



CompSci 401: Cloud Computing

Virtual Networks

Prof. Ítalo Cunha



Networking is key to cloud computing

- Cloud tenants access their resources over the Internet
- Users access applications over the Internet
- Applications communicate through the datacenter network

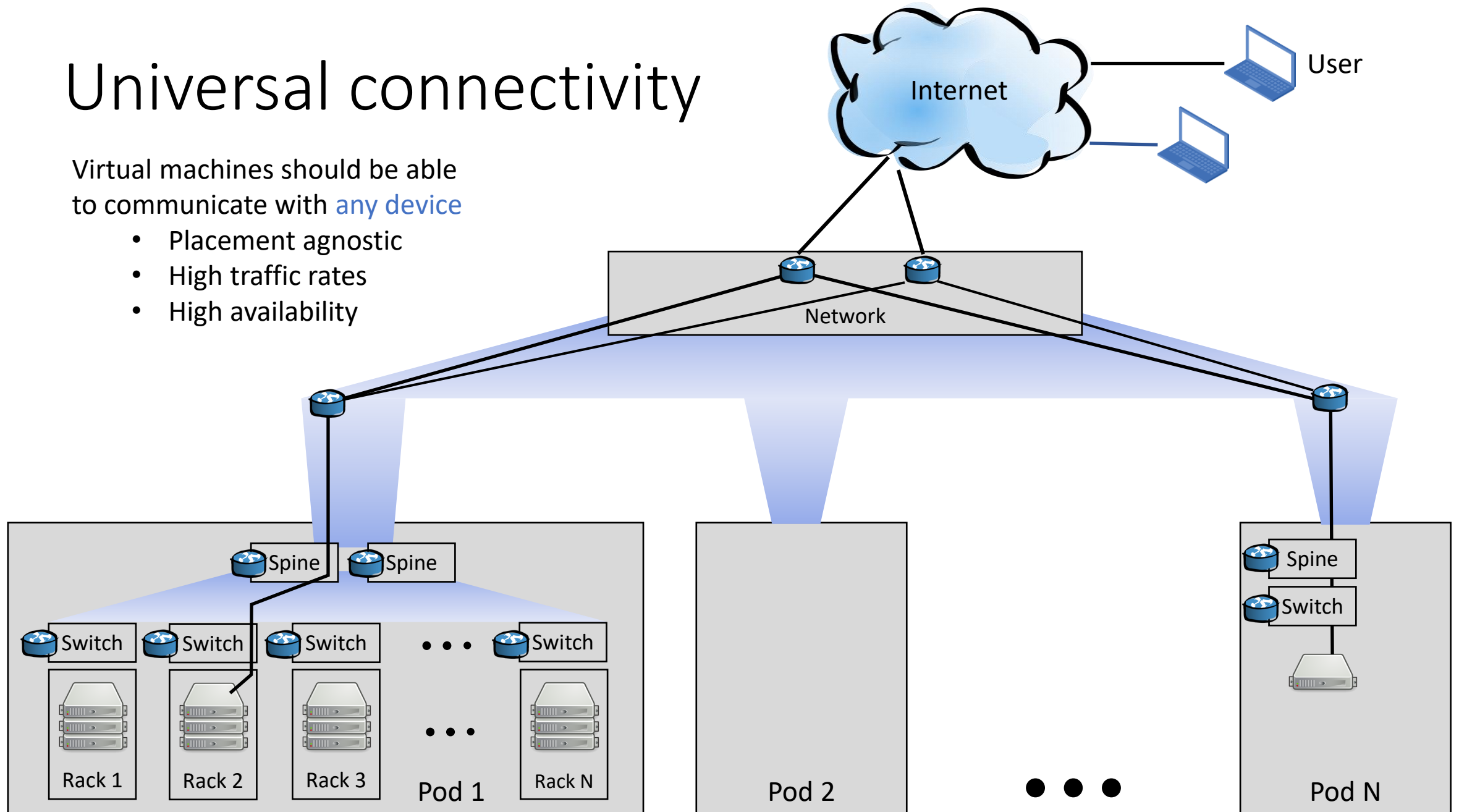
Networking is key to cloud computing

- Cloud tenants access their resources over the Internet
- Users access applications over the Internet
- Applications communicate through the datacenter network
- Universal connectivity
- Safe, isolated communication

Universal connectivity

Virtual machines should be able to communicate with **any device**

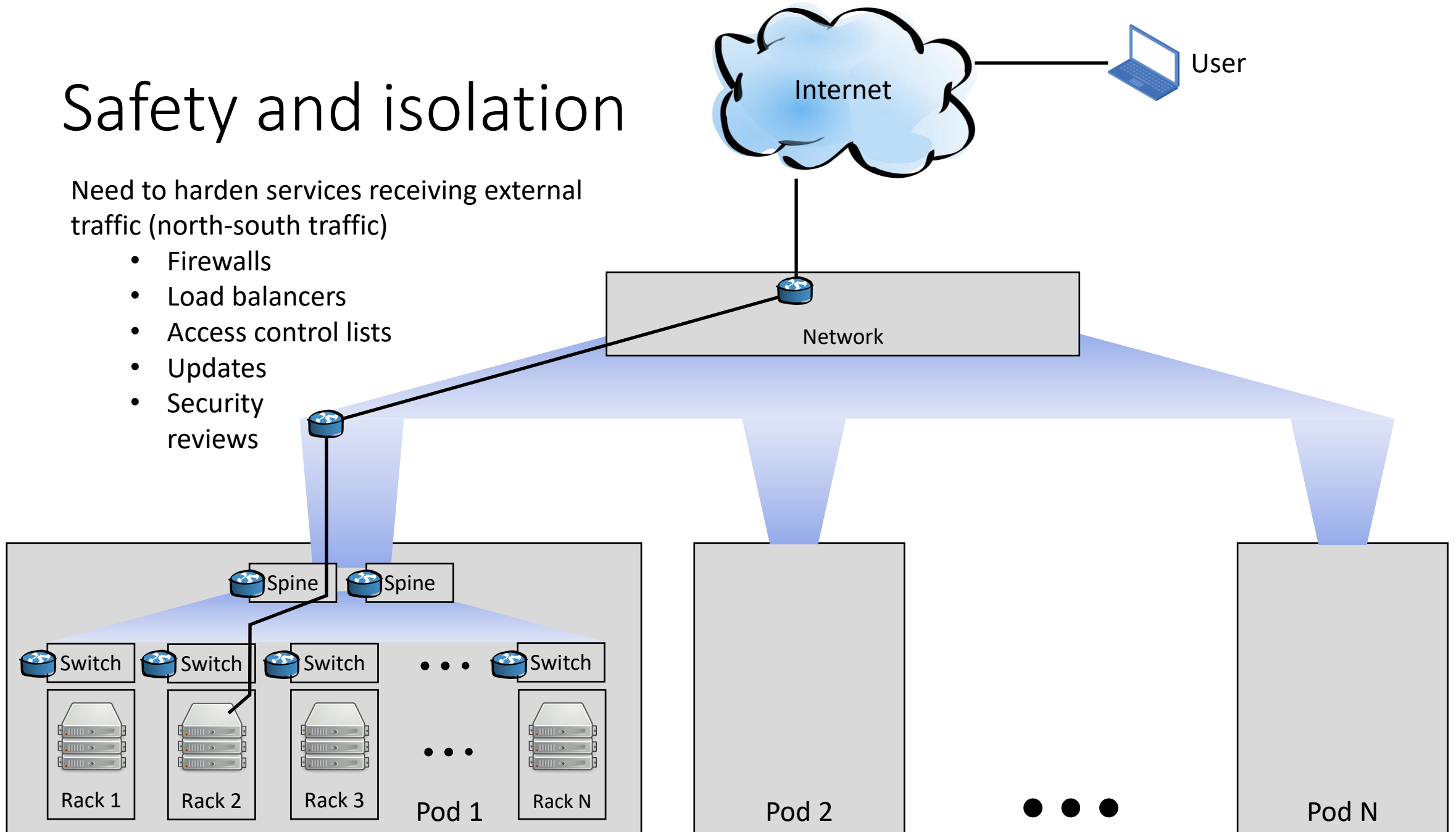
- Placement agnostic
- High traffic rates
- High availability



Safety and isolation

Need to harden services receiving external traffic (north-south traffic)

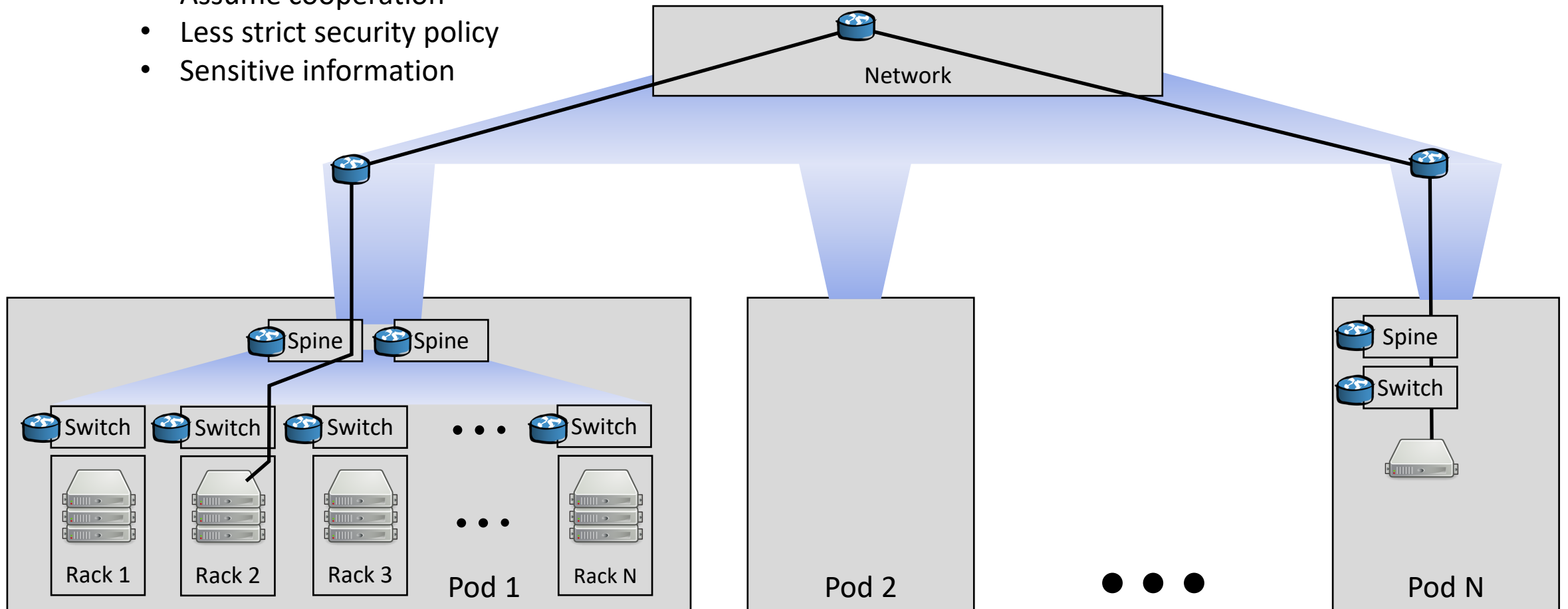
- Firewalls
- Load balancers
- Access control lists
- Updates
- Security reviews



Safety and isolation

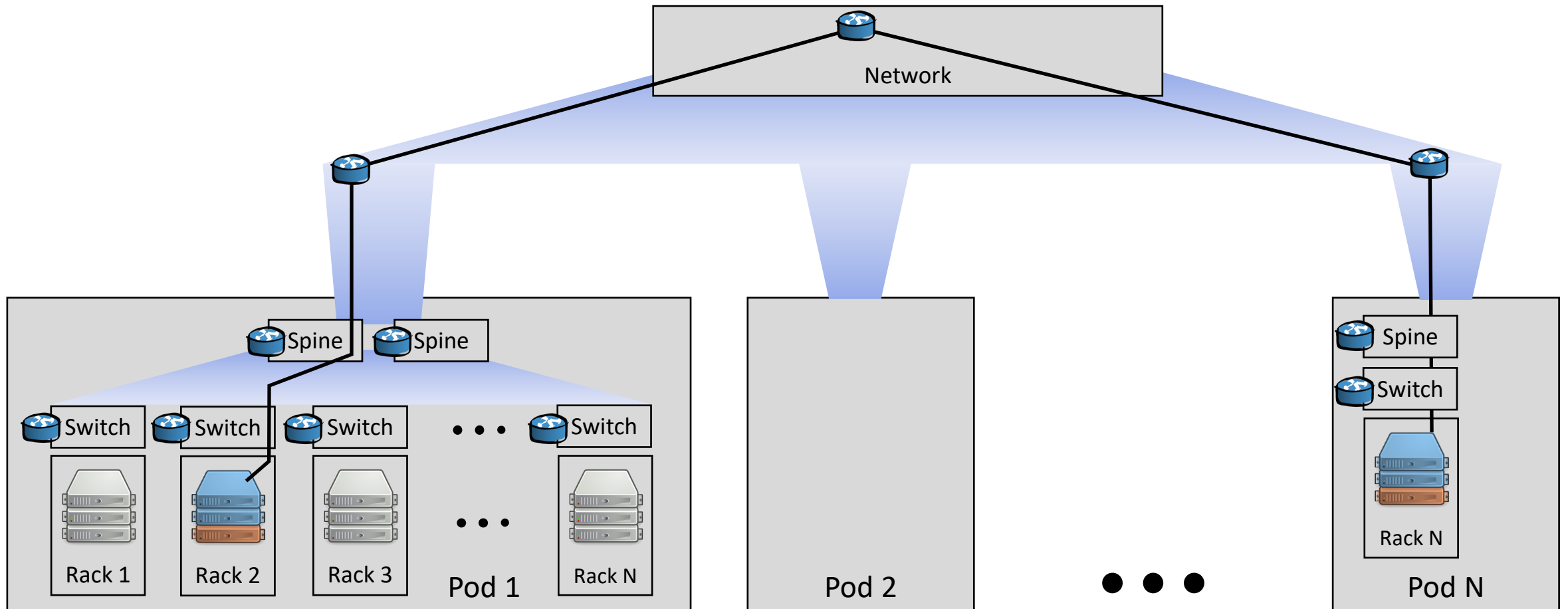
Internal APIs might accept requests from other services of the same application

