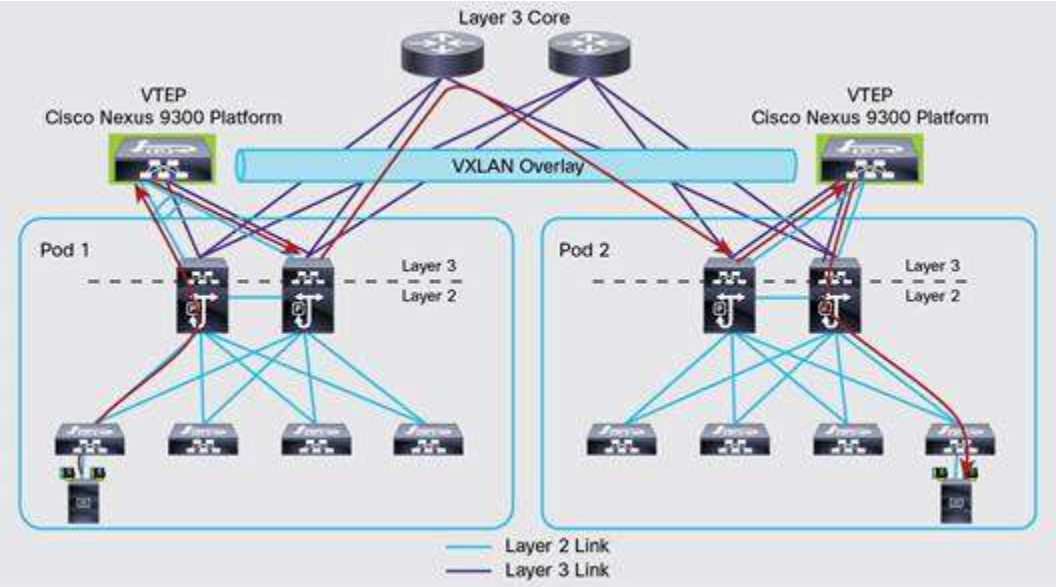
## Virtual Extensible LAN (VXLAN):

- In data centers, VXLAN is the most commonly used protocol to create overlay networks.
- That sit on top of the physical network, enabling the use of a virtual network of switches.
- VXLAN standard to IETF as solution to DC network challenges posed by traditional VLAN.
- VXLAN is designed to provide the same Ethernet L2 network services as VLAN does today.
- Virtual eXtensible Local Area Network (VXLAN) but with greater extensibility and flexibility.
- The VXLAN standard provides for the elastic workload placement and higher scalability.
- The VXLAN standard of Layer2 segmentation that is required by today's app demands.
- Enables up to 16 million VXLAN segments to coexist in the same administrative domain.
- The VXLAN provides solution to extend Layer 2 networks across Layer 3 infrastructure.
- The VxLAN is a way to group devices at layer-2 and VxLAN does not have this limitation.
- Virtual Extensible LAN uses a 24-bit header, which gives us about 16 million VNI's to use.
- VXLAN is tunneling protocol that tunnels Ethernet (L2) traffic over an IP (L3) network.
- L2 networks were not designed to support hundreds of thousands of MAC addresses.
- Layer 2 networks were not designed to support tens of thousands of Virtual LANs.
- The VXLAN is designed to address the issues being seen in traditional Layer 2 networks.
- VXLAN Network Identifier (VNI) identifies VXLAN and has similar function as the VLAN ID.
- We use 24 bits for the VNI, which means we can create 16,777,215 ( 16 million) VXLANs.
- That's a lot, compared to those 4094 VLANs with a 12-bit Virtual Local Area Network ID.
- Can create plenty of VXLANs, large service provider with even thousands of customers.
- With VXLAN, overlay is layer 2 Ethernet network & underlay network is layer 3 IP network.




- An overlay network is a virtual network that runs on top of a physical underlay network.
- Even if you never heard about this terminology before, you have probably seen it GRE.
- A Generic Routing Encapsulation GRE tunnel is a simple example of an overlay network.
- The Generic Routing Encapsulation GRE tunnel runs on top of a physical underlay network.

