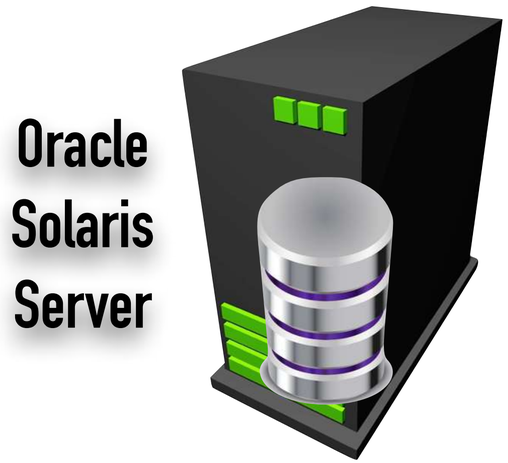
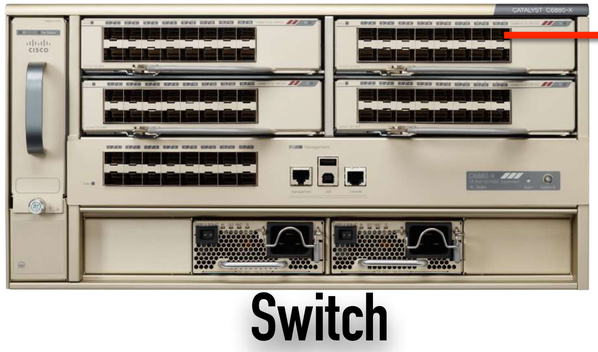
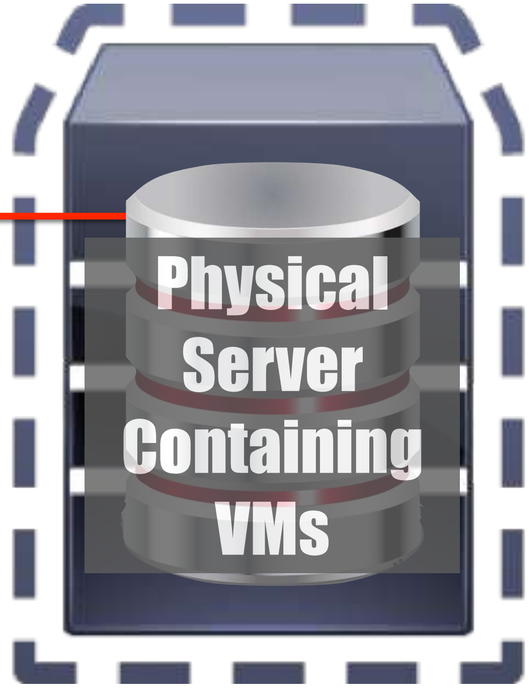
Module 2
Virtualization Technologies

Device Virtualization

Hypervisors

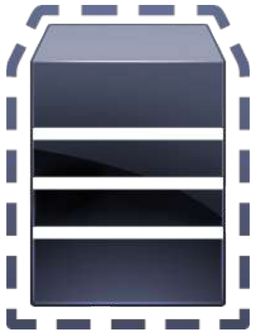




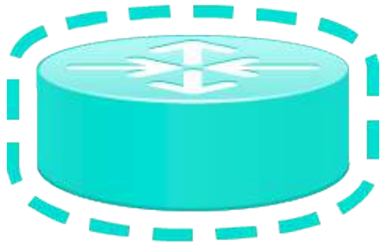


- **Hypervisor:** Software that can create, start, stop, and monitor multiple virtual machines.
  - **Type-1 (“Native” or “Bare Metal”):** Runs directly on the server’s hardware.
  - **Type-2 (“Hosted”):** Runs in a traditional operating system.