- Assume cooperation
- Less strict security policy
- Sensitive information



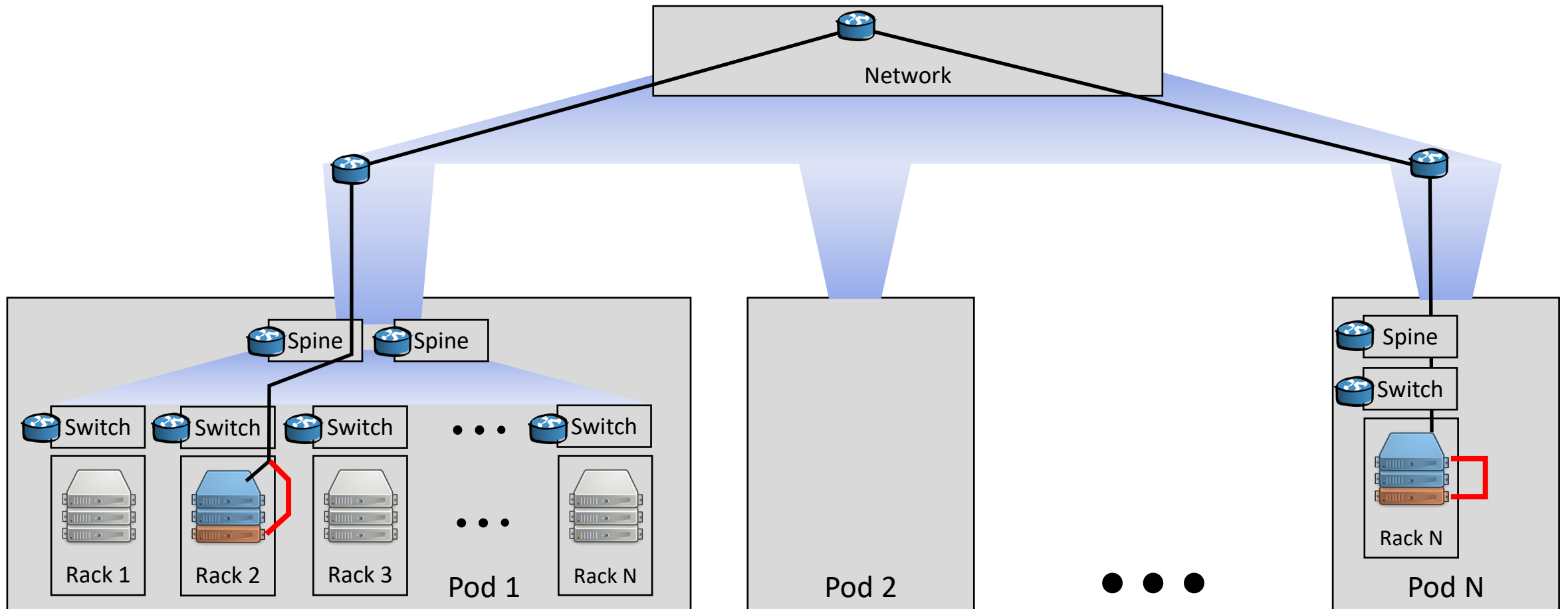
Safety and isolation

Unauthorized access or information
snooping by **third parties**



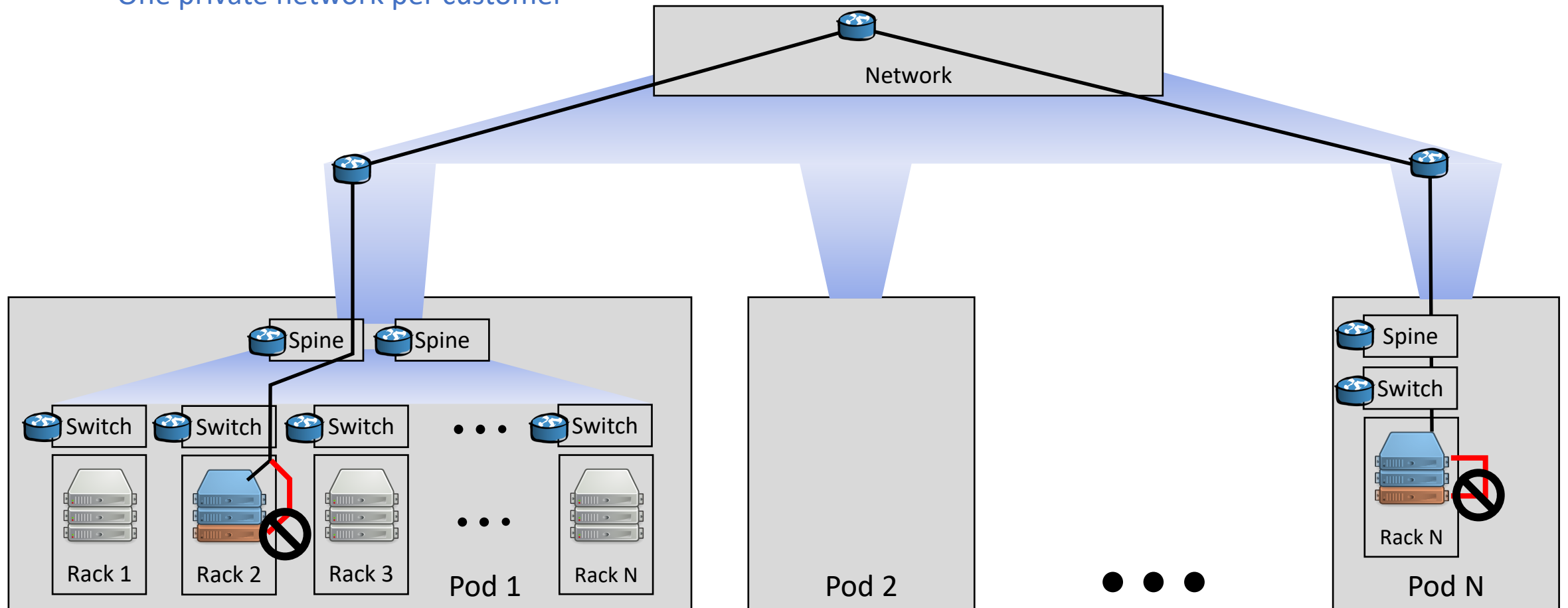
Safety and isolation

Unauthorized access or information
snooping by **third parties**

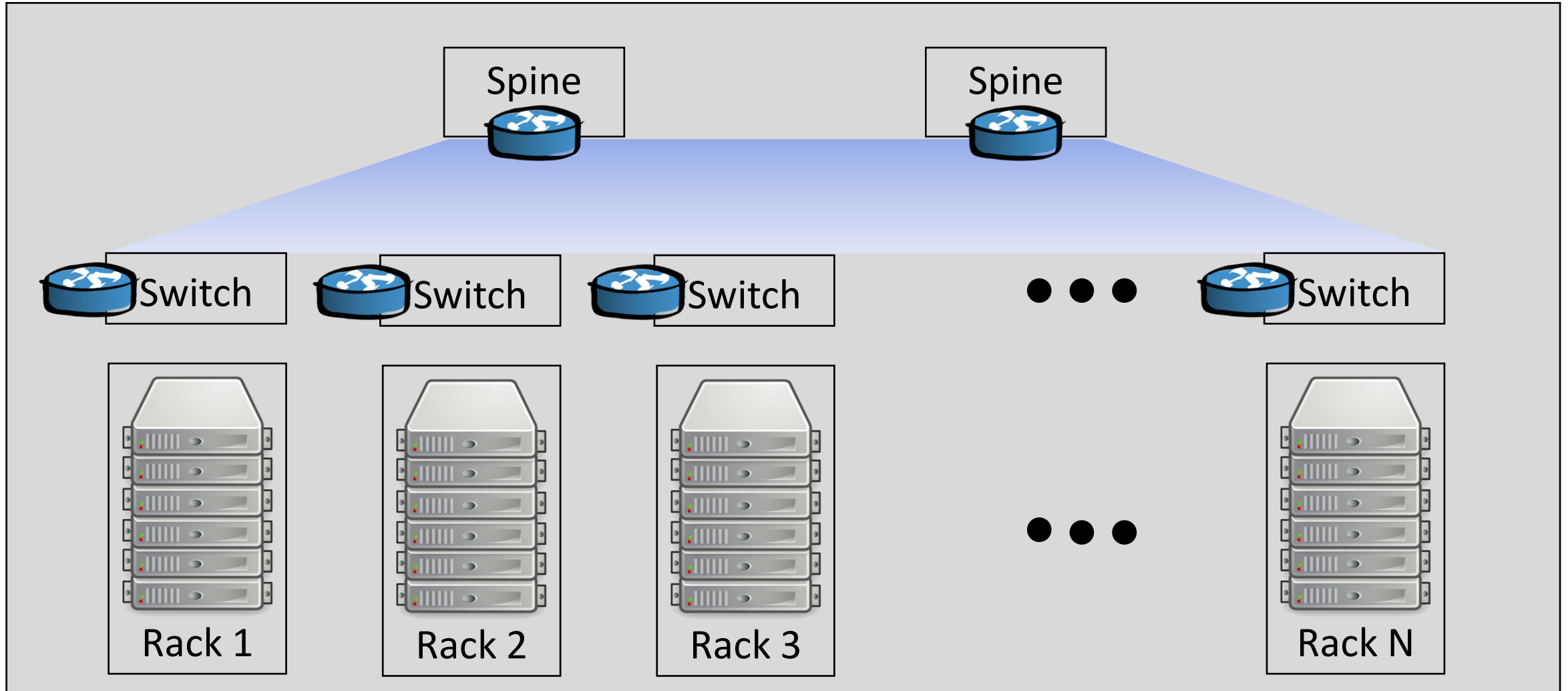


Safety and isolation

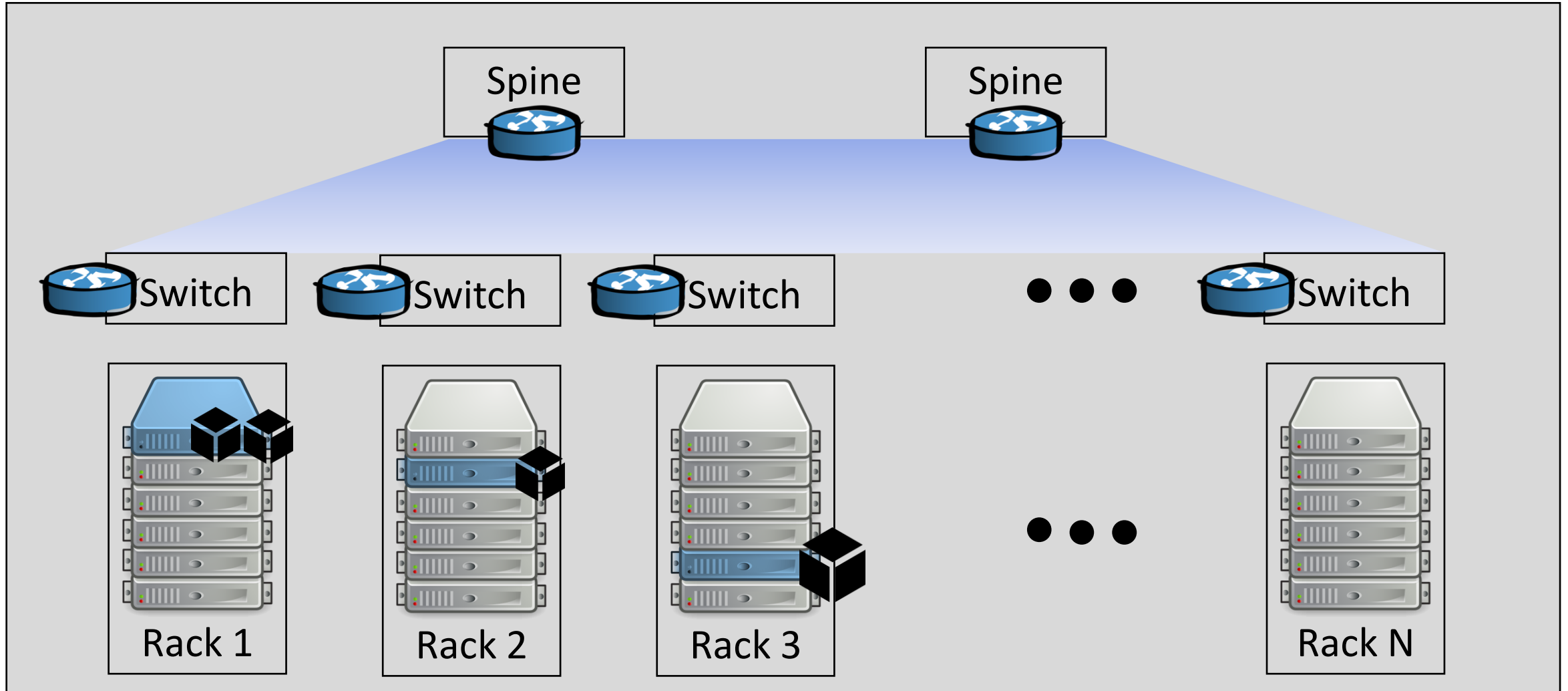
- Third parties should not have access to a customer's resources or their data
- One private network per customer