VXLAN is a modern network protocol widely deployed in data center clouds, and the Software defined networking nowadays. VLAN is a mechanism of segmenting the layer2 network, separating the single broadcast domains into multiple ones. Because the VLAN has a 12bit tag, the maximum allowed VLAN is 4094, which is more than enough for a traditional network, but not so much for a modern network where everything is in the cloud with multi-tenants. Since VLAN uses STP and you have multiple redundancy links between the switches, only one among them will be in a forwarding state. This creates another problem that it cannot use half of the link efficiently, so you need to work a way around to use the links effectively. In contrast, the VXLAN is a tunneling encapsulation protocol that uses mac in UDP encapsulation.
VXLAN maps VLAN ID into the VXLAN VNID. Instead of just carrying the VLANs within the same layer2 domain, you can stretch the VLAN from one location to another over layer3 or underlay network. You can have VLAN 100 in location A and VLAN 100 in Location B. With the help of VXLAN, you can talk to geographically separated VLAN via layer3. As if it is the same L2 domain. Basically, there will be a VXLAN tunnel created between the VTEP's. And the VXLAN virtual tunnel act as an Overlay network and actual network act as underlay network.

There are some limitations if you think about VLAN's today. Only 4094 VLANs are available to use, with many customers moving into the cloud and physical servers are replaced with VM's. The availability of just 4094 VLAN's is not so sufficient. Especially if you are a cloud company or any network service provider giving services to multiple customers, you will, for sure, run out of those VLANs pretty quickly. So, we need something that can help us to have the same VLANs across multiple customers. So, we can use VLAN 100 with customer A as well as with customer B while the VXLAN logically separates both. Since the VXLAN header is 24bit, you can carry up to 16million VNID's, and it provides great flexibility for the service provider when it comes to multi-tenant environments in the cloud. We still use VLAN today in the network, but the VXLAN provides more encapsulation options while using VLAN's.

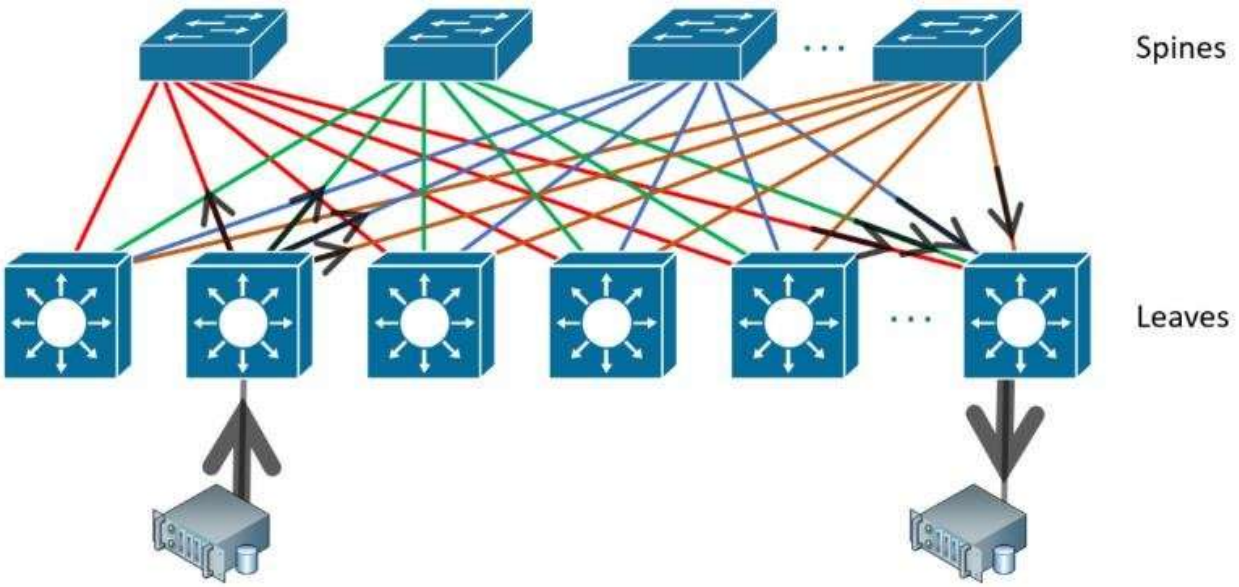
The traditional network devices cannot read the VXLAN packet, to use VXLAN you need to use VTEP known as VXLAN tunnel endpoint device. VTEP's can encapsulate and decapsulate the VXLAN packets; there are two types of VTEPs. Hardware-based and software-based. VTEP's are usually configured with IP addresses.

In virtualization, the host where you have the VM's resides is called the Host machine (the hypervisor), and the VM's are called Guest VM's. Similarly, the physical networks are called the Underlay network, and the network that runs on top of the physical networks is called the overlay network.
When the Underlay (Internet) network goes down, the overlay network would also go down because there is no layer3 IP reachability to the remote hosts. When the overlay network goes down, the Underlay network continues to work, However, your production traffic will be down.

