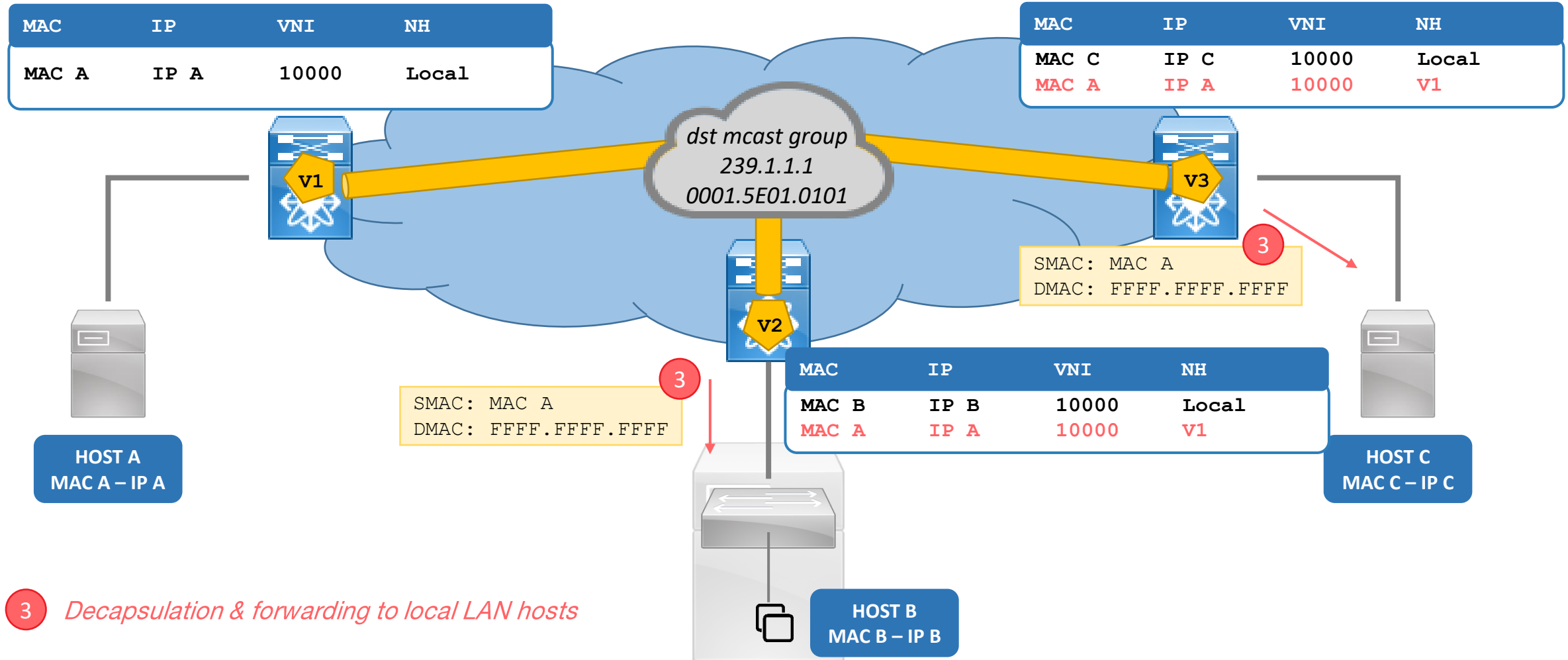
*Flood & Learn*



# Virtual eXtensible LAN - VXLAN



## Flood & Learn

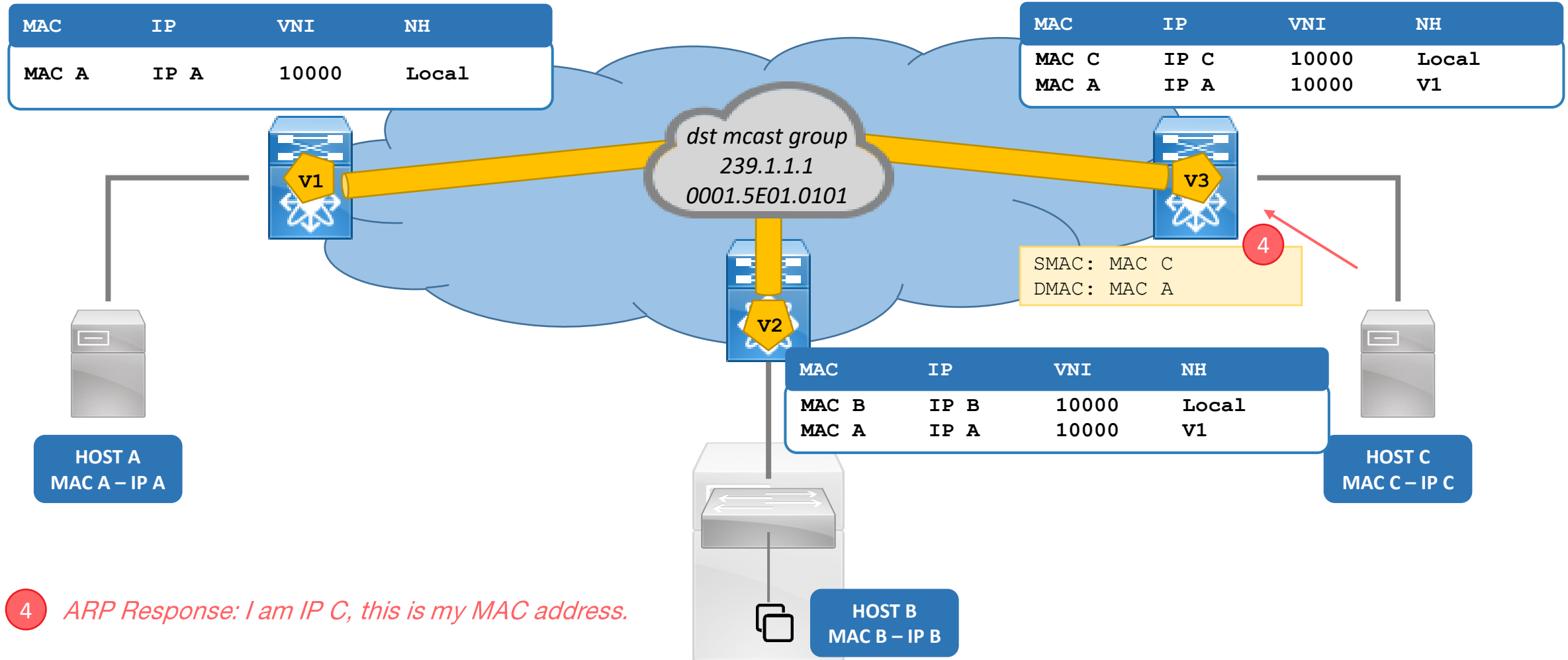


3 Decapsulation & forwarding to local LAN hosts

# Virtual eXtensible LAN - VXLAN



## Flood & Learn

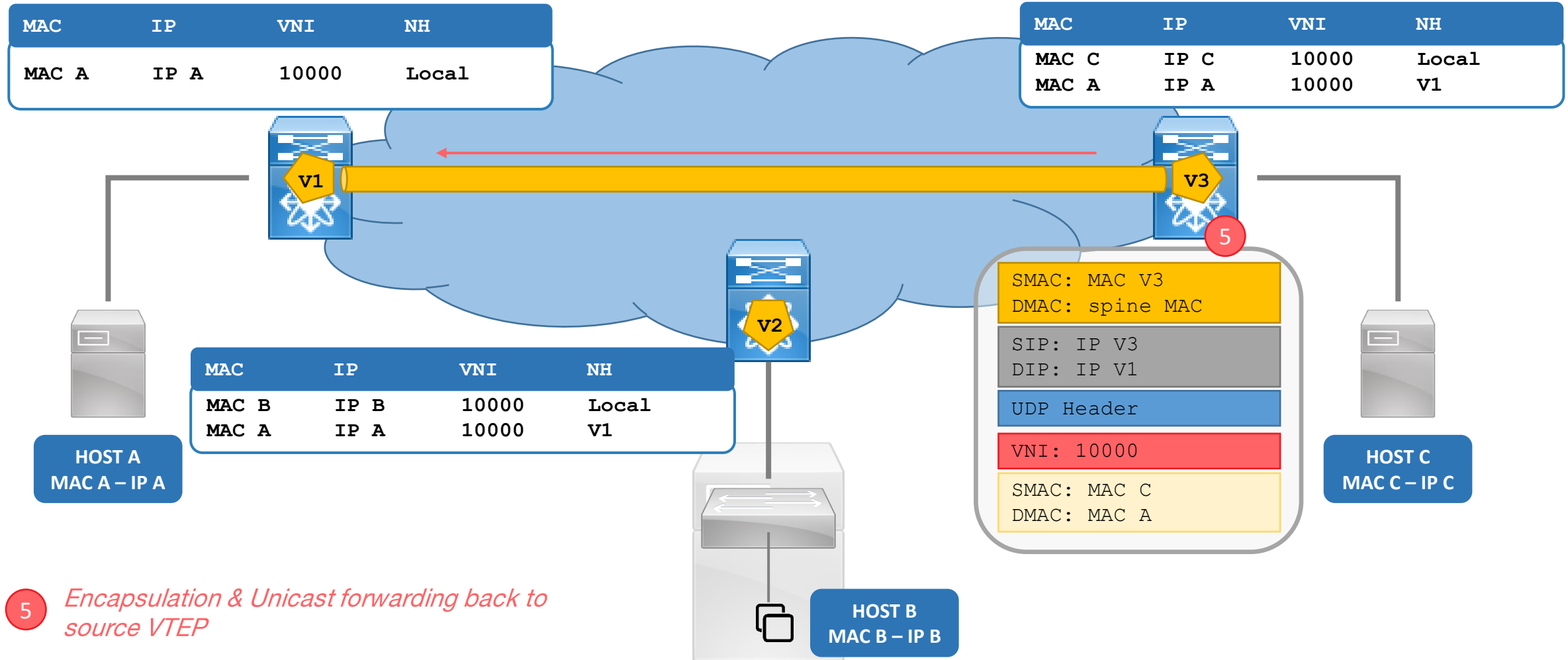