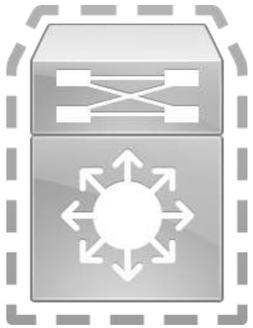
Virtual Machines



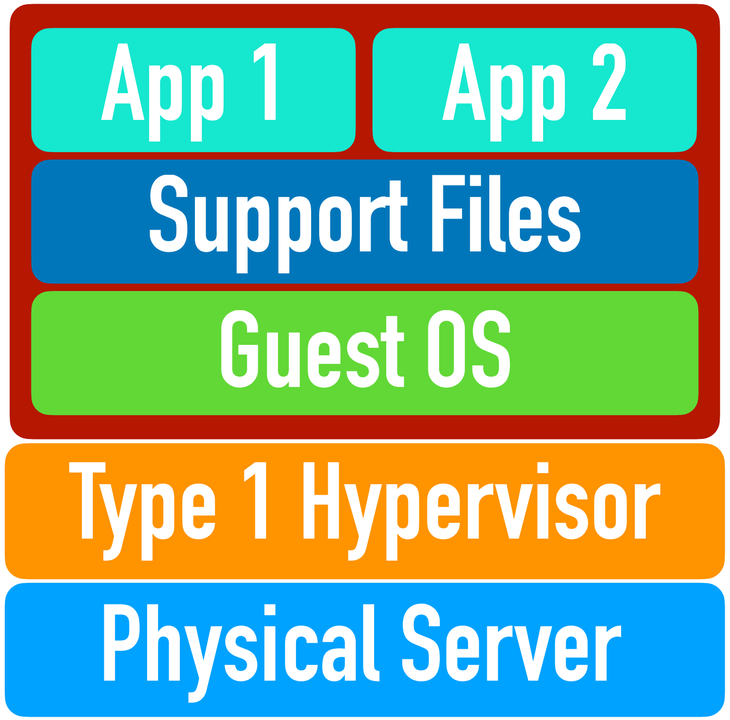
Virtual Server

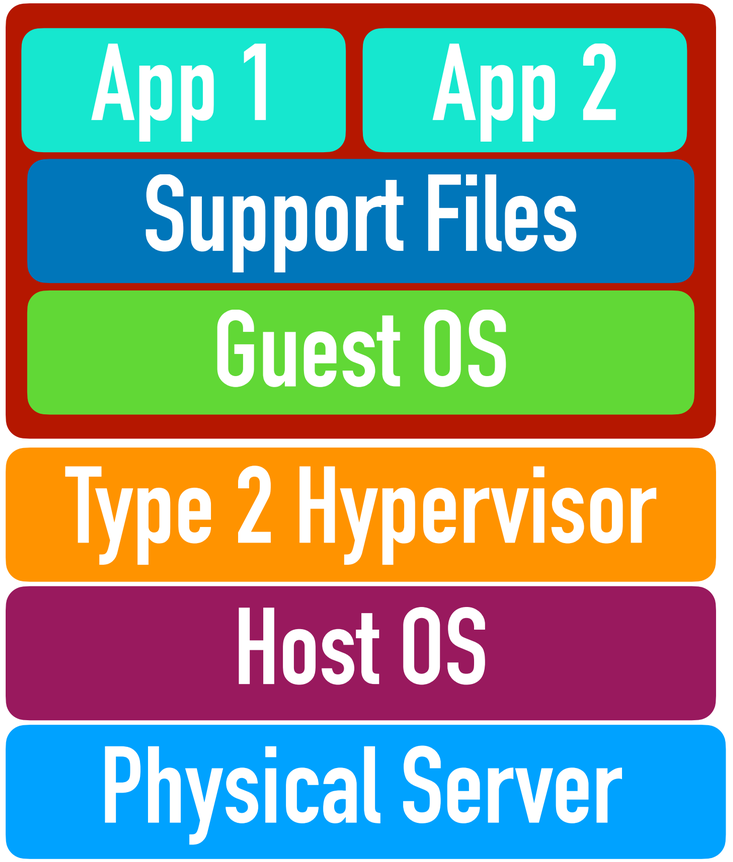


Virtual Router



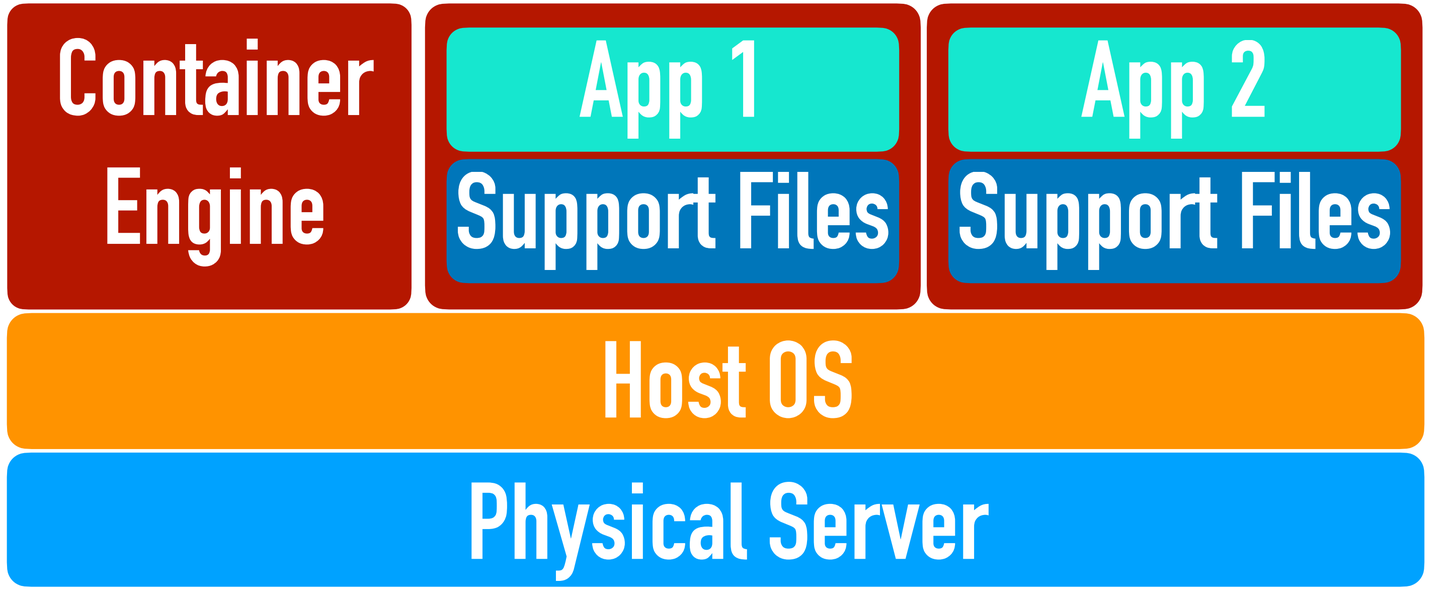
Virtual Switch



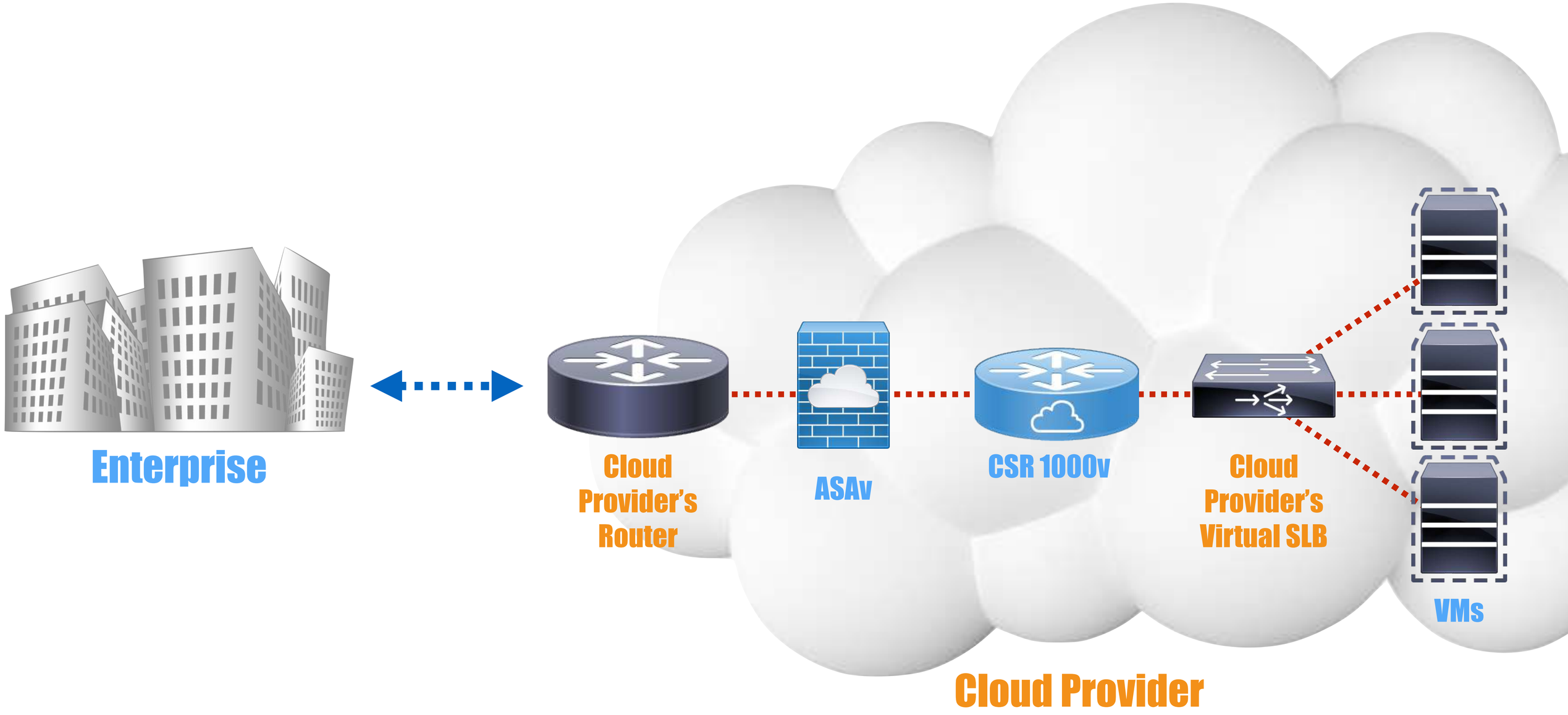


Containers

- Multiple containers share same host OS
- Container Engine creates Container Image
- Container Image contains an app and resources required by the app
- Container Engine runs Container Image
- Sometimes called a “lightweight VM”