## Packet Walk:

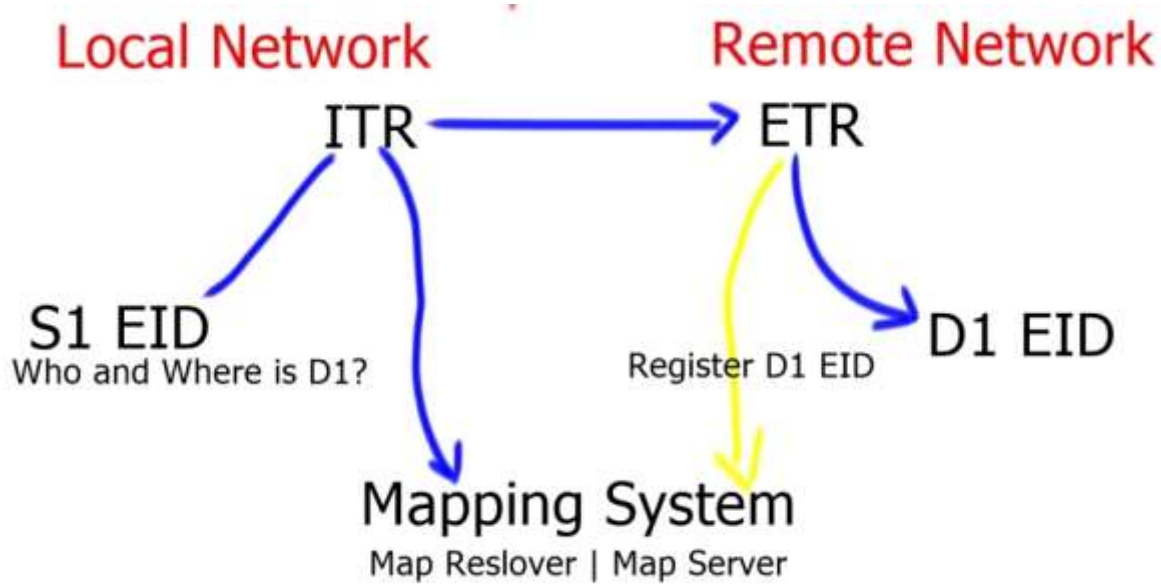
Let's take a moment to see how traffic passes through a simple VxLAN network.


1. A frame arrives on a switch port from a host. This port is a regular untagged (access) port, which assigns a VLAN to the traffic.
2. The switch determines that the frame needs to be forwarded to another location. The remote switch is connected by an IP network. It may be close or many hops away.
3. The VLAN is associated with a VNI, so a VxLAN header is applied. The VTEP encapsulates the traffic in UDP and IP headers. UDP port 4789 is used as the destination port. The traffic is sent over the IP network.
4. The remote switch receives the packet and decapsulates it. A regular layer-2 frame with a VLAN ID is left.
5. The switch selects an egress port to send the frame out. This is based on normal MAC lookups. The rest of the process is as normal.



## Locator ID Separation Protocol (LISP):

- Cisco Locator ID Separation Protocol (LISP) is a mapping and encapsulation protocol.
- Routing scalability is most important problem facing the Internet and must be solved.
- Internet routing tables have grown exponentially, putting a burden on BGP Routers.
- Need powerful routers with enough RAM to store all prefixes in Internet routing table.
- LISP (Location Identifier Separation Protocol) is a routing and addressing architecture.
- LISP (Location Identifier Separation Protocol) developed by Cisco Systems but open.
- Creates two addresses for each network node: one for its identity & another for location.
- LISP is routing architecture & data & control plane protocol created to address routing.
- Originally it was designed for the Internet, but nowadays, you also see LISP in data center.
- LISP is used in environments like data centers, IoT, WAN, and campus (Cisco SD-Access).
- LISP creates new model in how IP addressing is assigned device identity which known EID.
- The Endpoint Identifier (EID), and its location, known as its Routing Locator (RLOC).
- Into two different namespaces, creating separate IP addresses for the EID and RLOC.
- Endpoint Identifier (EID) is assigned to the hosts like Computers, laptops, printers, etc.
- Routing Locators (RLOC) is assigned to routers. We use the RLOC address to reach EIDs.
- Tunneling protocol uses DNS-like system to figure out to which router send IP packetes.



Well, in LISP a very similar like DNS Domain Name System. If a router needs to send a packet to 76.74.254.123, and that route is not in the local routing table – it sends a query to the LISP Map Resolver. The LISP Map Resolver then looks at its database and tells the router that the network can be reached via 4.71.170.2. The router then sends a LISP encapsulated packet to 4.71.170.2 to be then forwarded onto its ultimate destination.