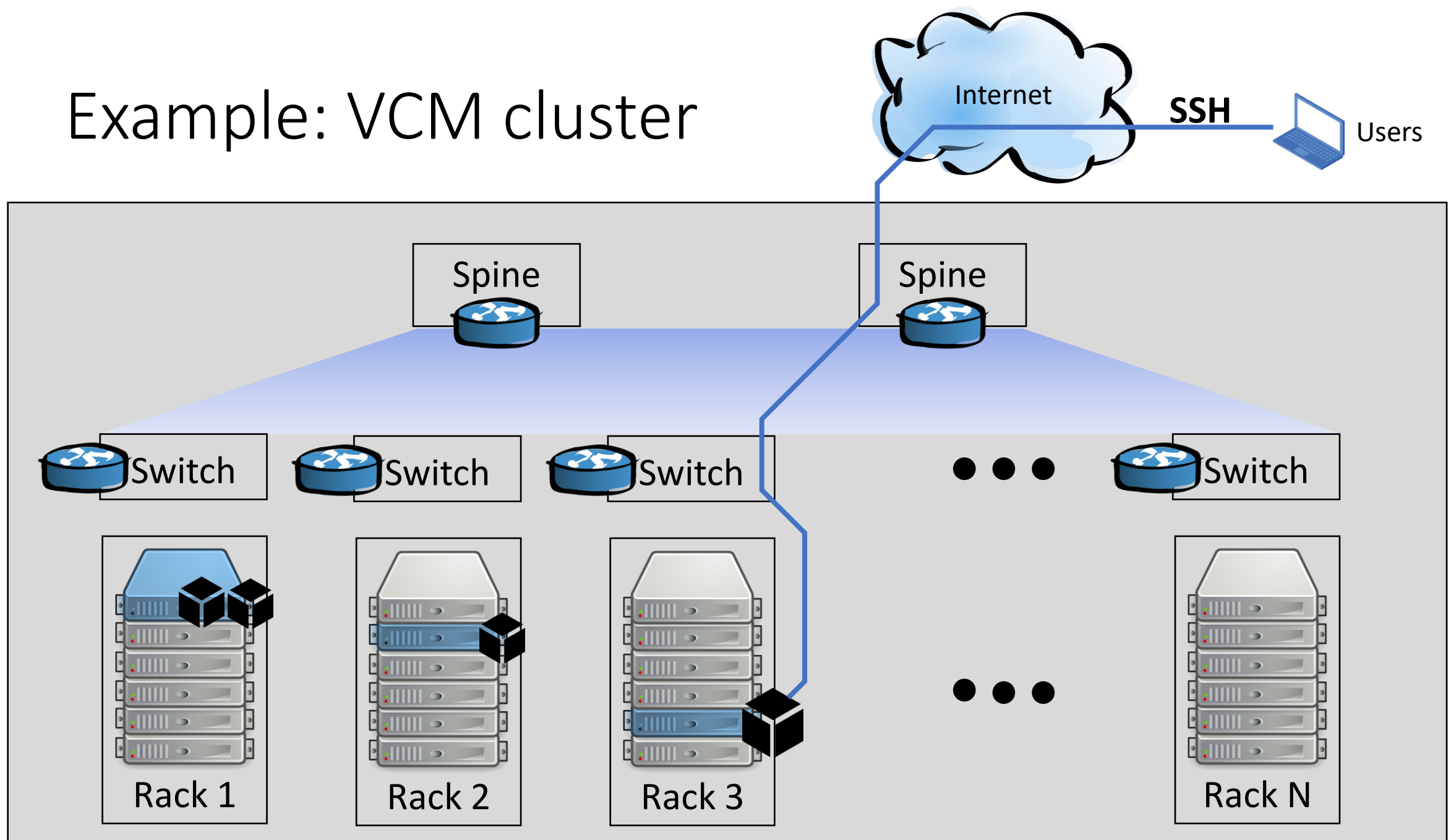
Example: VCM cluster



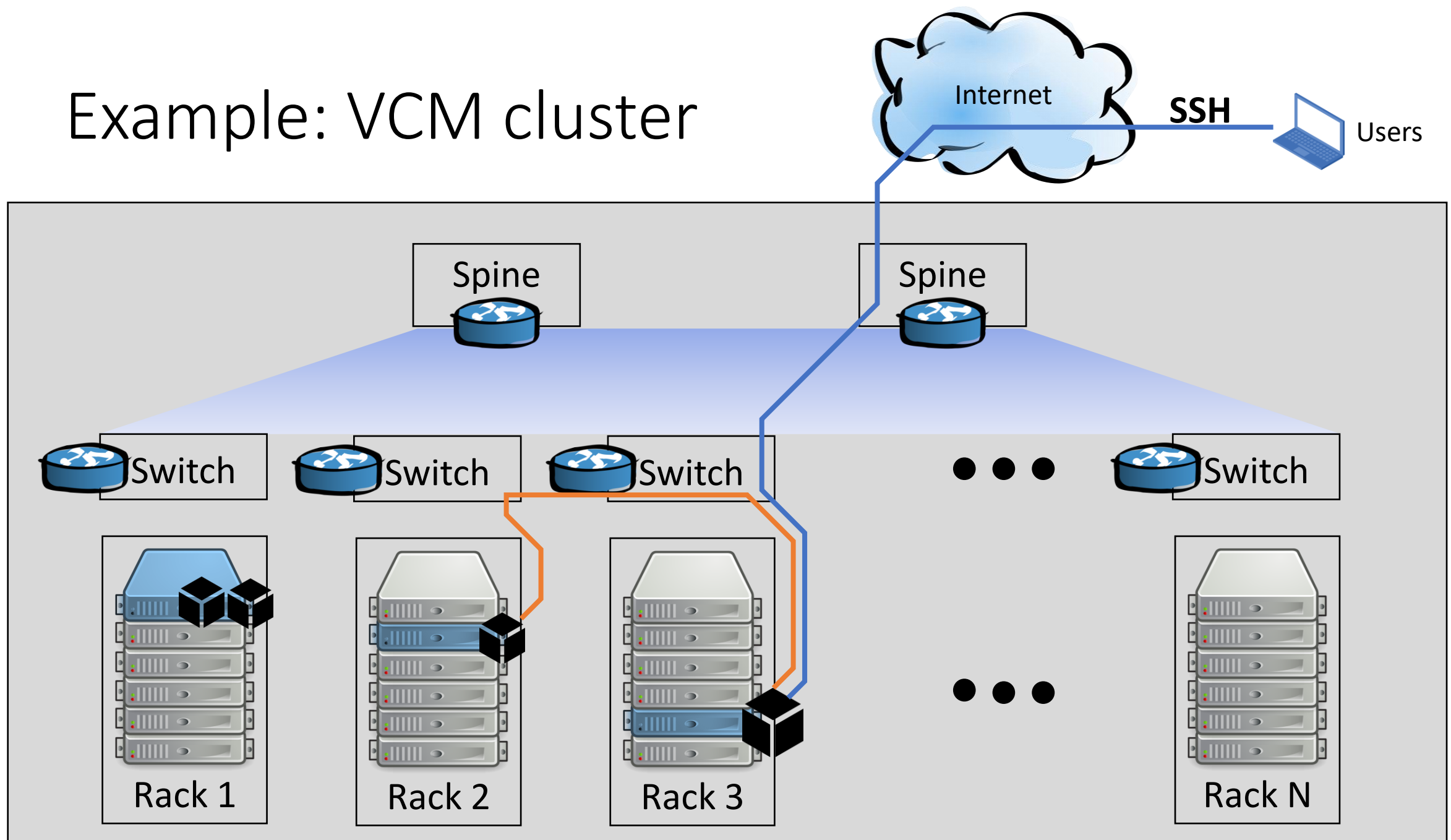
Example: VCM cluster



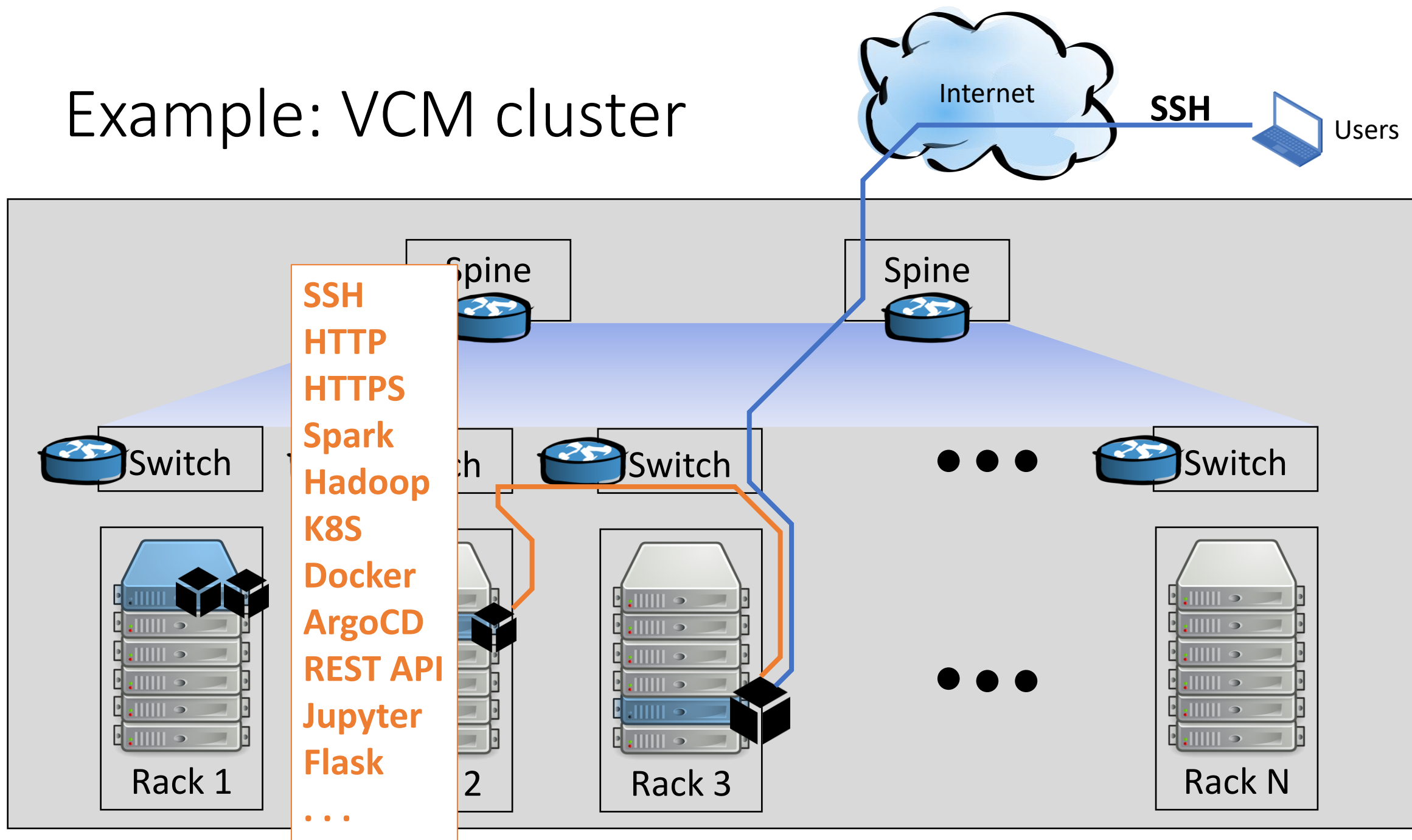
Example: VCM cluster



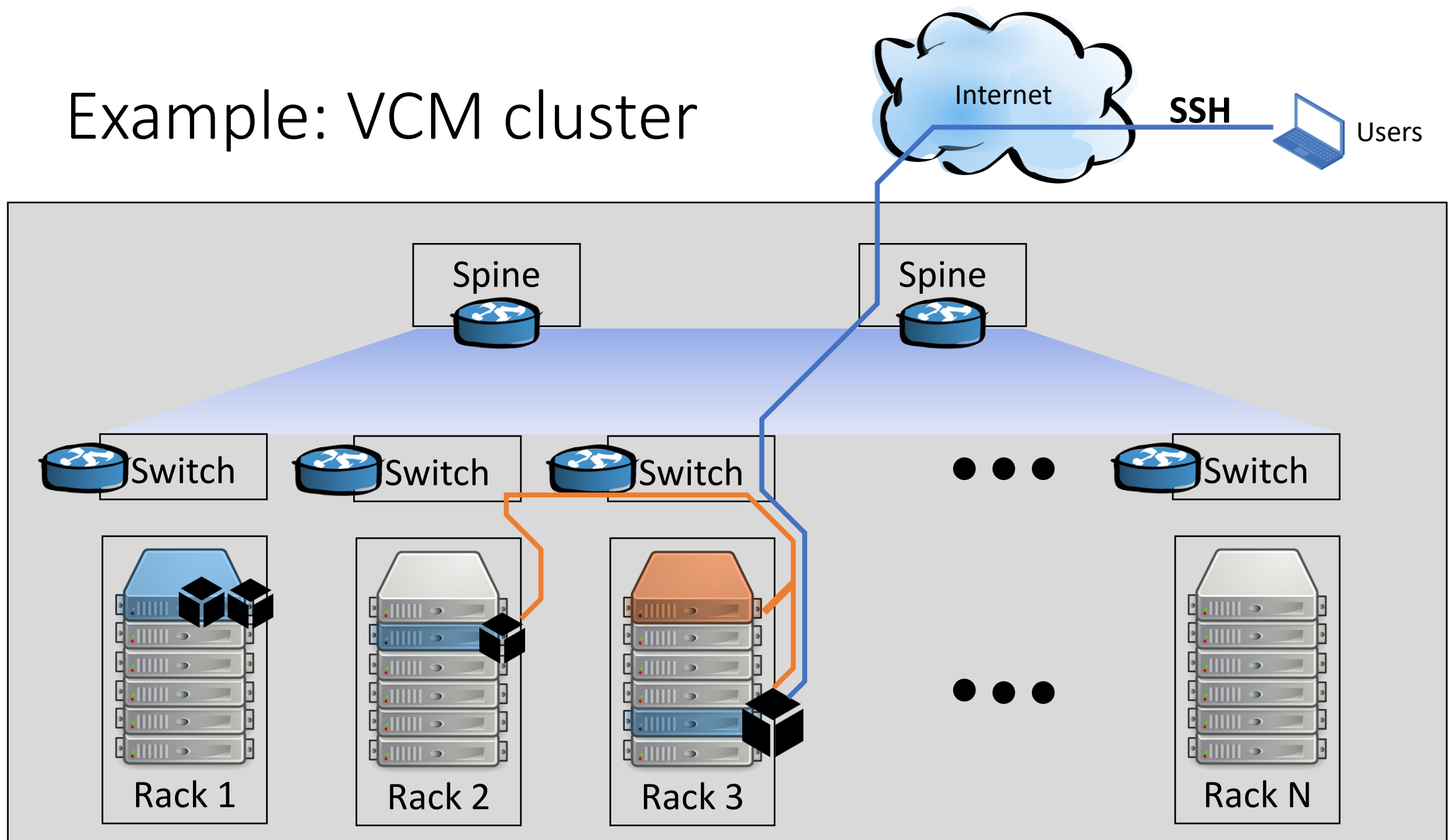
Example: VCM cluster