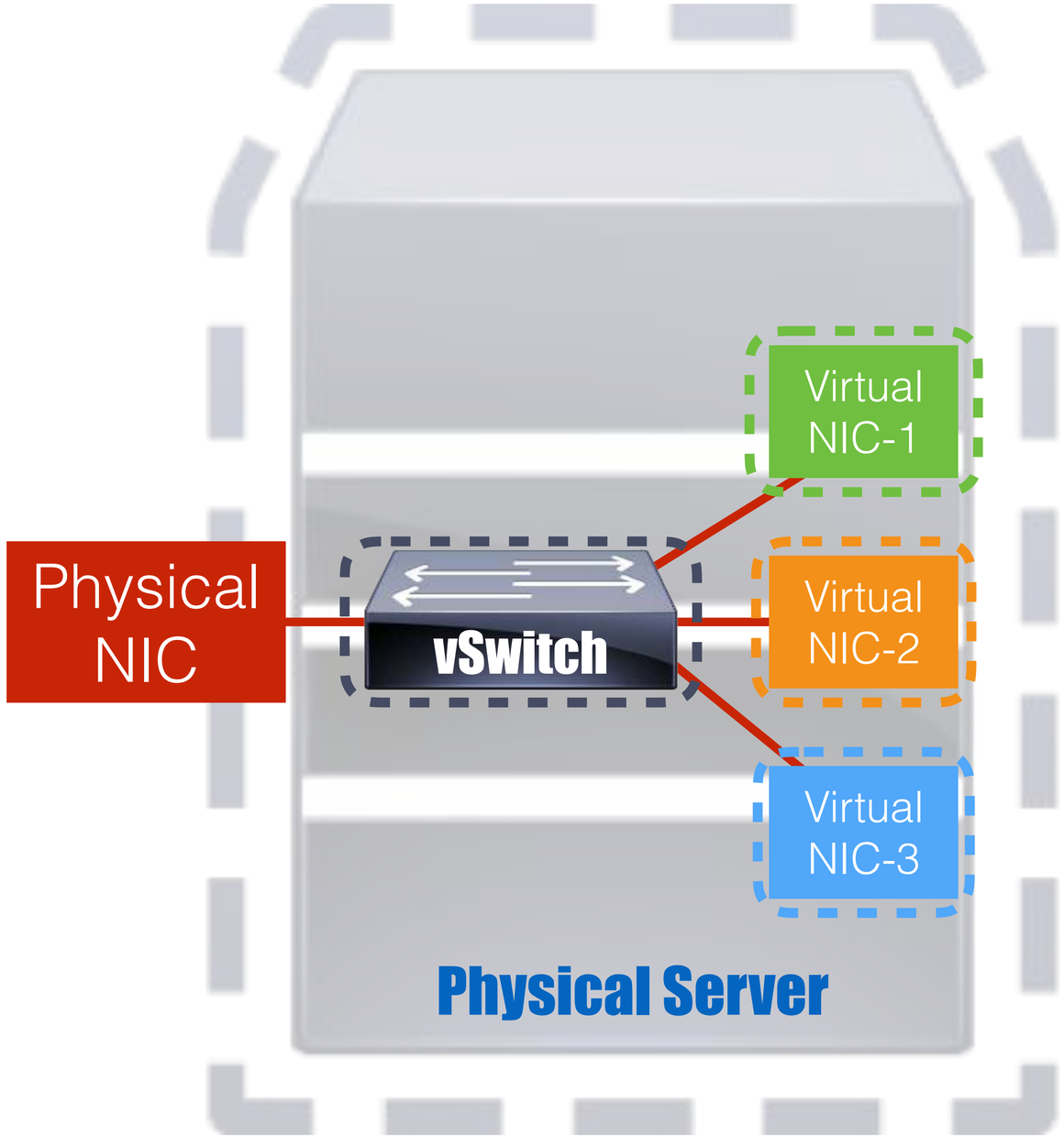


Virtual Machines in the Cloud



DEMO: Creating a VM

Virtual Switches

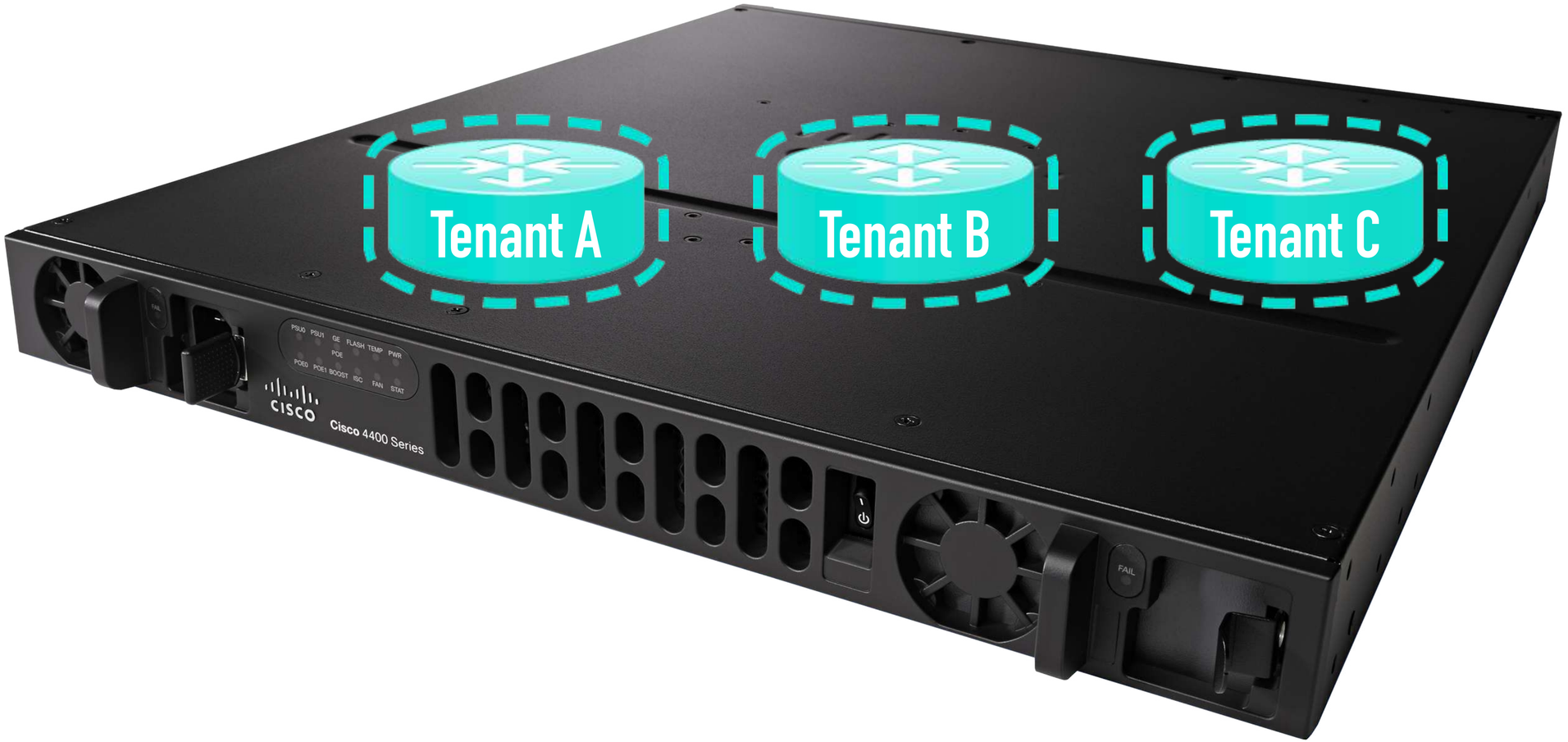


- **Virtual NIC:** Software associated with a unique MAC address, which can be used by a VM to send and receive packets.
- **Virtual Switch:** Software that can connect to other virtual switches, virtual NICs and to a physical NIC.

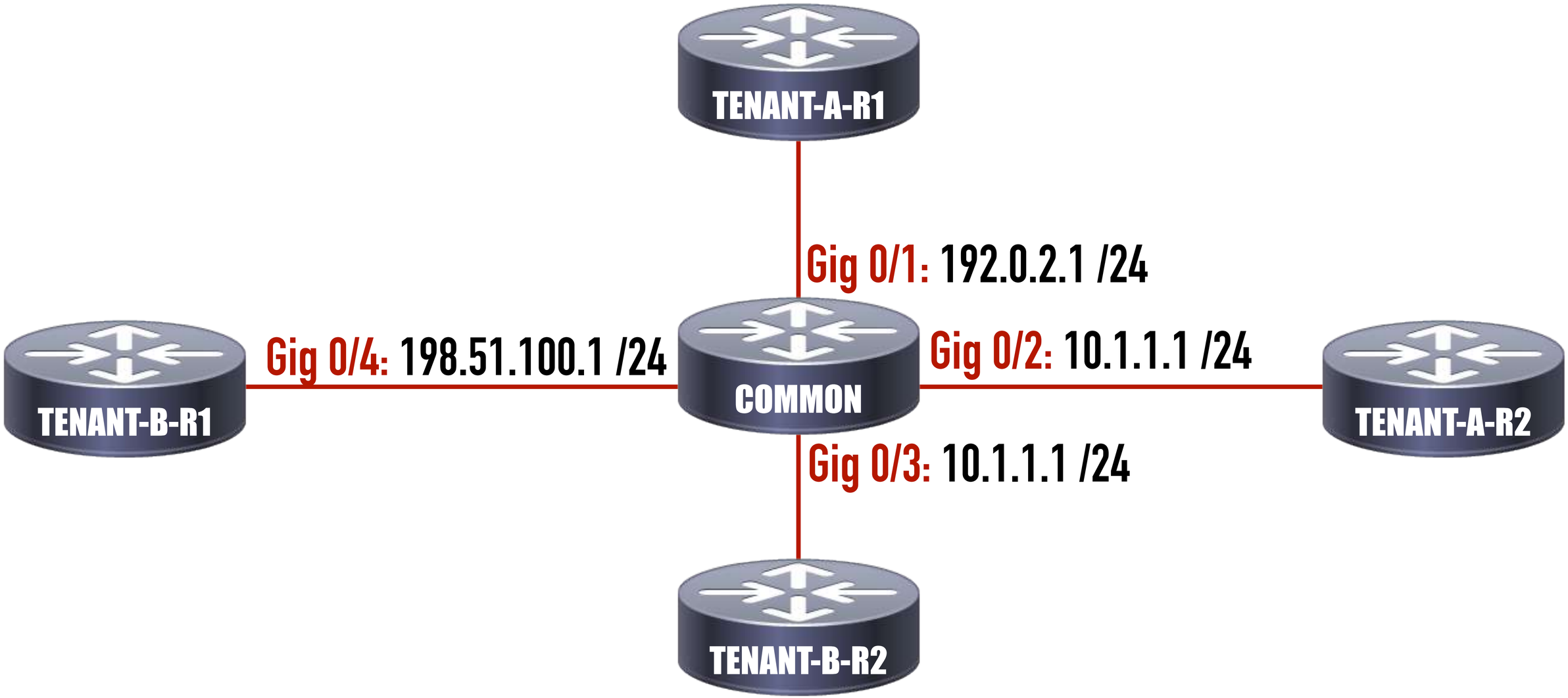
DEMO: Creating a Virtual Switch

Data Path Virtualization

Virtual Routing and Forwarding (VRF)



VRF Demo


TENANT-A-R1
Gig 0/1: 192.0.2.1 /24
TENANT-B-R1
Gig 0/4: 198.51.100.1 /24
COMMON
Gig 0/2: 10.1.1.1 /24
TENANT-A-R2
Gig 0/3: 10.1.1.1 /24
TENANT-B-R2

Site-to-Site VPN

- Can use common broadband technologies
- Transparent to the client devices
- Can use routers or dedicated VPN concentrators