4 ARP Response: I am IP C, this is my MAC address.

# Virtual eXtensible LAN - VXLAN



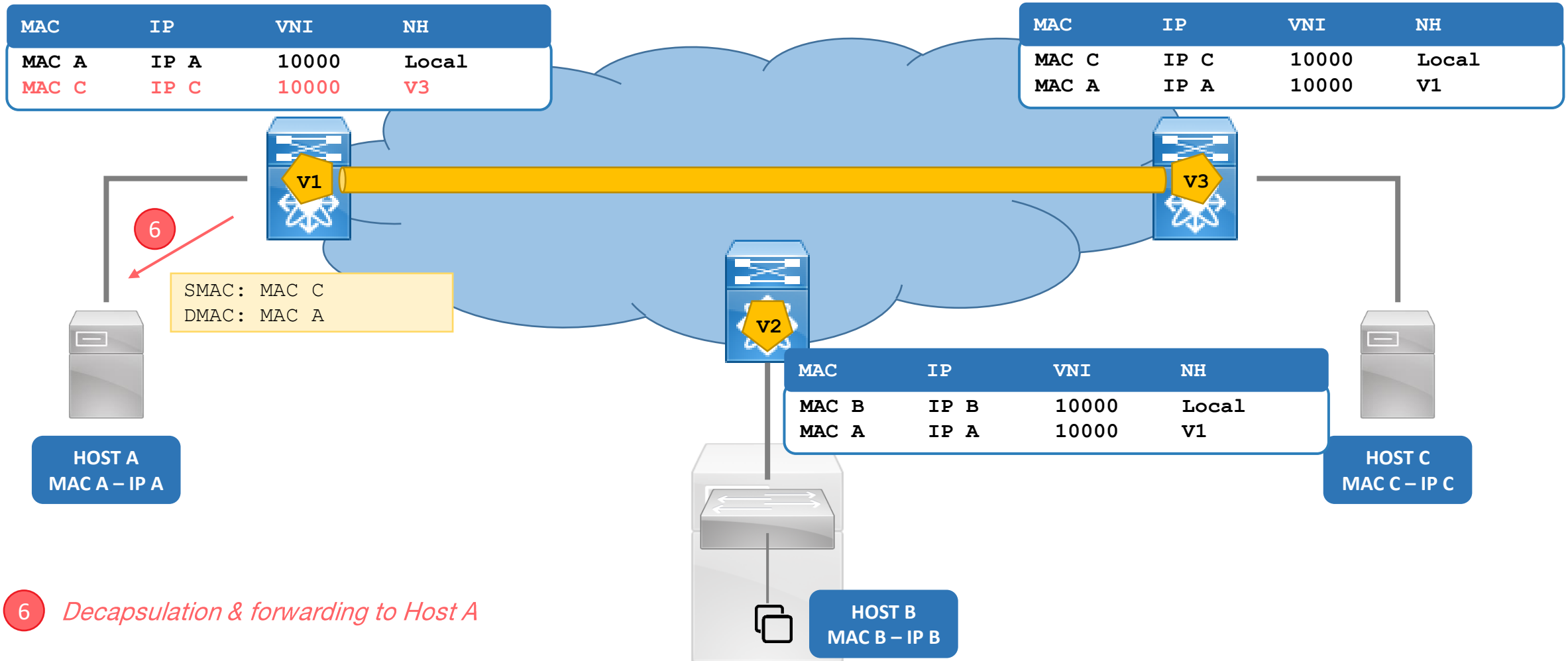
*Flood & Learn*



# Virtual eXtensible LAN - VXLAN



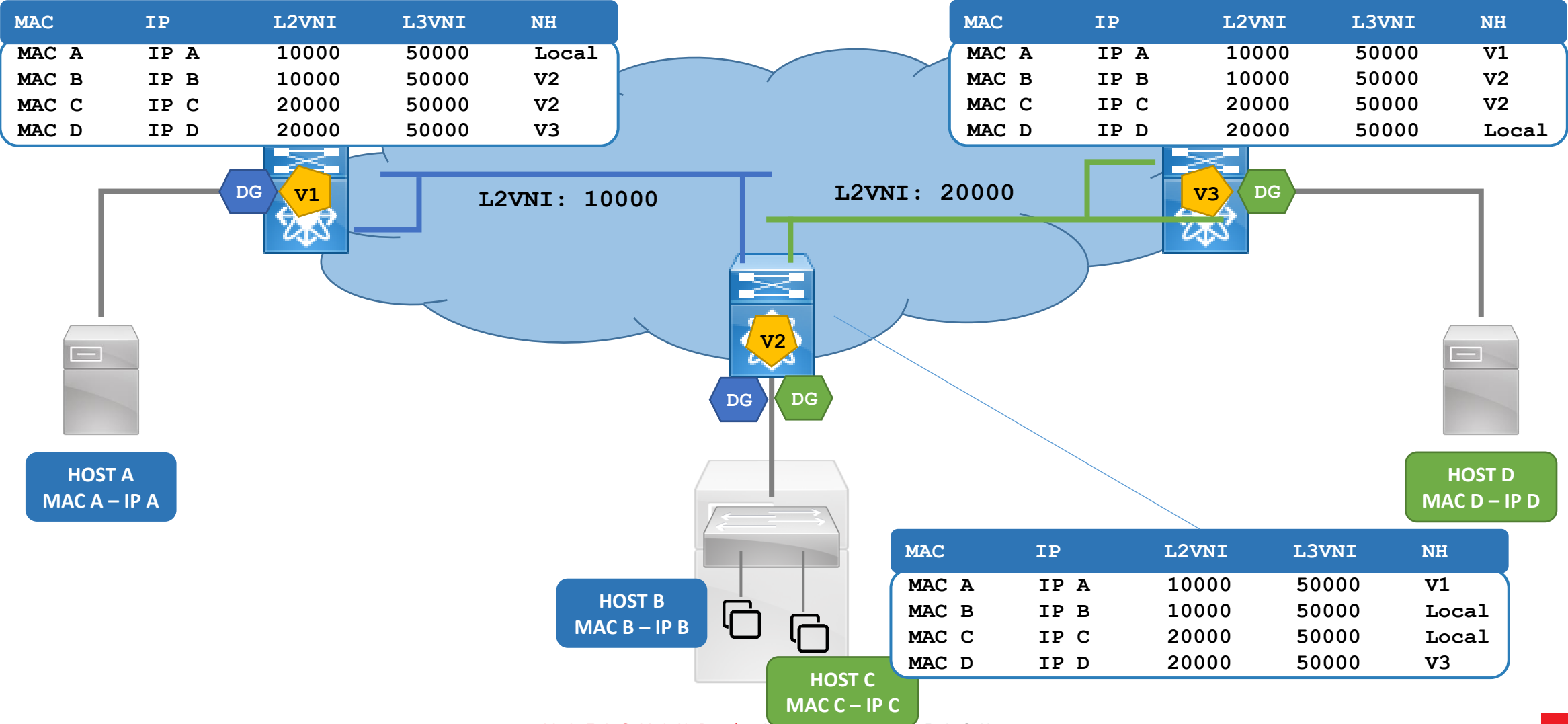