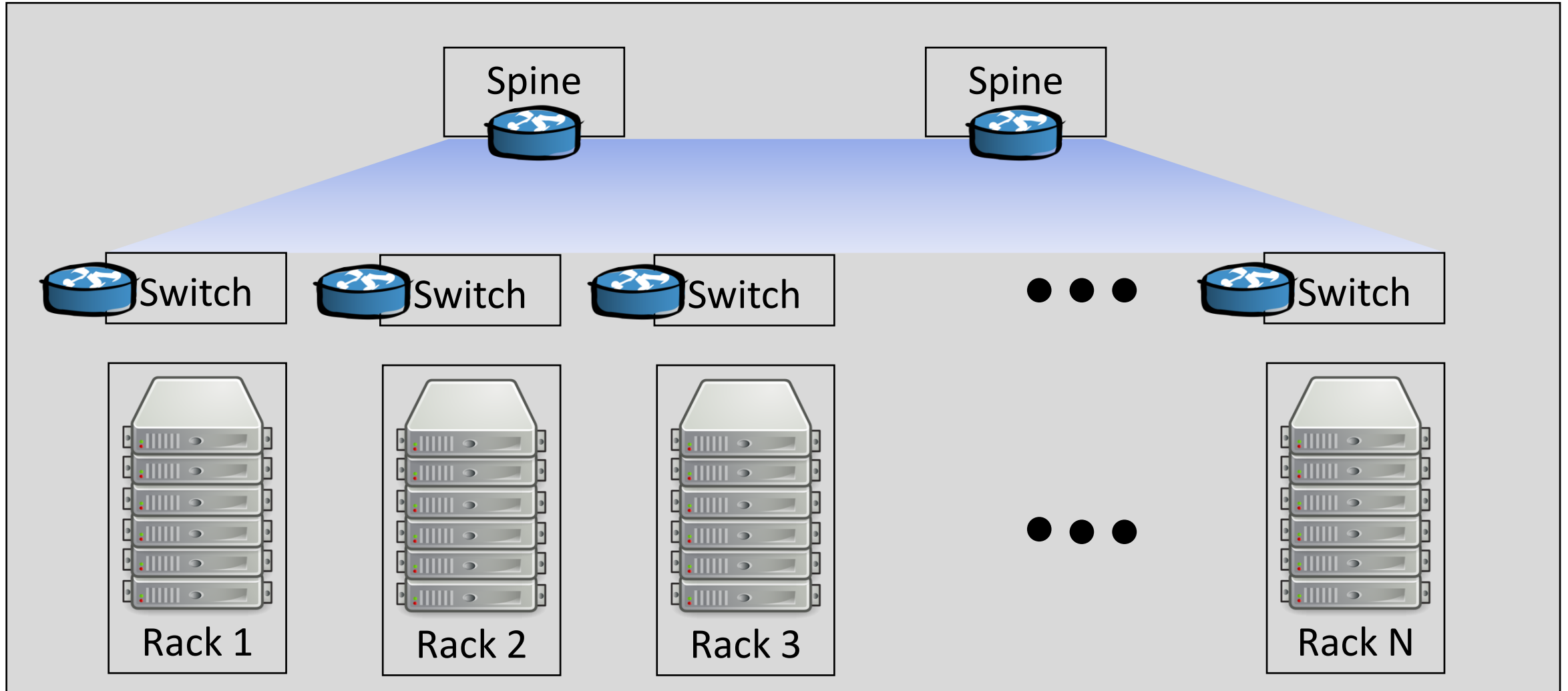
Example: VCM cluster



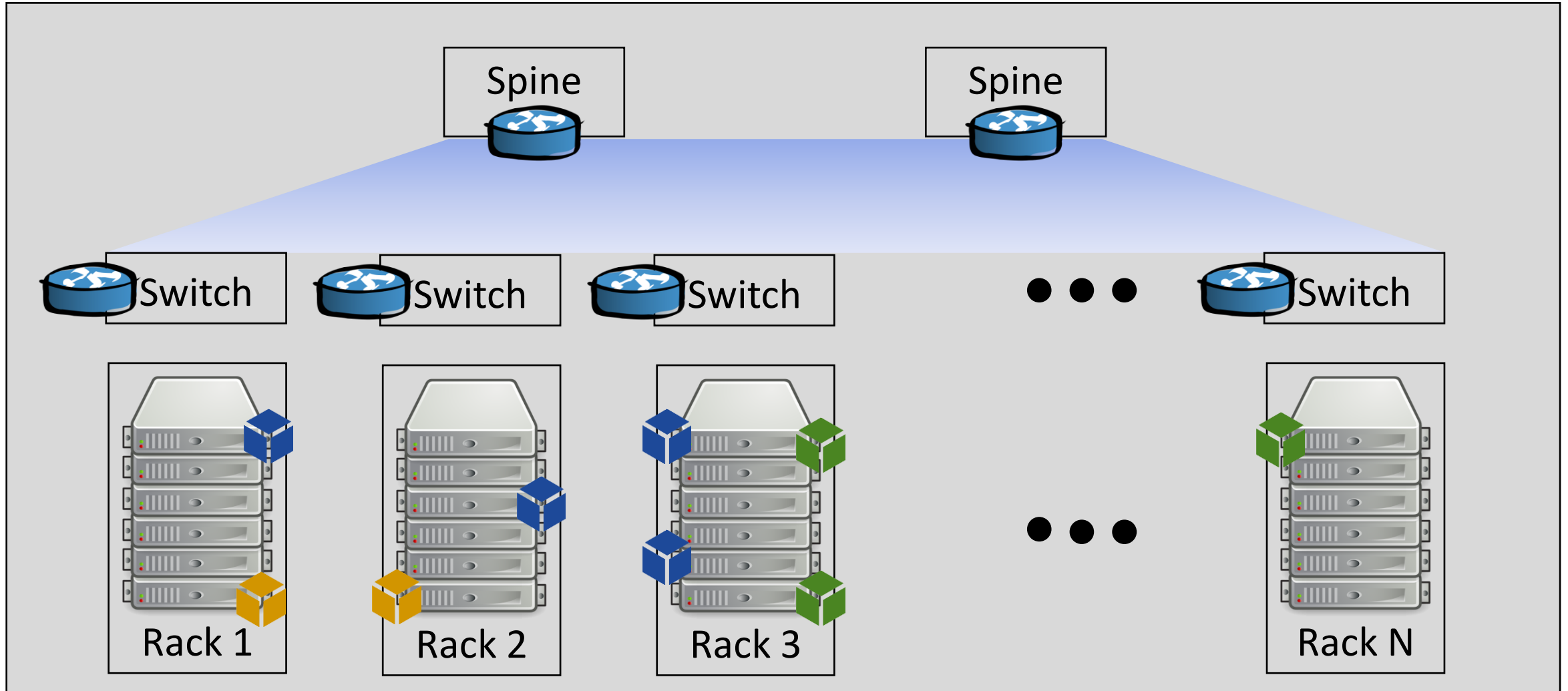
Example: VCM cluster



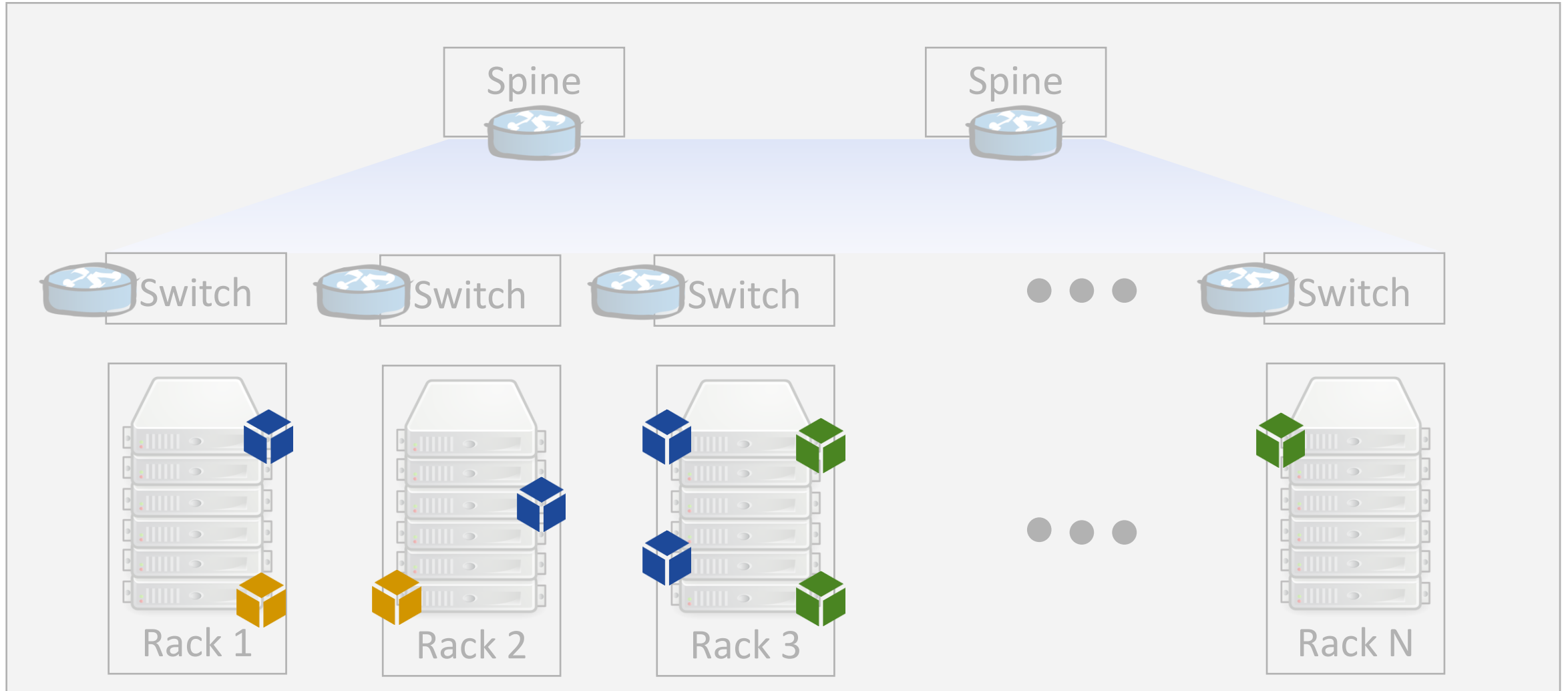
Virtual, overlay, and underlay networks



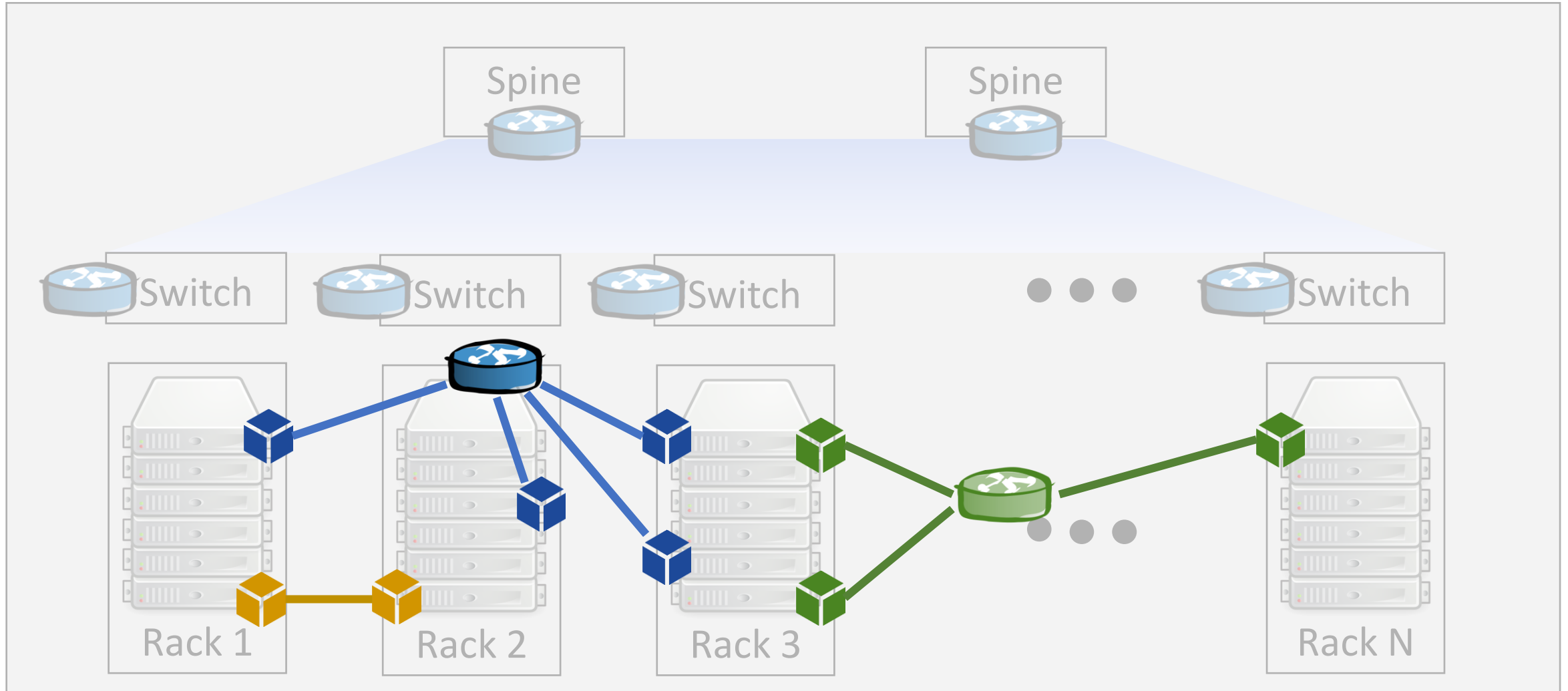
Virtual, overlay, and underlay networks