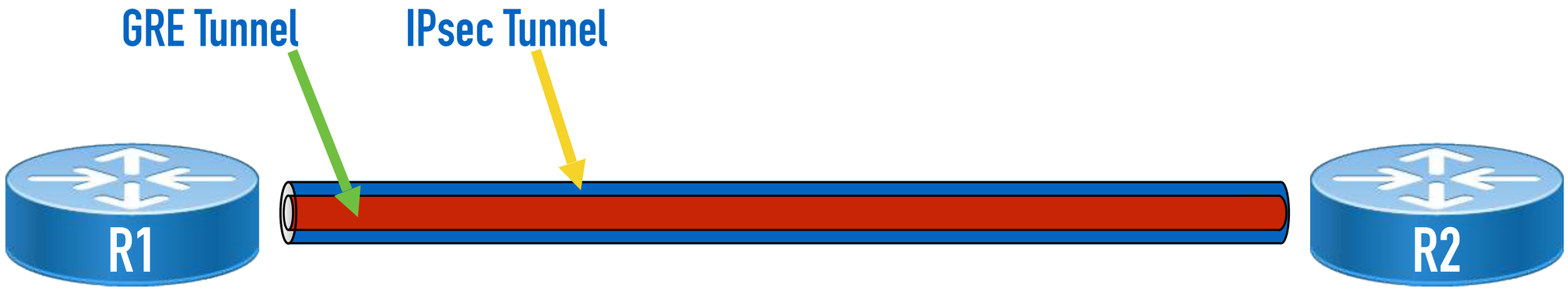
Generic Routing Encapsulation

1. Does not provide security
2. Can encapsulate nearly any type of data

IP Security (IPsec)

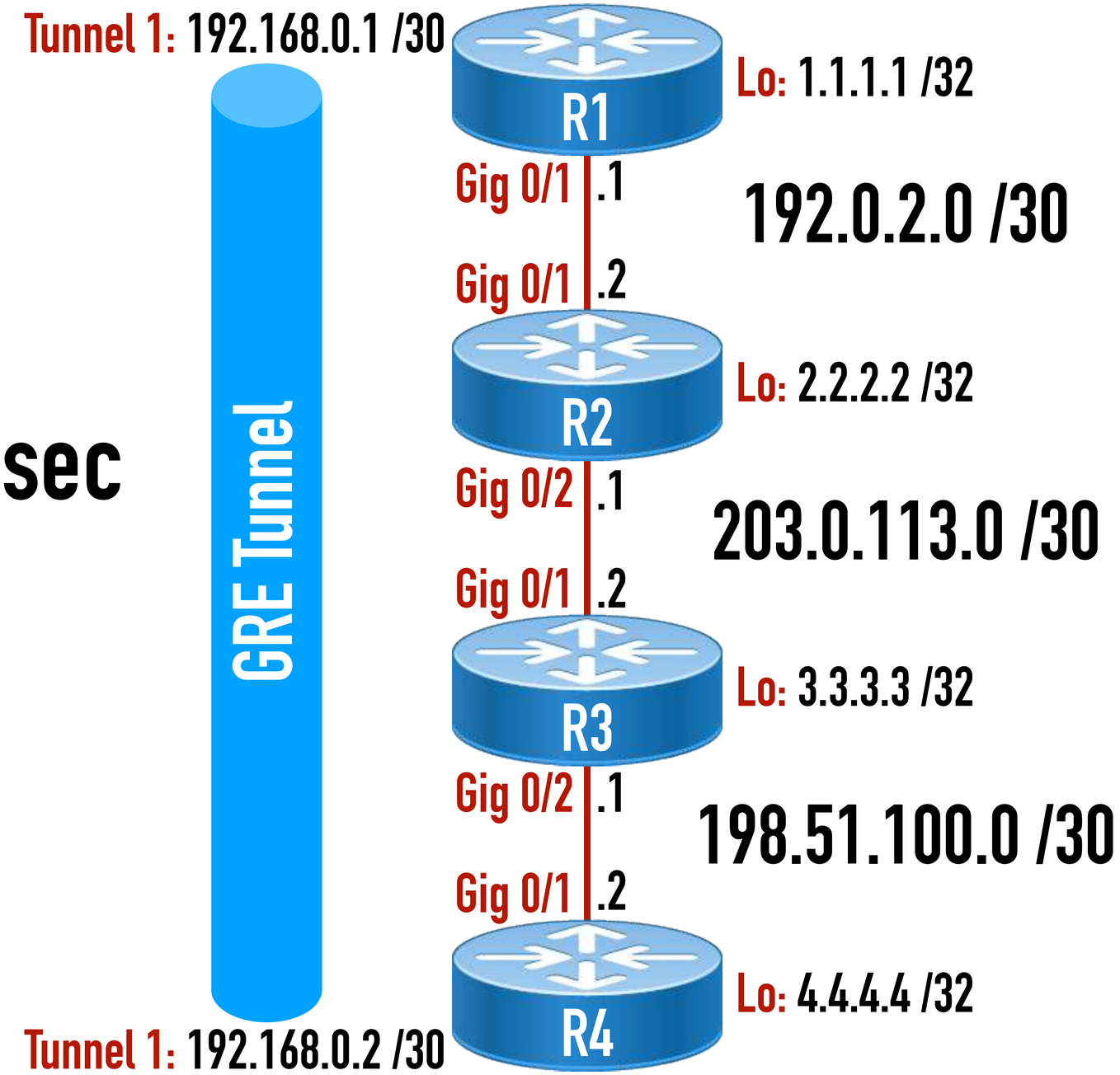
1. Provides
   - Confidentiality: Encryption
   - Integrity: Hashing
   - Authentication: PSKs or Digital Signatures
   - Anti-replay: Applies Serial Numbers to Packets
2. Can encapsulate unicast IP packets
3. Two Modes
   - Transport Mode: Uses Packet's original header
   - Tunnel Mode: Encapsulates entire packet
4. Setup Steps
   - Step #1: Establish an Internet Key Exchange (IKE) Phase 1 tunnel (a.k.a. Internet Security Association and Key Management Protocol [ISAKMP] tunnel)
   - Step #2: Establish IKE Phase 2 Tunnel

GRE over IPsec



- GRE encapsulates nearly any traffic type into GRE packets, which are unicast IP packets
- The GRE packets are protected over the IPsec tunnel