## Flood & Learn



# Virtual eXtensible LAN - VXLAN



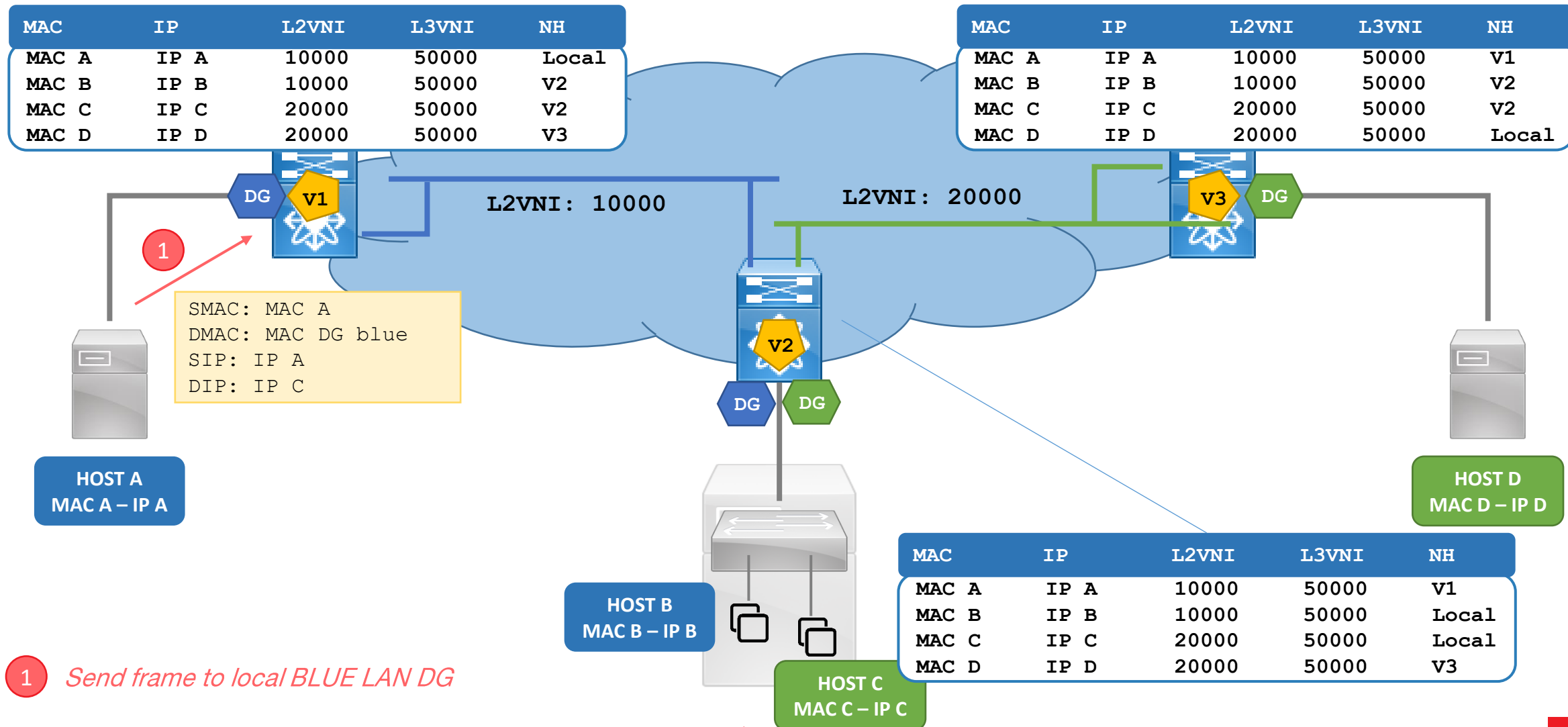
## Inter-VLAN Routing



# Virtual eXtensible LAN - VXLAN



## Inter-VLAN Routing



1 Send frame to local BLUE LAN DG

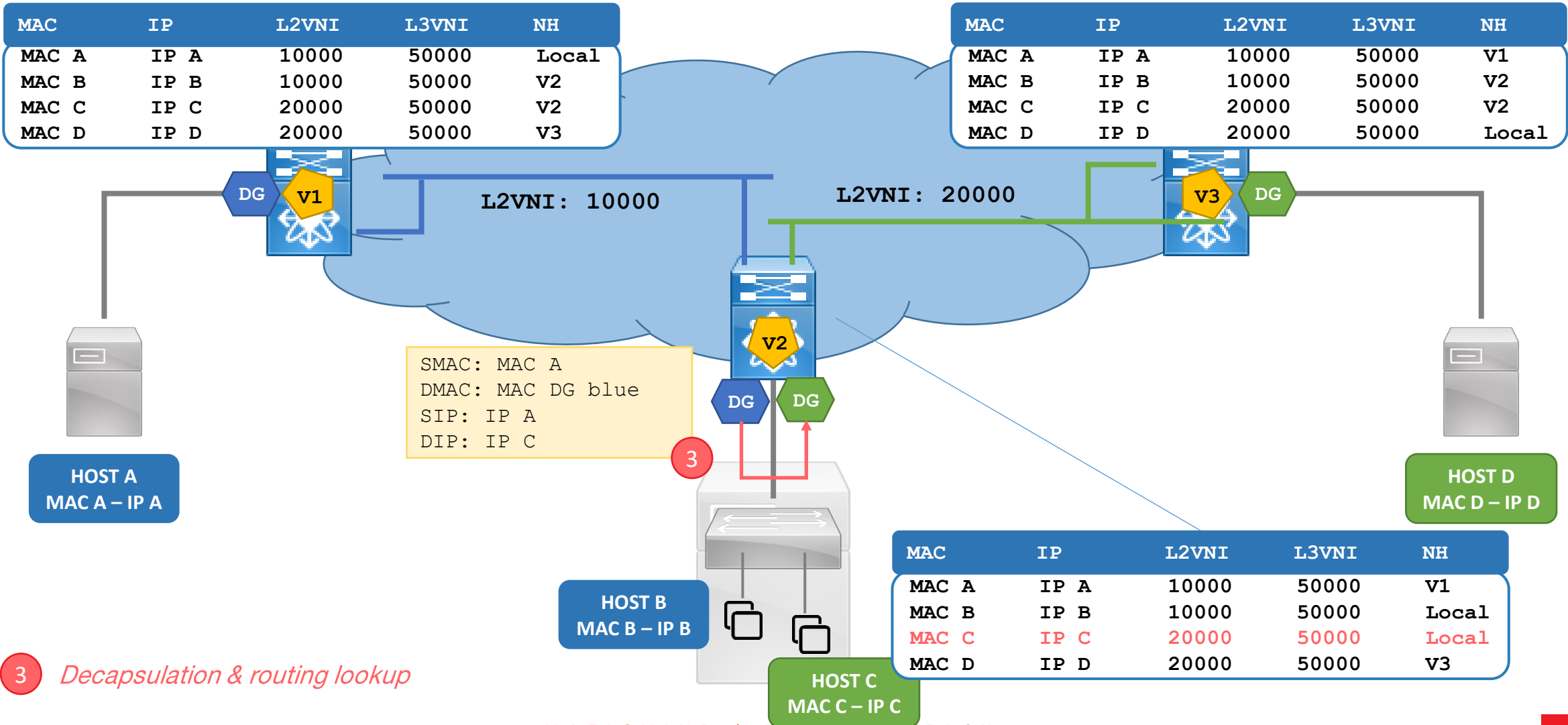




# Virtual eXtensible LAN - VXLAN



## Inter-VLAN