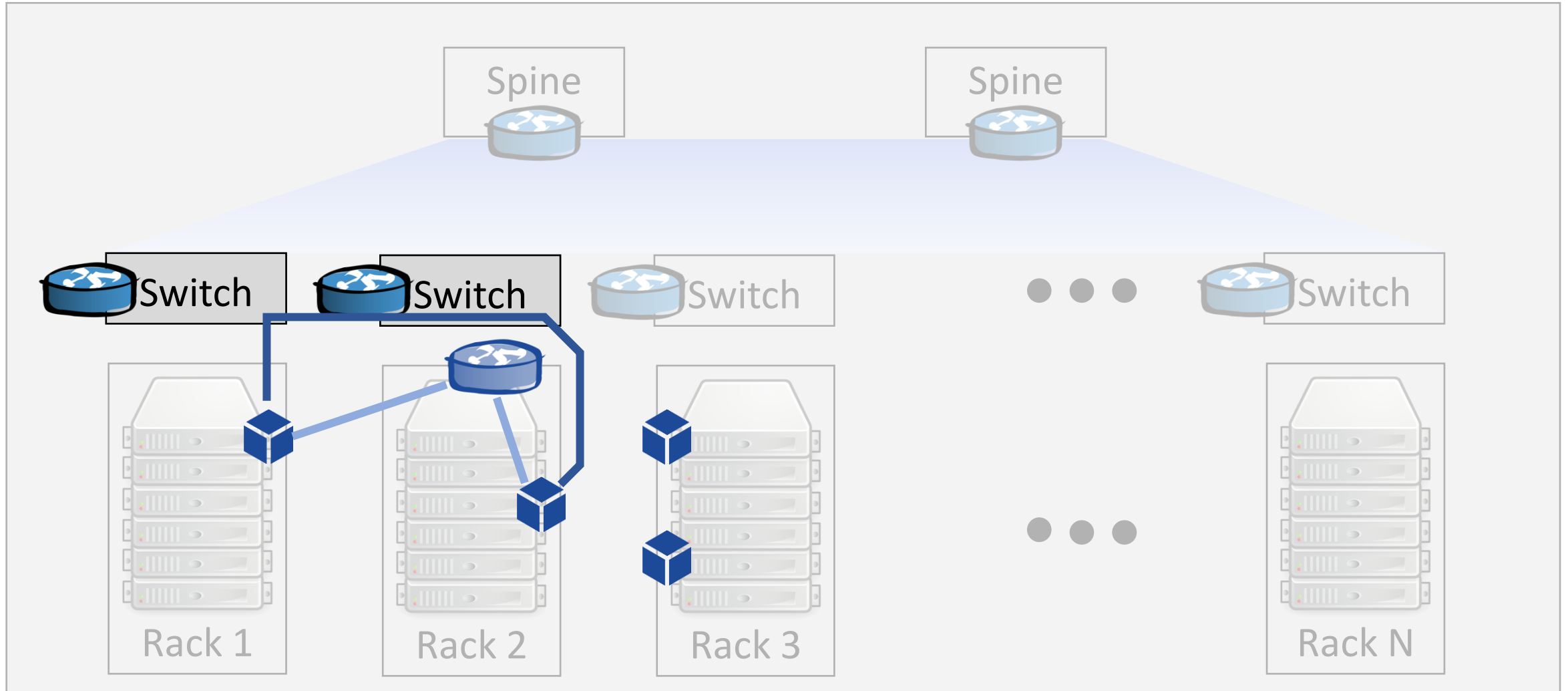
Virtual, overlay, and underlay networks



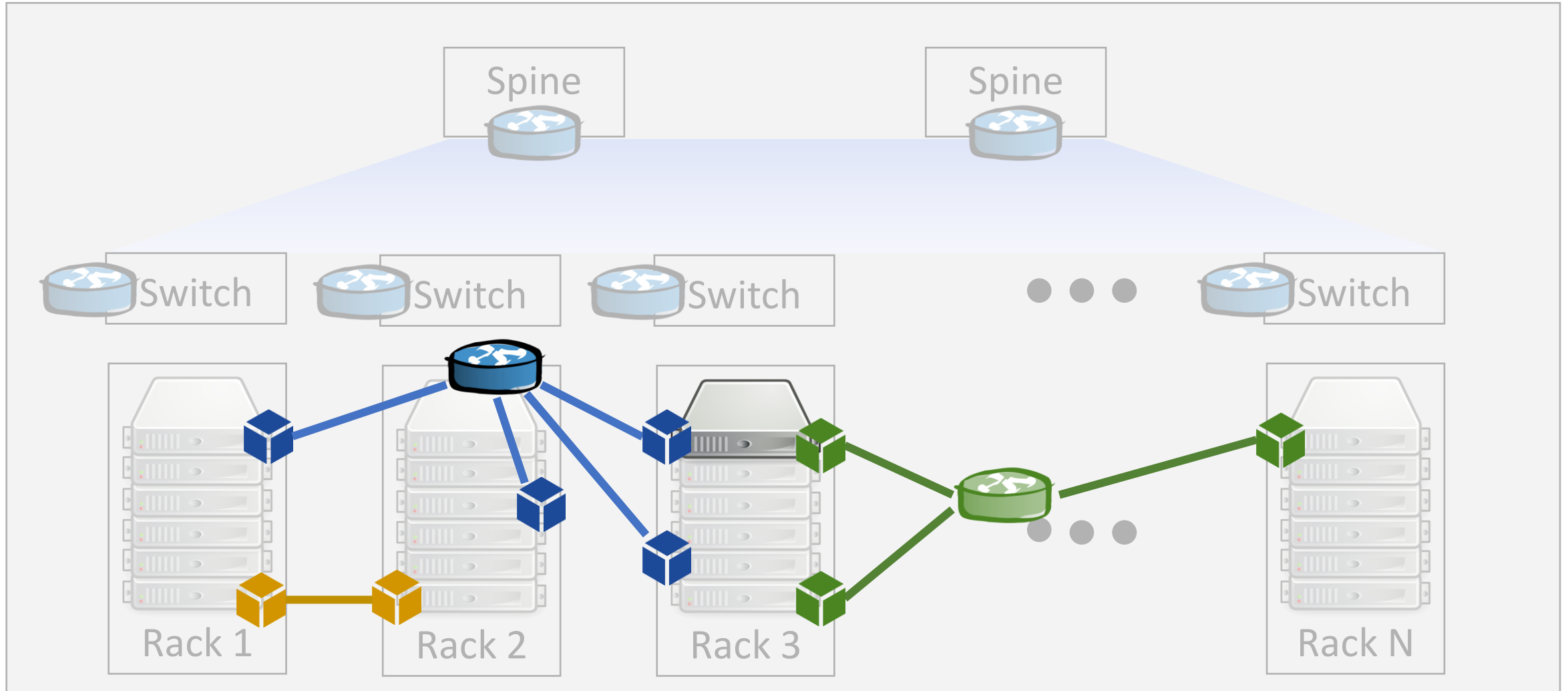
Virtual, **overlay**, and underlay networks



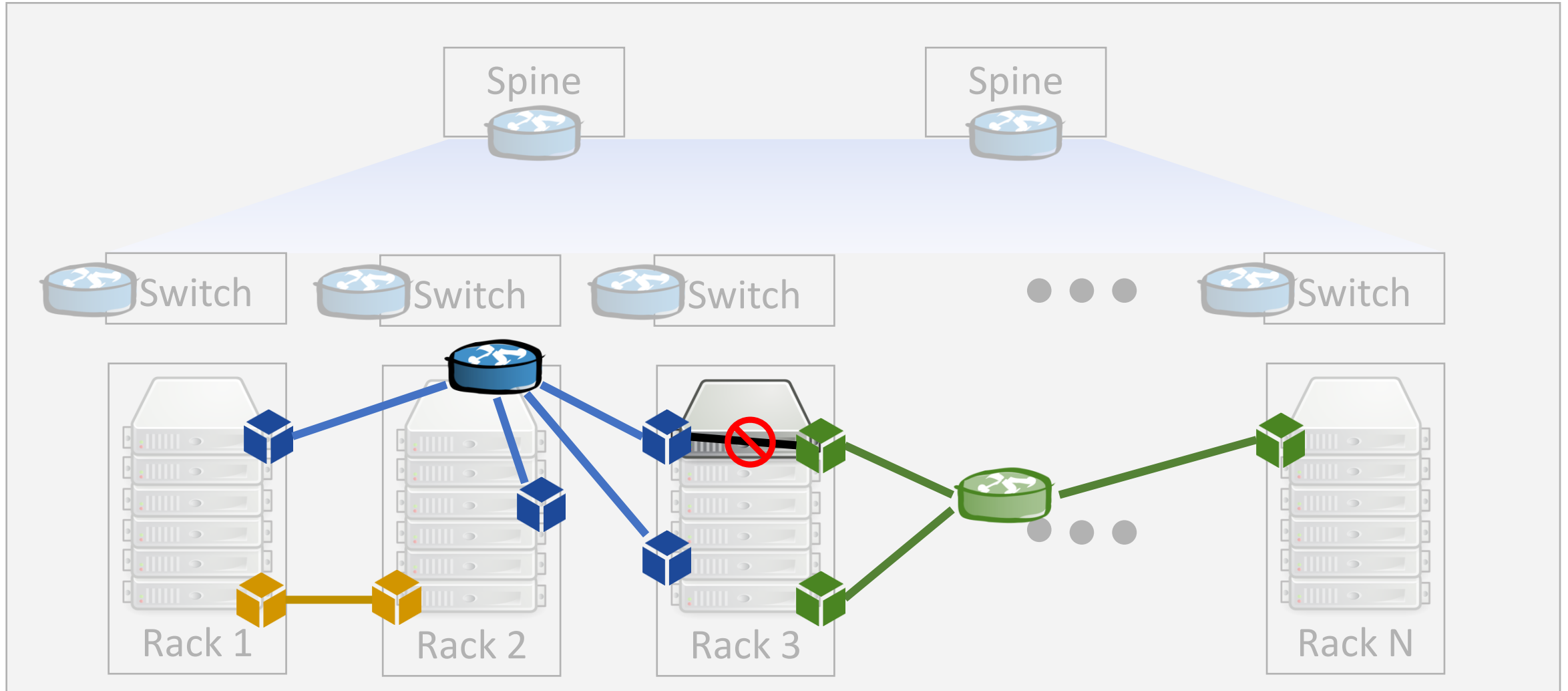
Virtual, overlay, and **underlay** networks