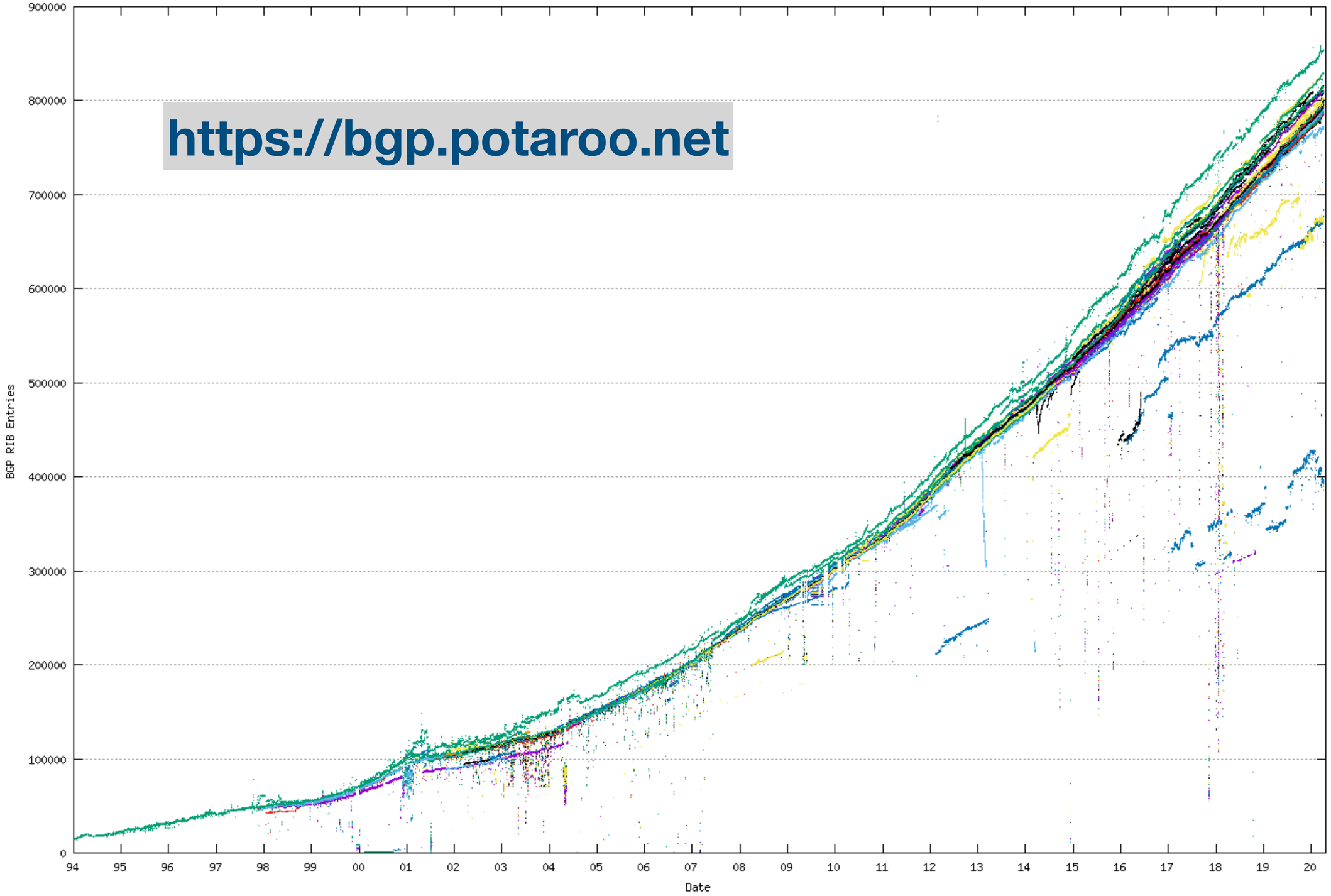
GRE over IPsec Demo



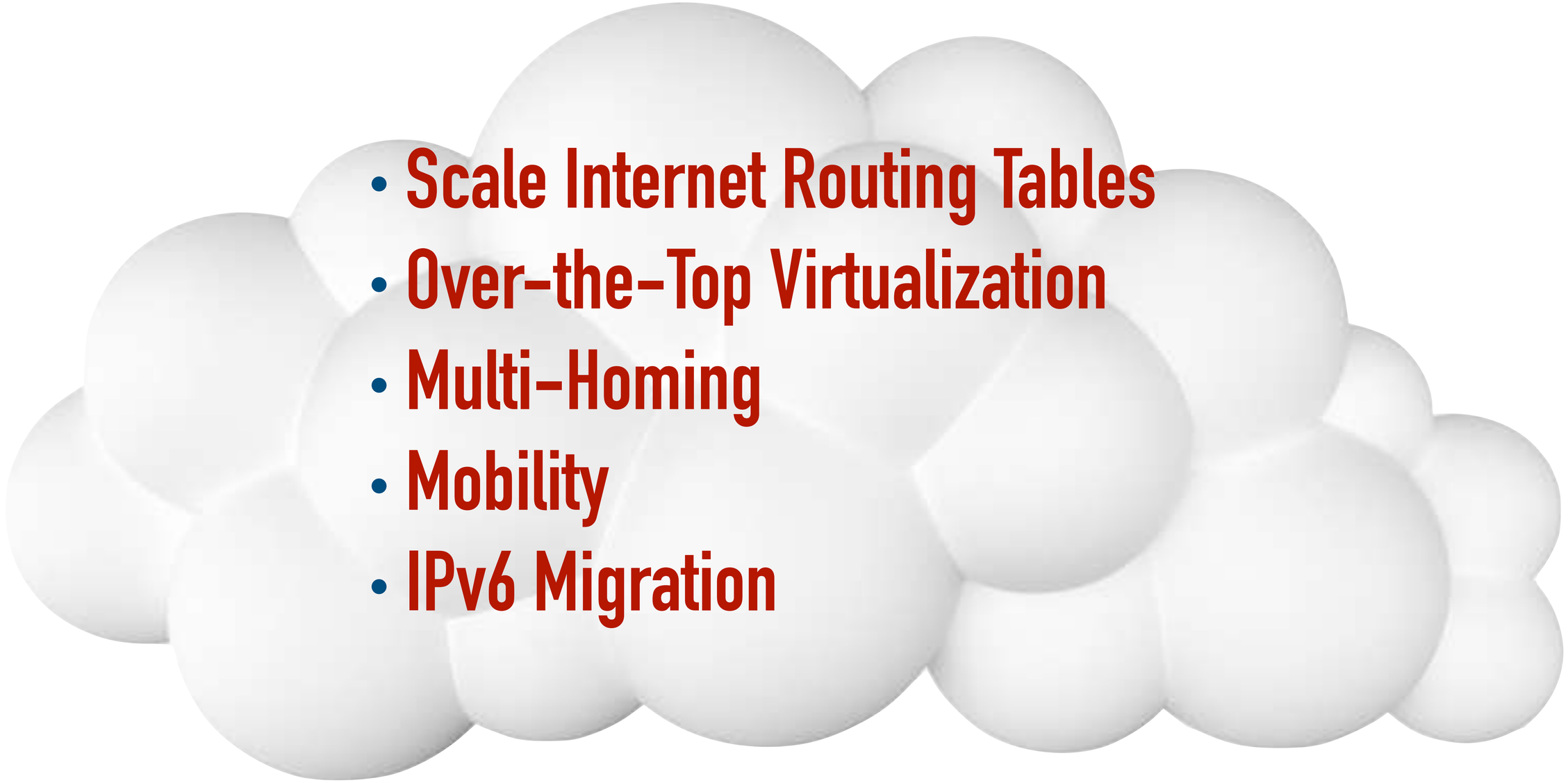
Network Virtualization

Location/ID Separation Protocol (LISP)