Routing

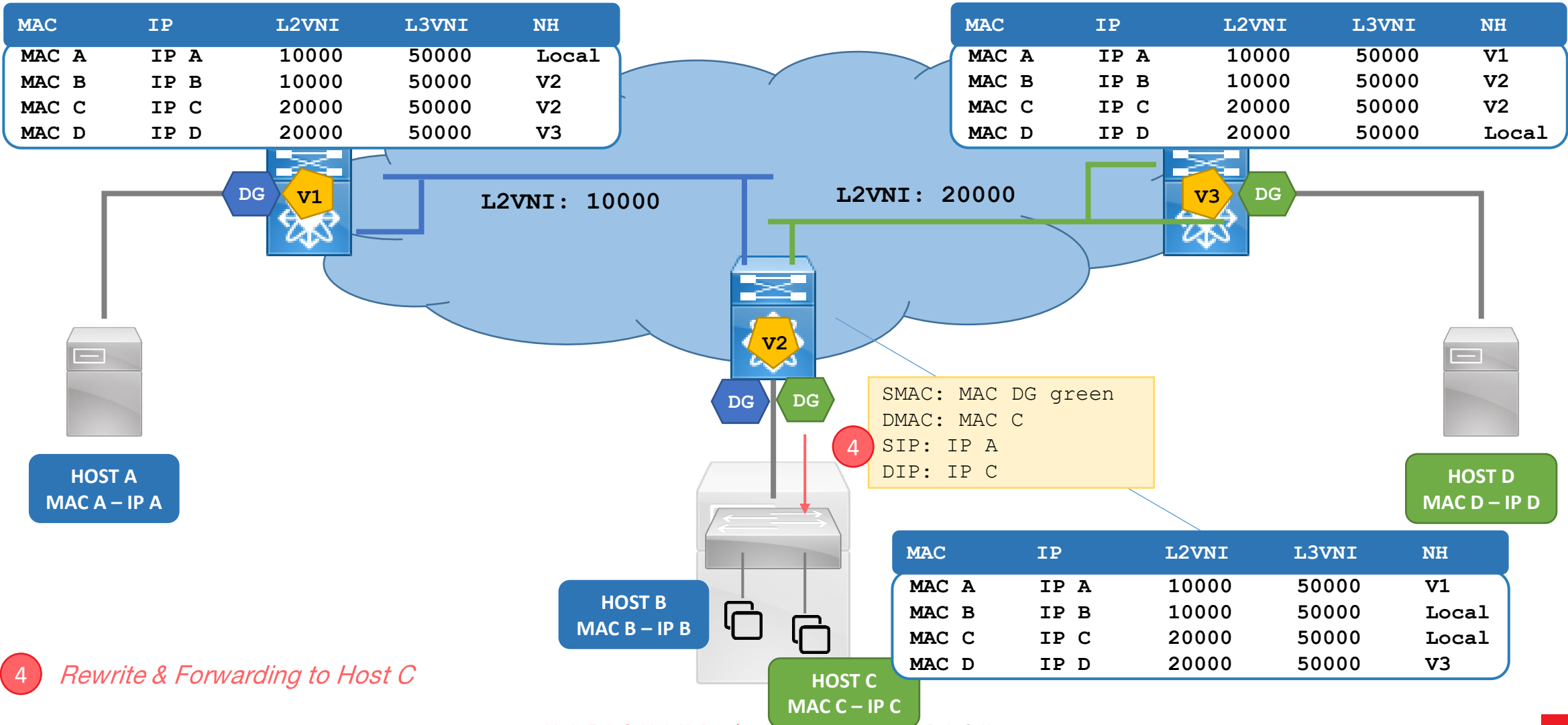


3 Decapsulation & routing lookup

# Virtual eXtensible LAN - VXLAN



## Inter-VLAN Routing

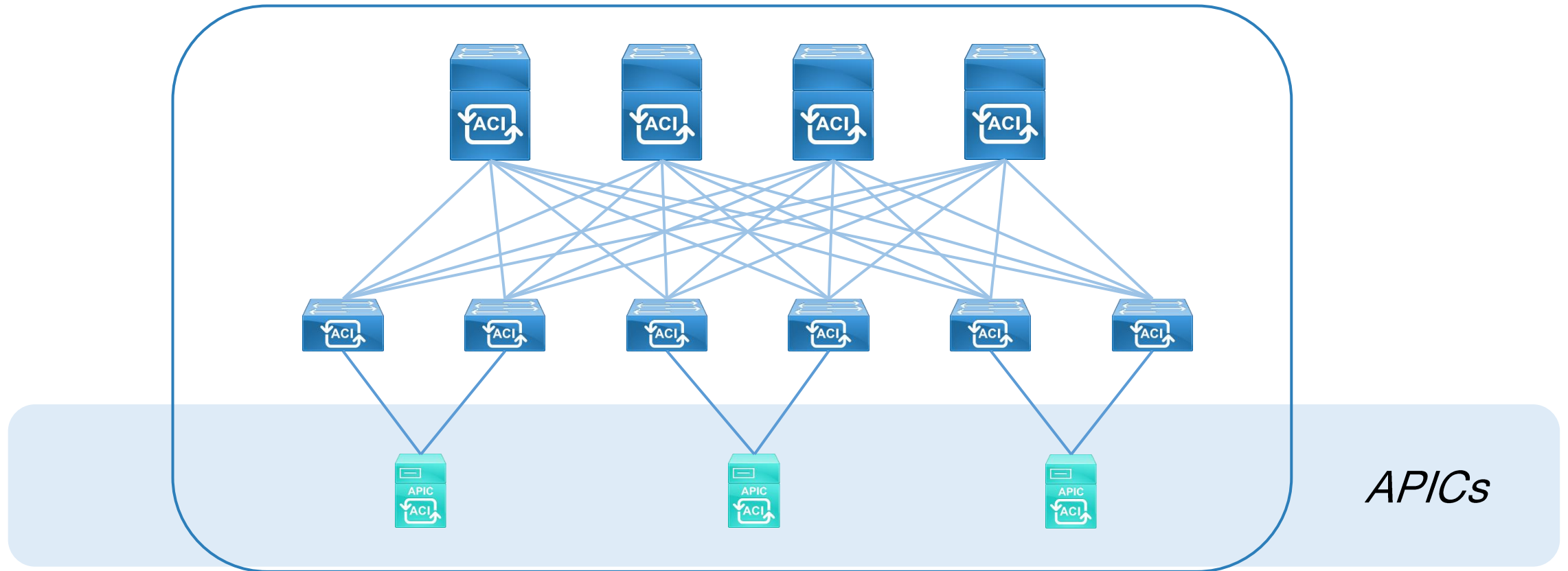


4 Rewrite & Forwarding to Host C

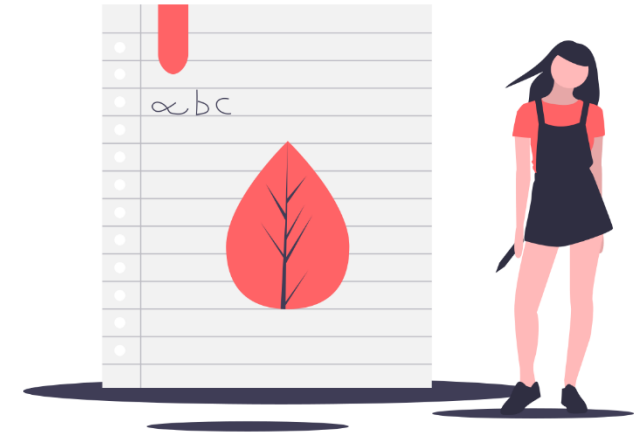
**DEMO LAB 0**



# Application Policy Infrastructure Controller - APIC



# APIC – What is?



## ***The APIC is ...***

*... the policy controller.*

*... the holder of defined policies.*

*... required in order to make any changes.*

*... deployed as a redundant cluster.*

## ***The APIC is not ...***

*...the control plane and/or an SDN controller.*

*...in the data path of the Cisco ACI Fabric.*



# APIC - Clustering

***Single Point of Management, No Single Point of Failure***

*APIC units are deployed with multiple servers in order to maximize controller availability.*