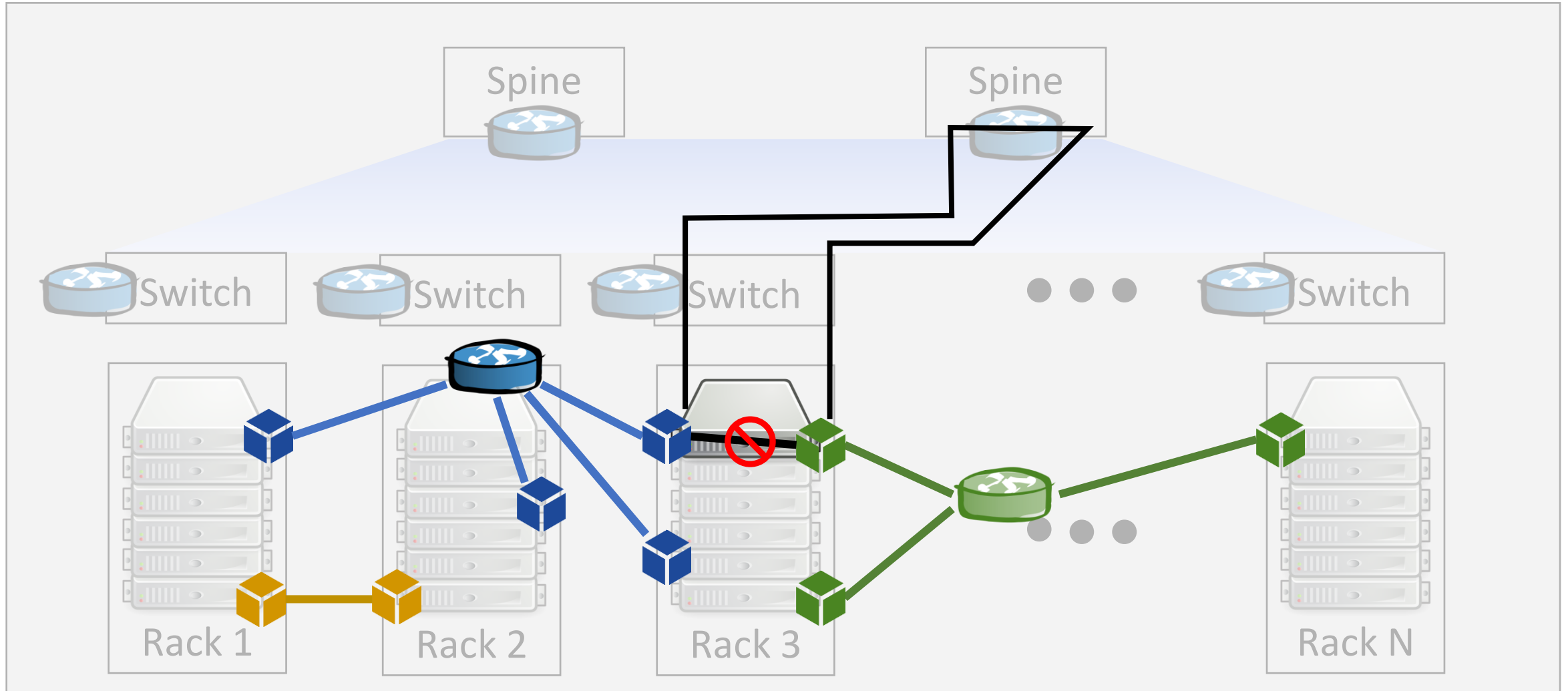
Virtual networks and isolation



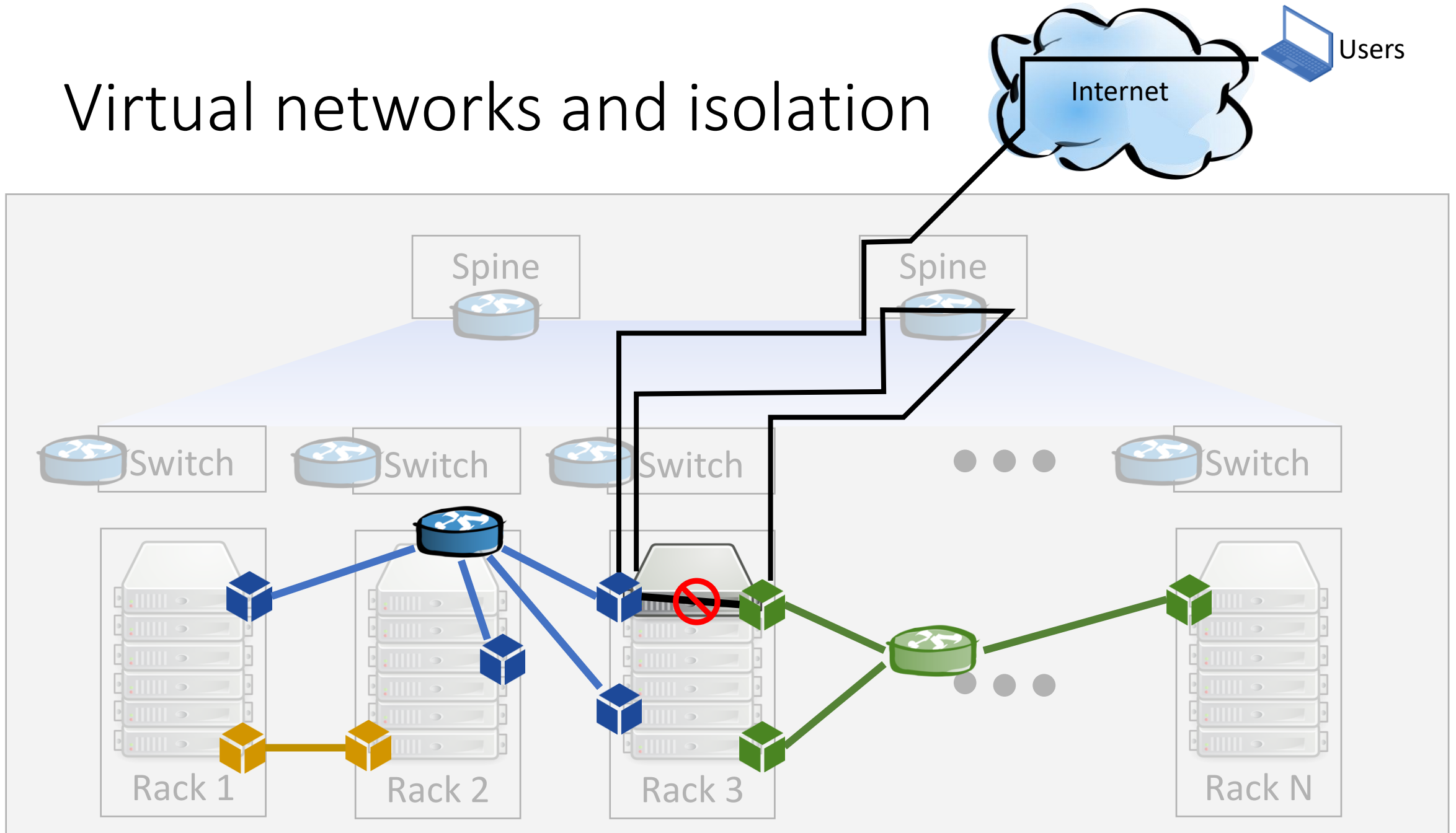
Virtual networks and isolation



Virtual networks and isolation



Virtual networks and isolation





CompSci 401: Cloud Computing

Building Virtual Networks

Prof. Ítalo Cunha



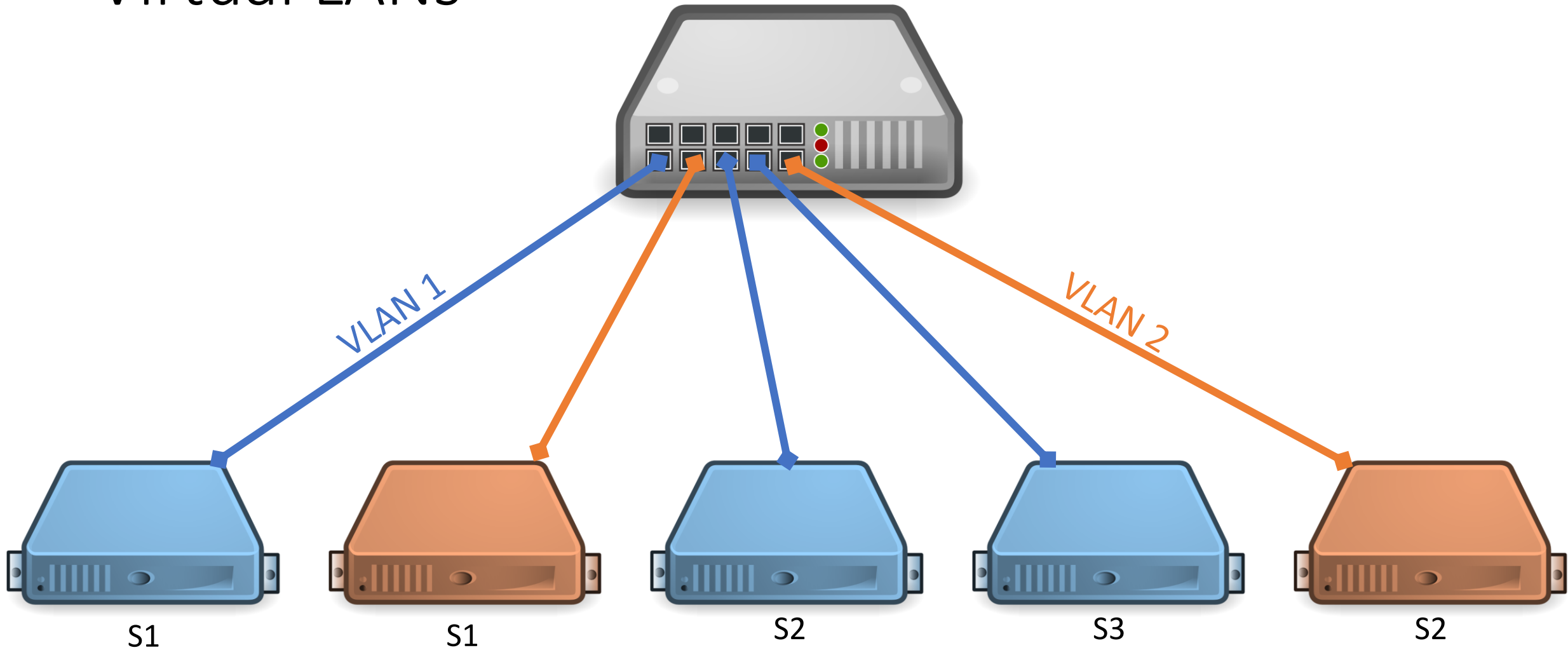
Virtual LANs

- VLANs are a tagging mechanism available on Ethernet switches
 - A switch port can be part of one or more VLANs
 - Only who operates the switch can configure VLANs (cloud provider)

Virtual LANs

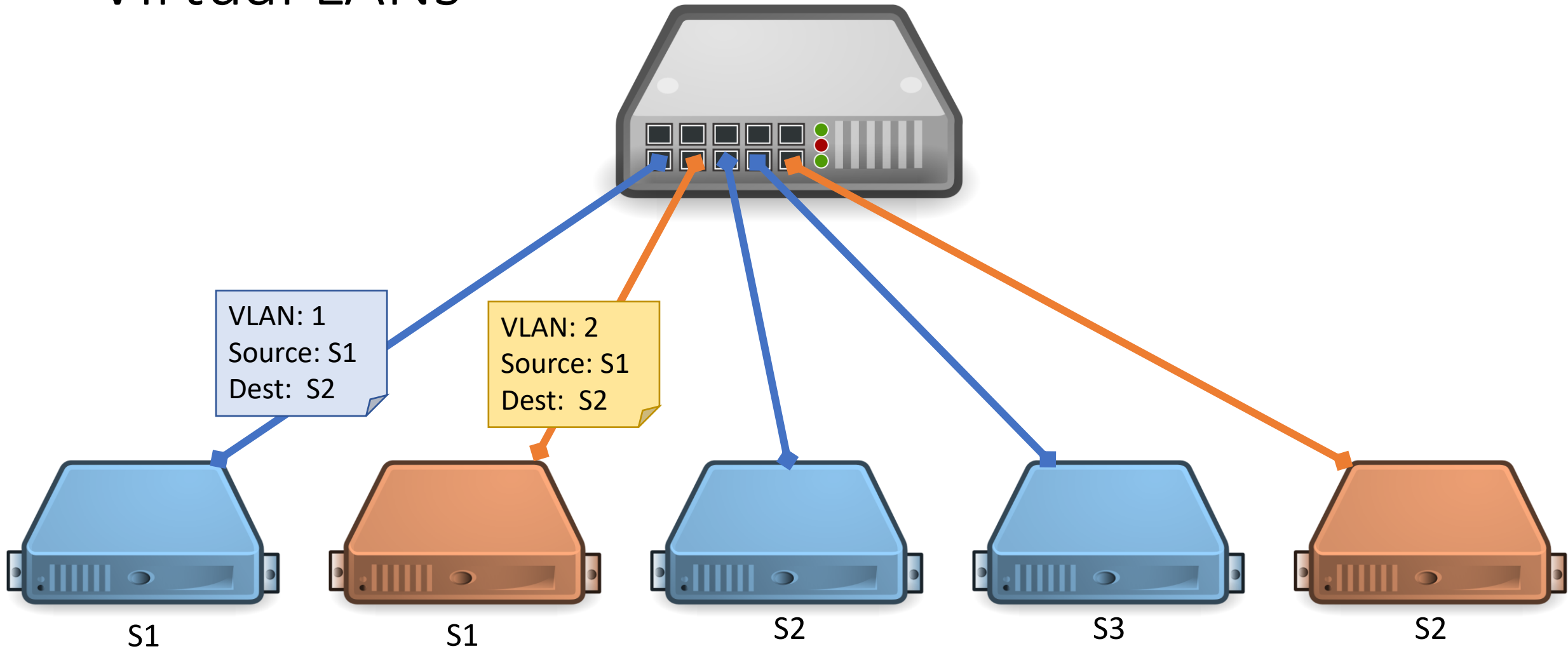
- VLANs are a tagging mechanism available on Ethernet switches
 - A switch port can be part of one or more VLANs
 - Only who operates the switch can configure VLANs (cloud provider)
- Packets must carry correct VLAN tags
 - Servers add VLAN tags to their packets
- VLANs provide isolation across ports