Internet


https://bgp.potaroo.net
BGP RIB Entries
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
94
95
96
97
98
99
00
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
Date

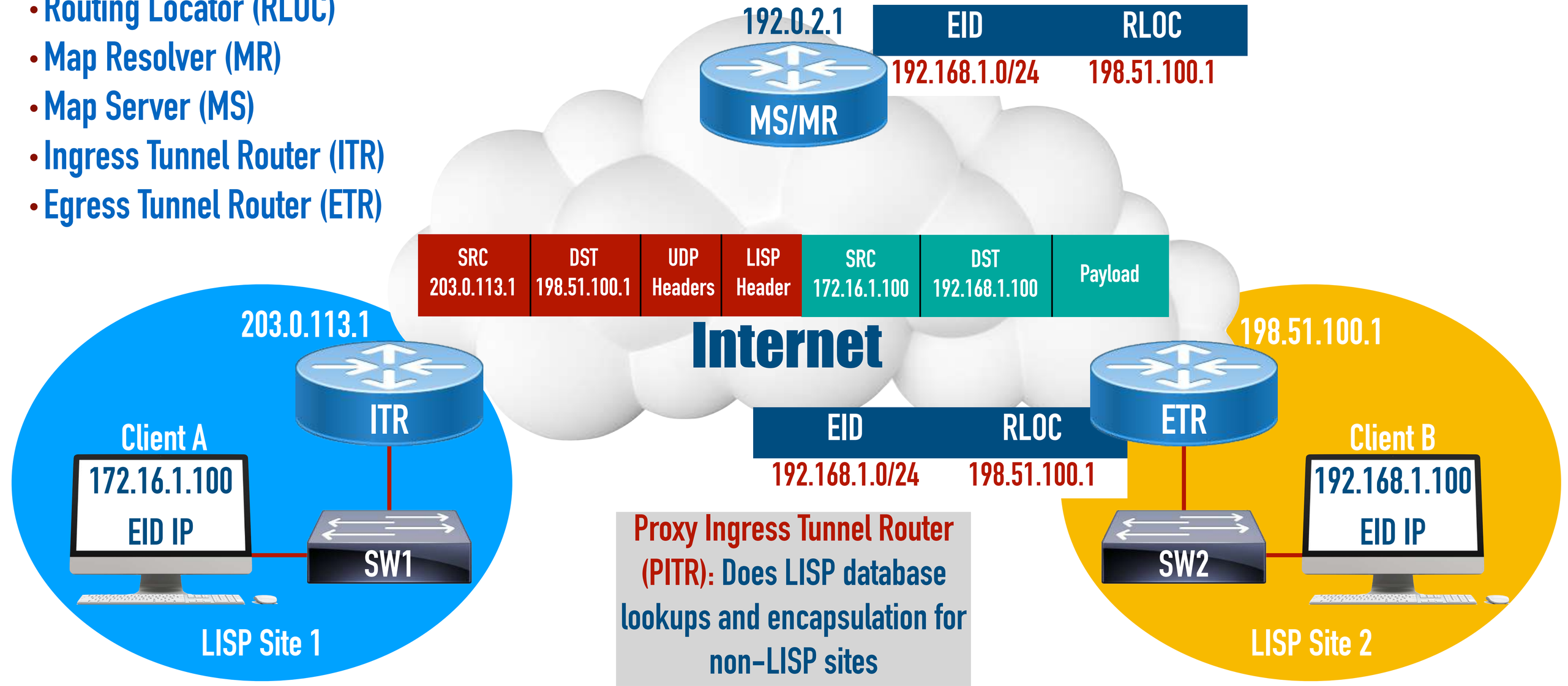
Sample LISP Benefits



- Scale Internet Routing Tables
- Over-the-Top Virtualization
- Multi-Homing
- Mobility
- IPv6 Migration

Location/ID Separation Protocol (LISP)

- Endpoint ID (EID)
- Routing Locator (RLOC)
- Map Resolver (MR)
- Map Server (MS)
- Ingress Tunnel Router (ITR)
- Egress Tunnel Router (ETR)

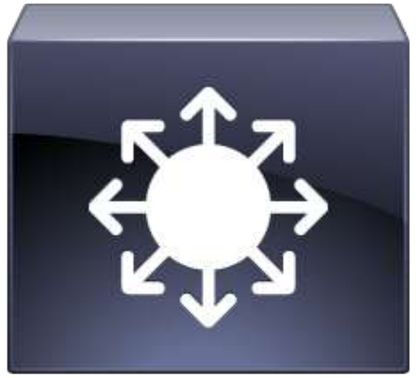


Proxy Ingress Tunnel Router (PITR): Does LISP database lookups and encapsulation for non-LISP sites

Virtual Extensible Local Area Network (VXLAN)