## ***APIC Cluster Benefits***

**Scalability**

Sharding

**Fault Tolerance**

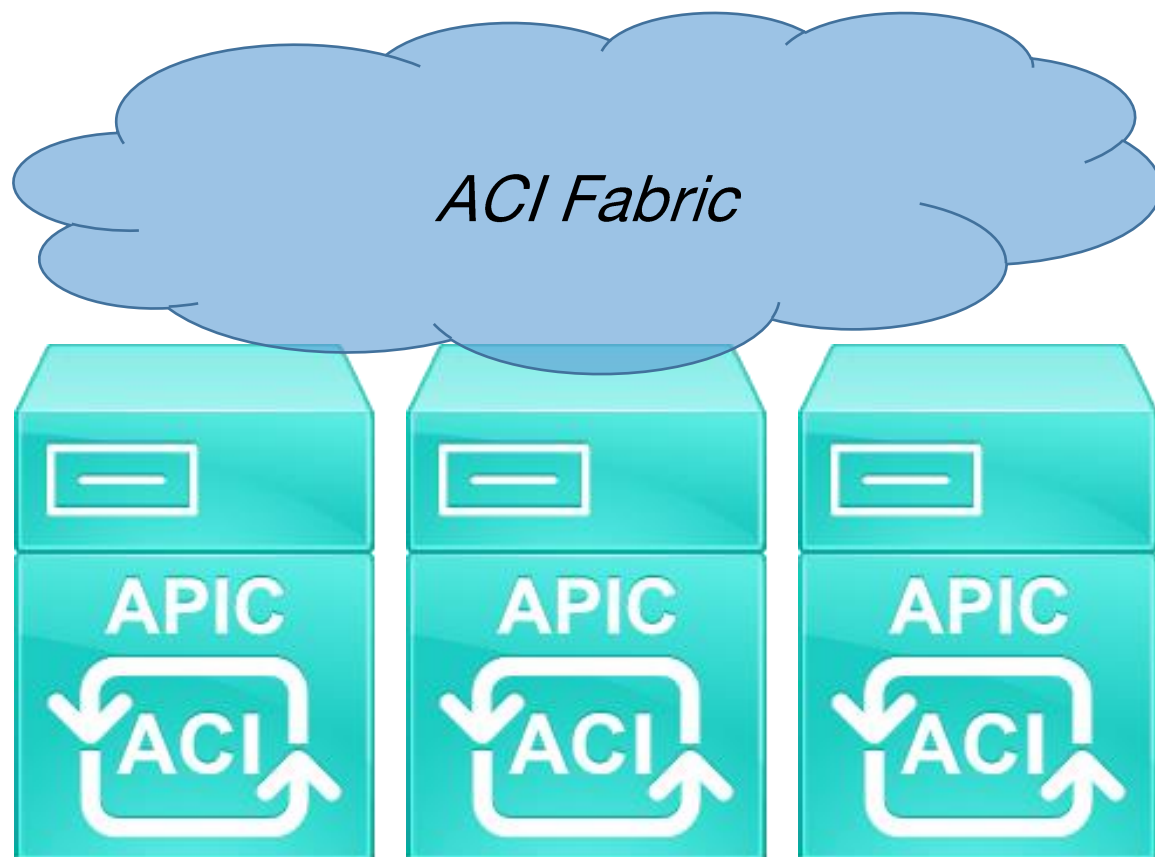
Replication

**Nondisruptive Upgrades**



# APIC - Clustering

## Sharding



## Sharding

*The overall system data is divided into segments (or shards) and is distributed across the APIC members of the cluster.*

Each service's data is divided into 32 shards

Each APIC holds a subset of shards

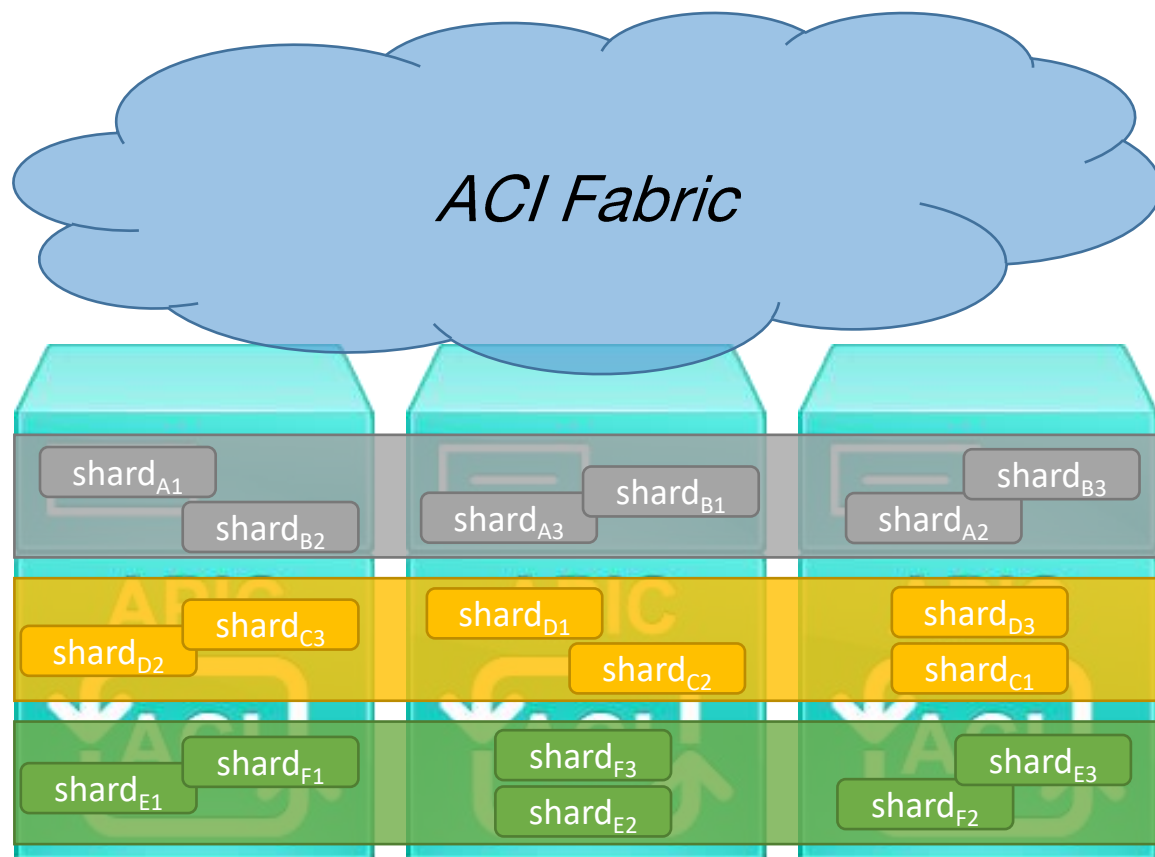
The shard layout changes as the cluster size changes