Virtual LANs

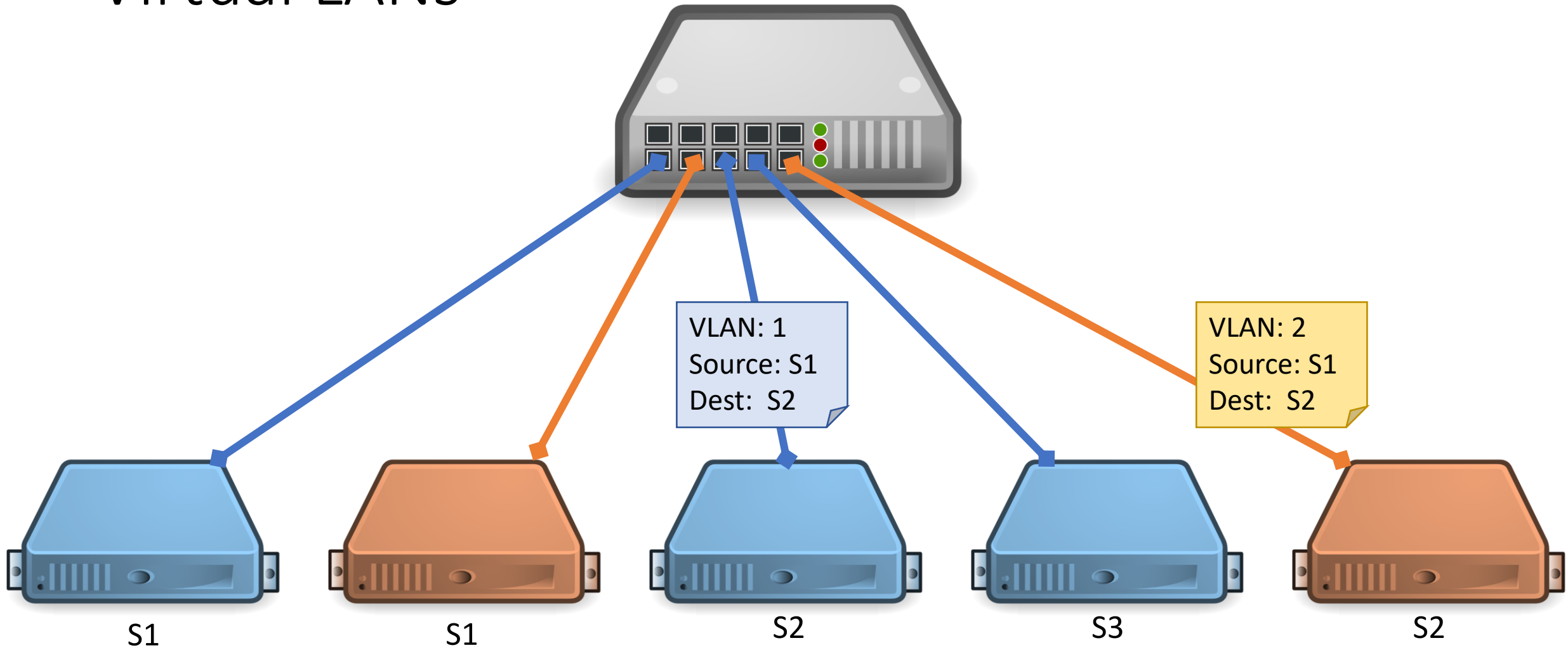


Servers on different VLANs can use the same IP address

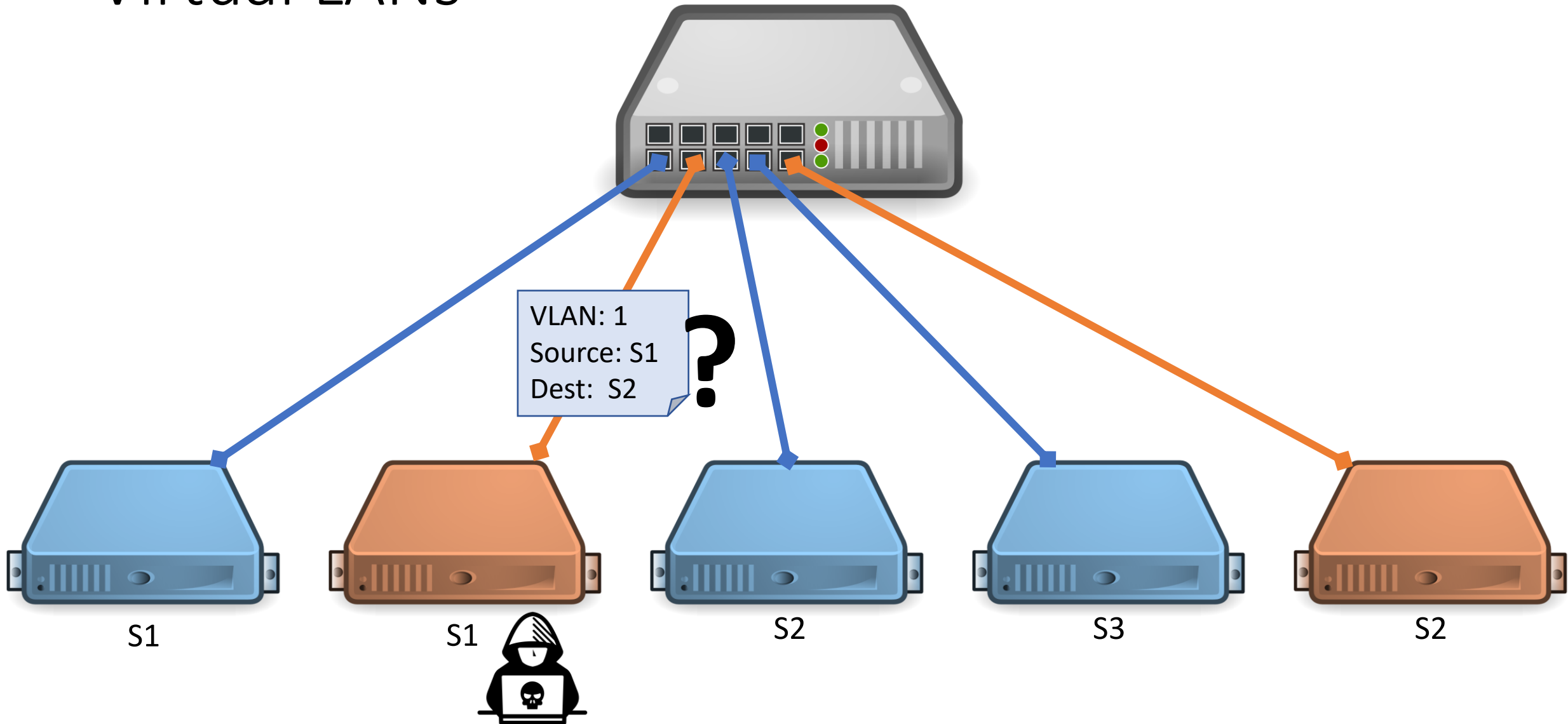
Virtual LANs



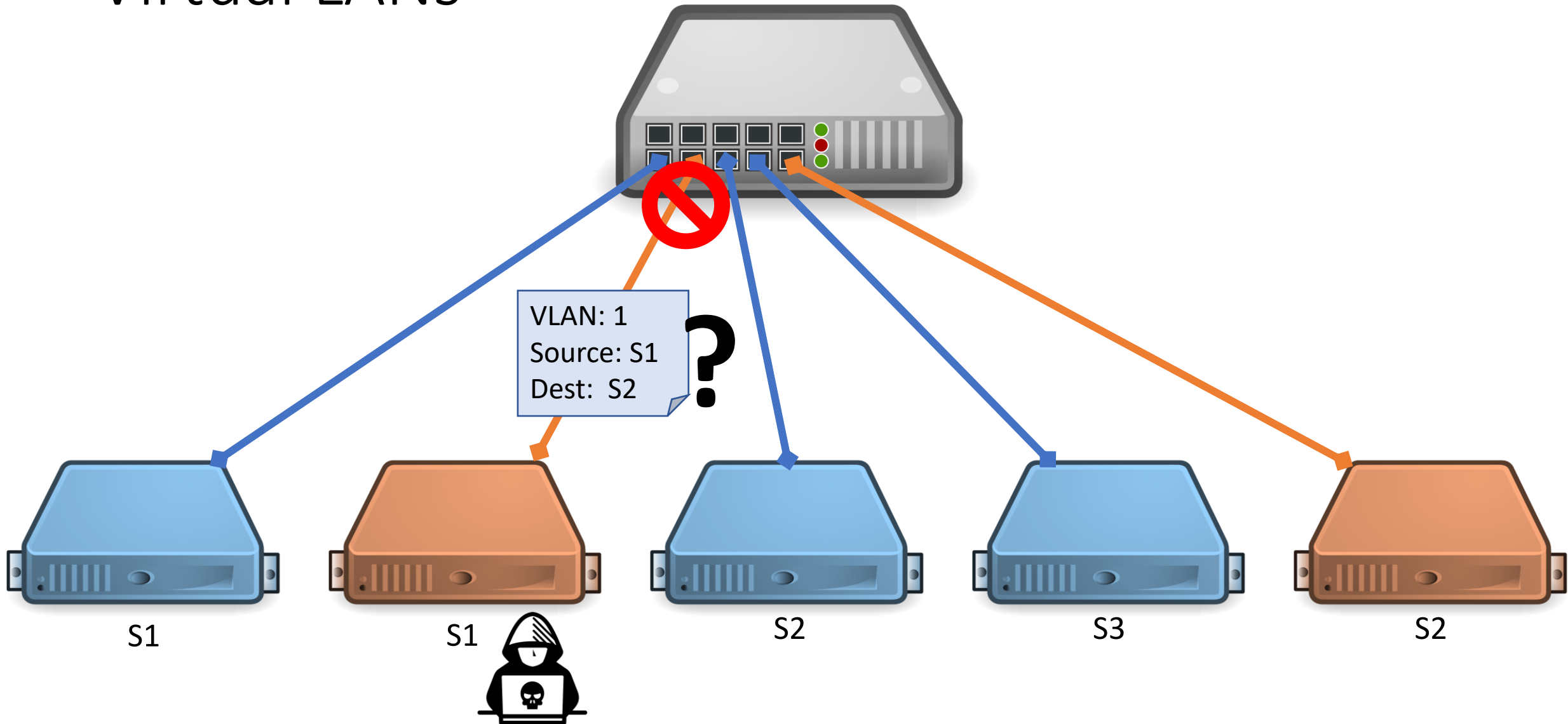
Virtual LANs



Virtual LANs

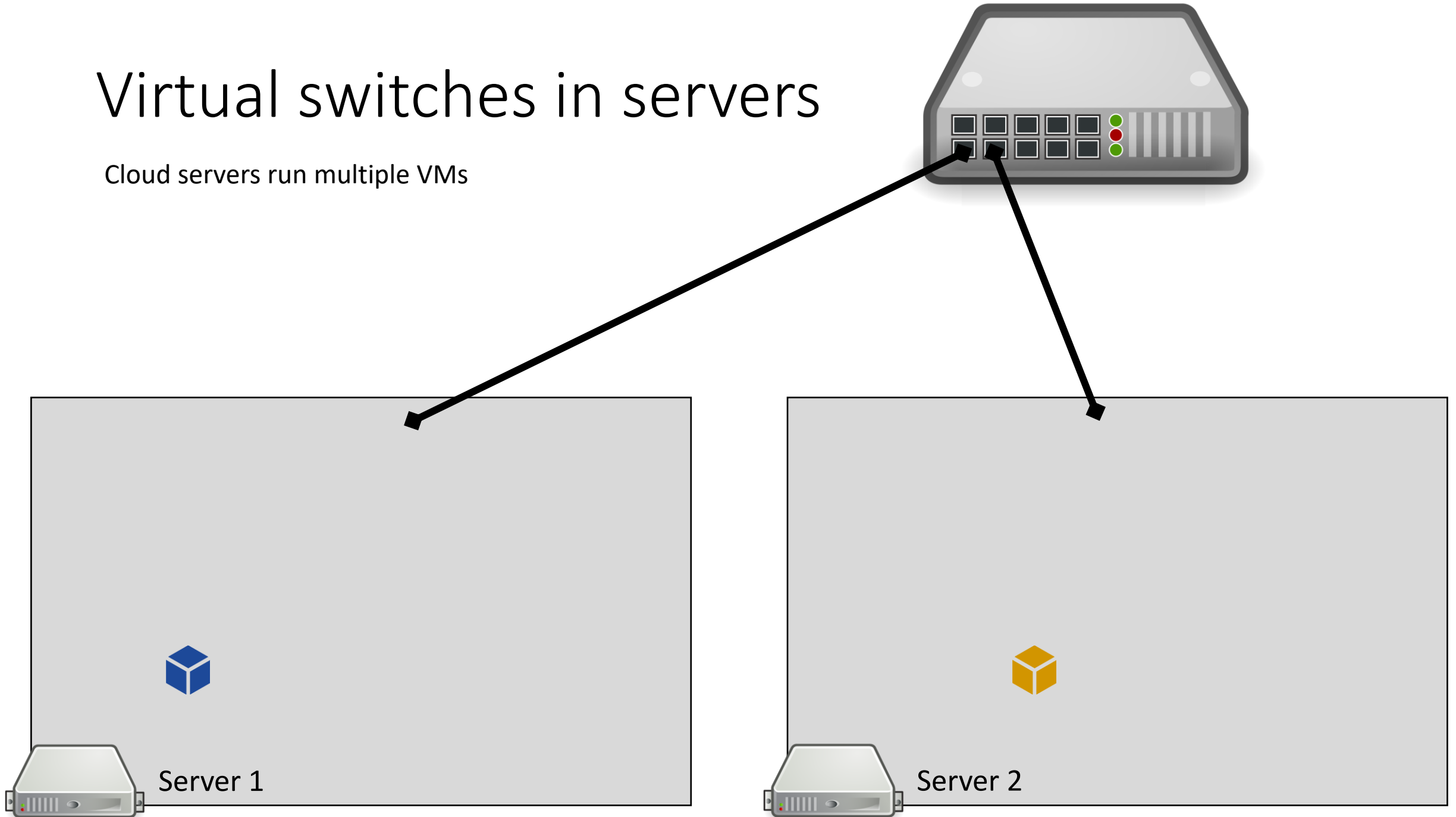


Virtual LANs



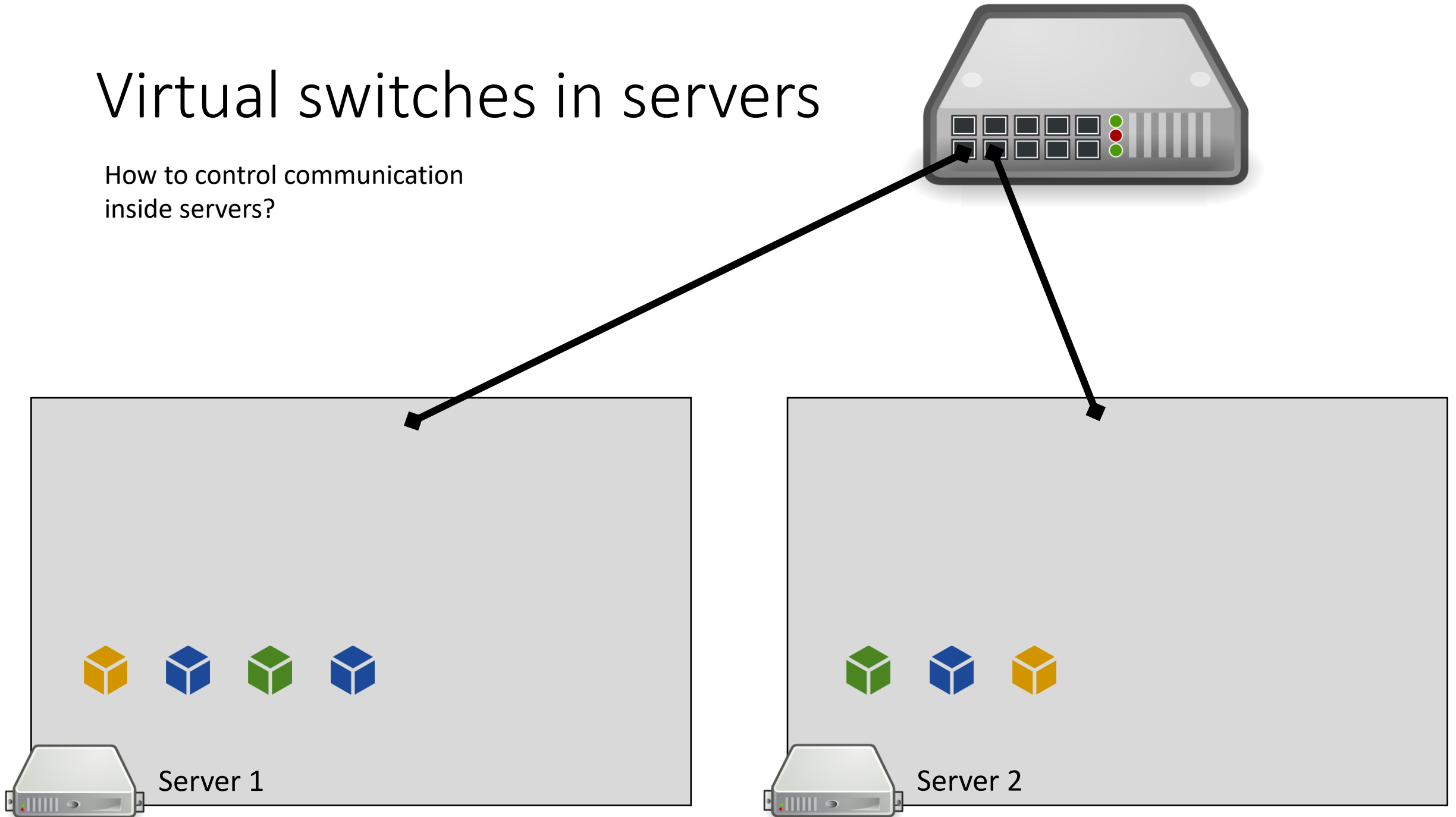
Virtual switches in servers

Cloud servers run multiple VMs



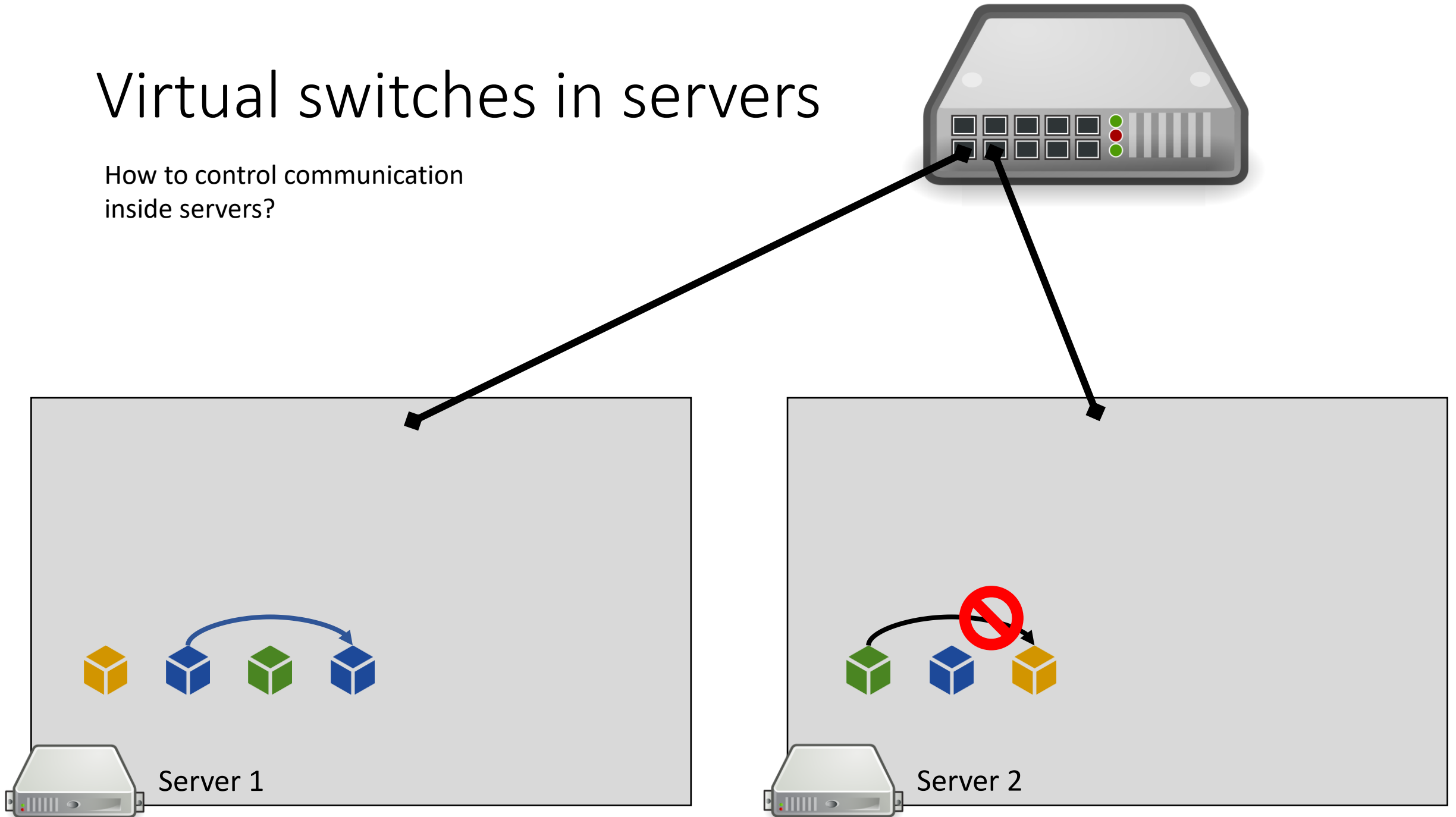
Virtual switches in servers

How to control communication
inside servers?