Traditional Ethernet Switch

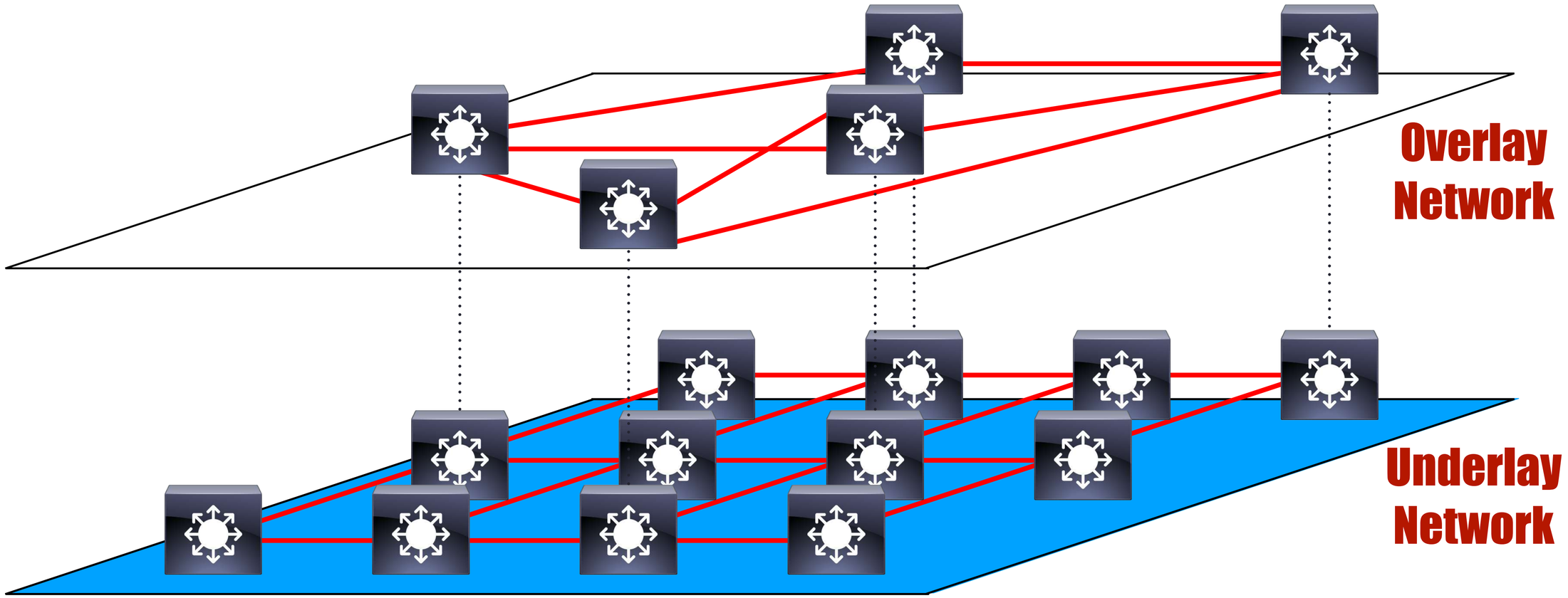
- 12-bit VLAN Field
- Over 4000 VLANs



VXLAN Switch

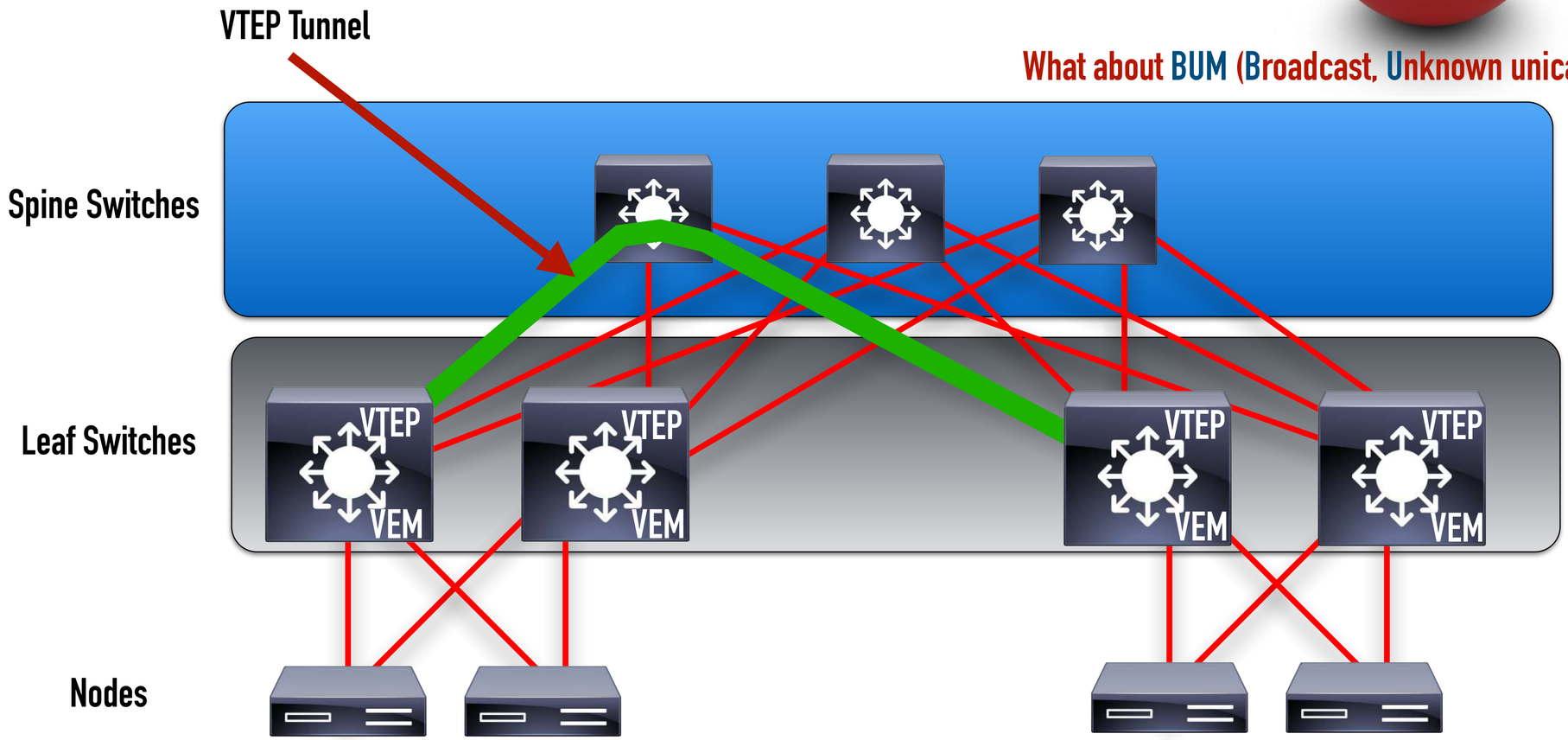
- VXLAN Network Identifier (VNI)
- 24-bit VNI Field
- Over 16 Million VXLANs

Overlay vs. Underlay Networks



Spine-Leaf Design

What about BUM (Broadcast, Unknown unicast, and Multicast) traffic?



- **Virtual Ethernet Module (VEM):** The device that does VXLAN encapsulation (has at least one IP address)
- **VXLAN Tunnel Endpoint (VTEP):** Using an IP address from the VEM, it can setup a temporary tunnel to a VTEP on another switch

VXLAN Communication

MAC	VNI	VTEP
AAAA.AAAA.AAAA	100010	E 1/1
BBBB.BBBB.BBBB	100010	192.168.1.33

- Server 1 wants to communicate with Server 2
- It sends an ARP Broadcast
- LEAF-SW1 learns the AAAA.AAAA.AAAA MAC address is attached to interface E 1/1, which is a member of VLAN 10. VLAN 10 is mapped to VNI 100010
- LEAF-SW1 sends the broadcast to the multicast group of 239.1.1.10
- LEAF-SW3 receives the ARP broadcast and floods it out its ports
- Server 2 responds with its MAC address of BBBB.BBBB.BBBB
- LEAF-SW3 knows that 10.1.1.200 is off one of its ports, so it sends an ARP reply and identifies itself as the VTEP to receive traffic destined for the BBBB.BBBB.BBBB MAC address