# APIC - Clustering

## Sharding



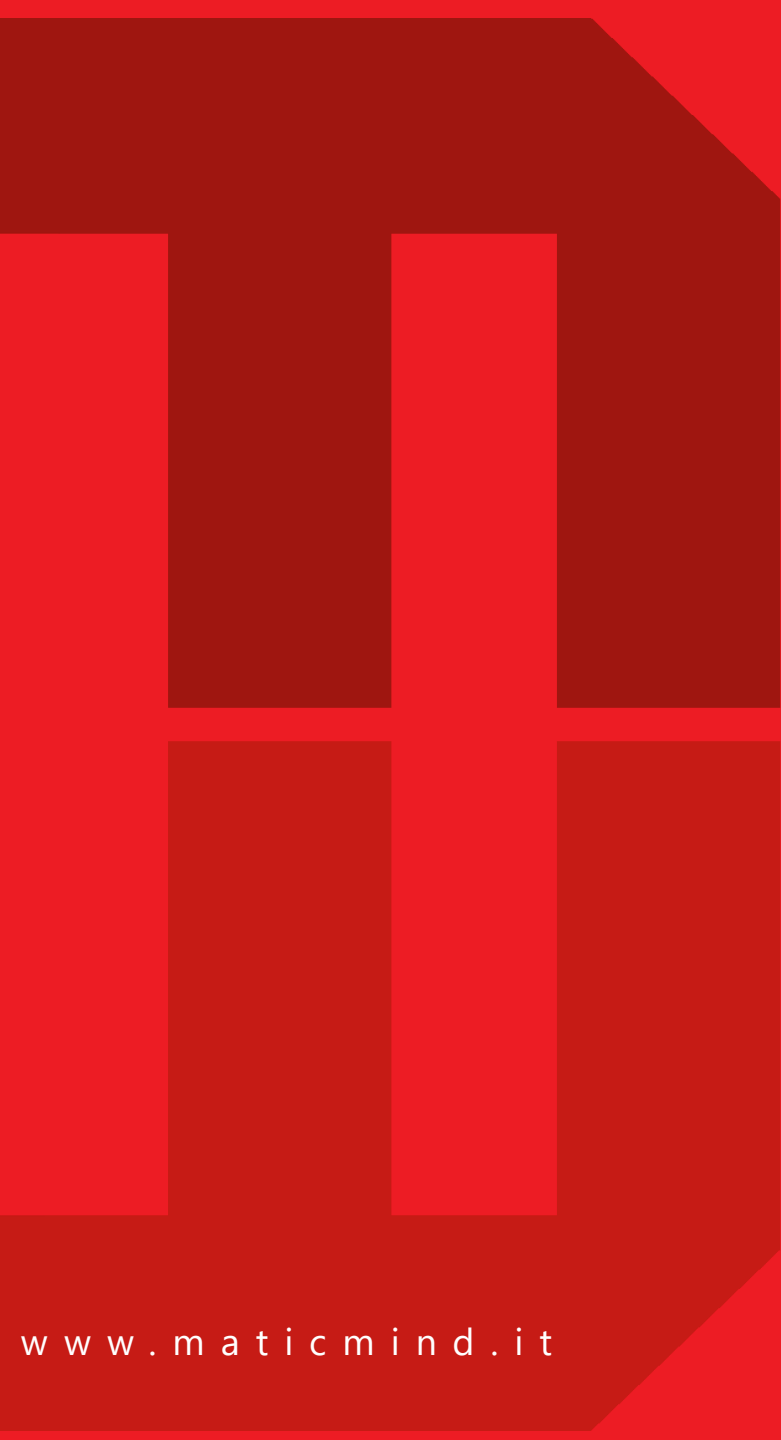
Each shard has three separate copies, all of which are distributed across the devices in the cluster.

Placement is determined with a hashing function

# *TO THE SECRET LAB!*

## *HANDS ON LAB 1*





DATA CENTER



COLLABORATION



NETWORK



APPLICATIONS



SECURITY