Virtual switches in servers

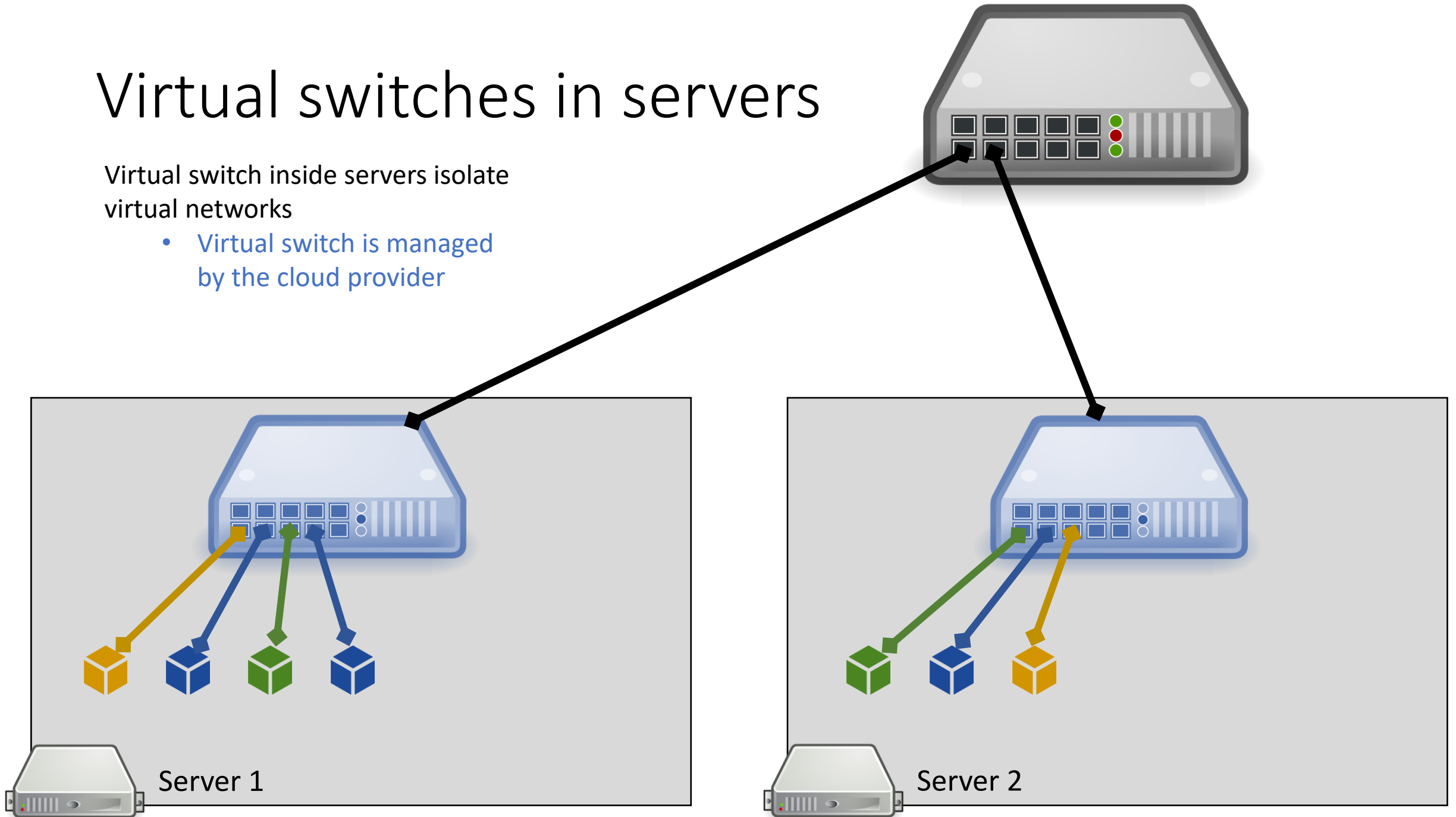
How to control communication
inside servers?



Virtual switches in servers

Virtual switch inside servers isolate virtual networks

- Virtual switch is managed by the cloud provider



Network virtualization technologies

- Packet tagging
 - VLANs, MAC rewriting
- Encapsulation
 - GRE, VXLAN, MPLS

Network virtualization technologies

- Packet tagging
 - VLANs, MAC rewriting
- Encapsulation
 - GRE, VXLAN, MPLS
- All these technologies operate on the same basic principles:
 - Packets carry a way to identify which virtual network they belong to
 - Packet routing and forwarding isolated across virtual networks



CompSci 401: Cloud Computing

Virtual Network Technologies

Prof. Ítalo Cunha



VLAN vs VXLAN

Ethernet packet tagged with VLAN



Plain Ethernet packet



VLAN vs VXLAN

Ethernet packet tagged with VLAN

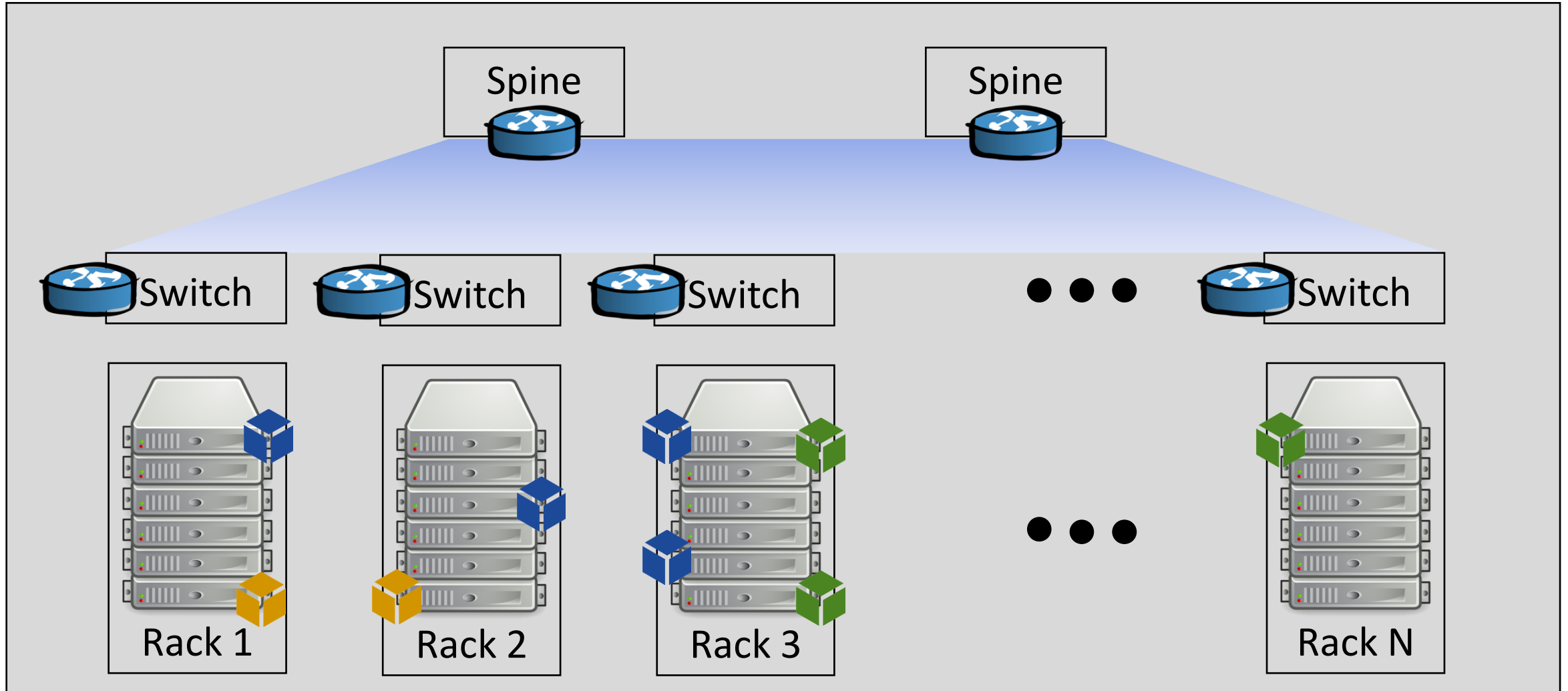


12-bit identifier: 4096 VLANs

Plain Ethernet packet



Cloud providers may have tens of thousands of virtual networks!



VLAN vs VXLAN

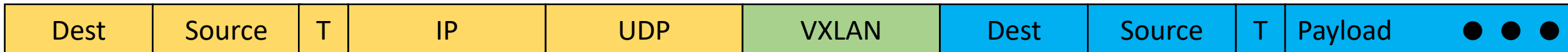
VXLAN encapsulates the **original packet** and route packets based on an **outer header**

- **Outer header** built by the network
- Transparent to virtual machines

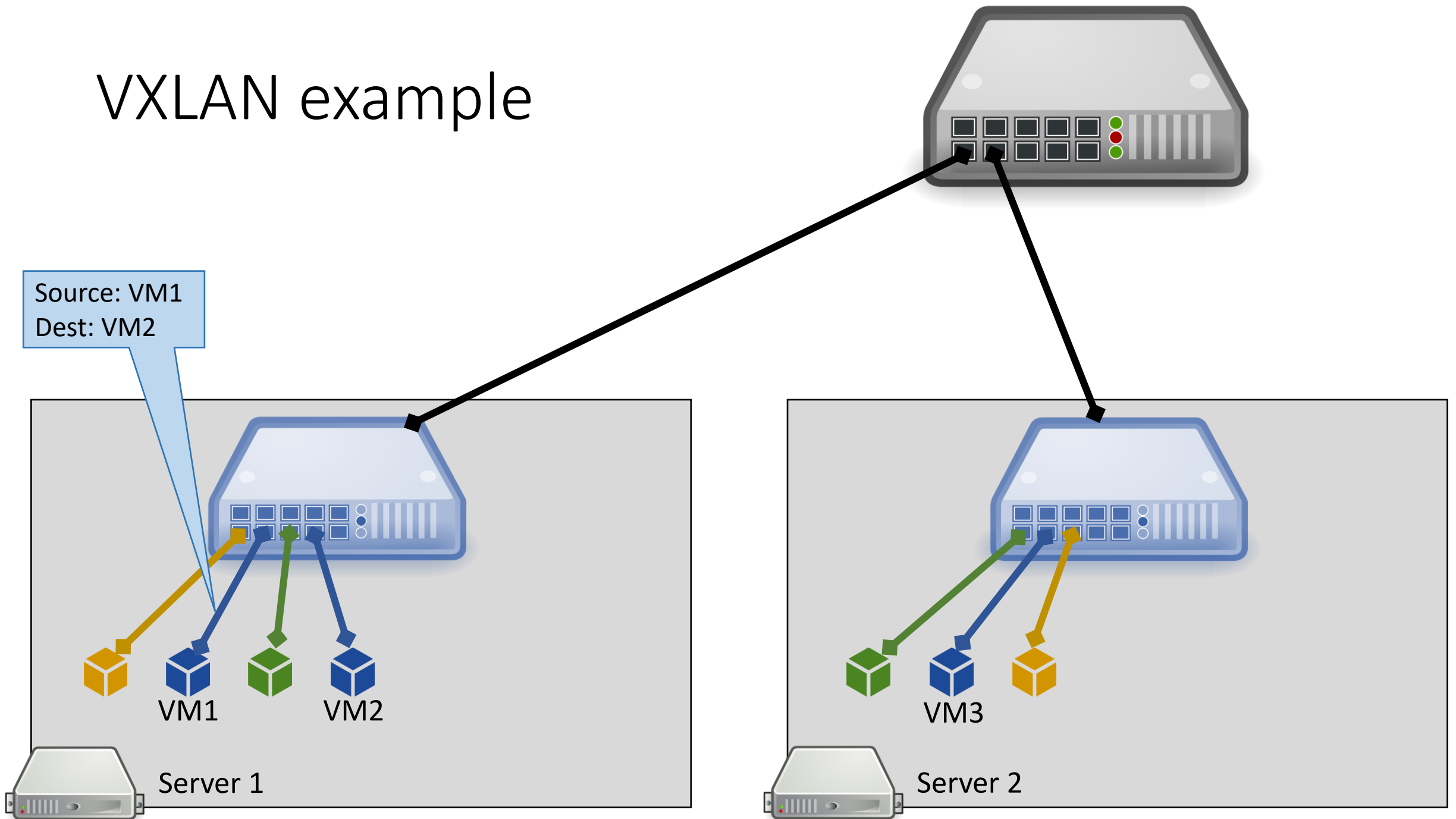
Plain **Ethernet packet**



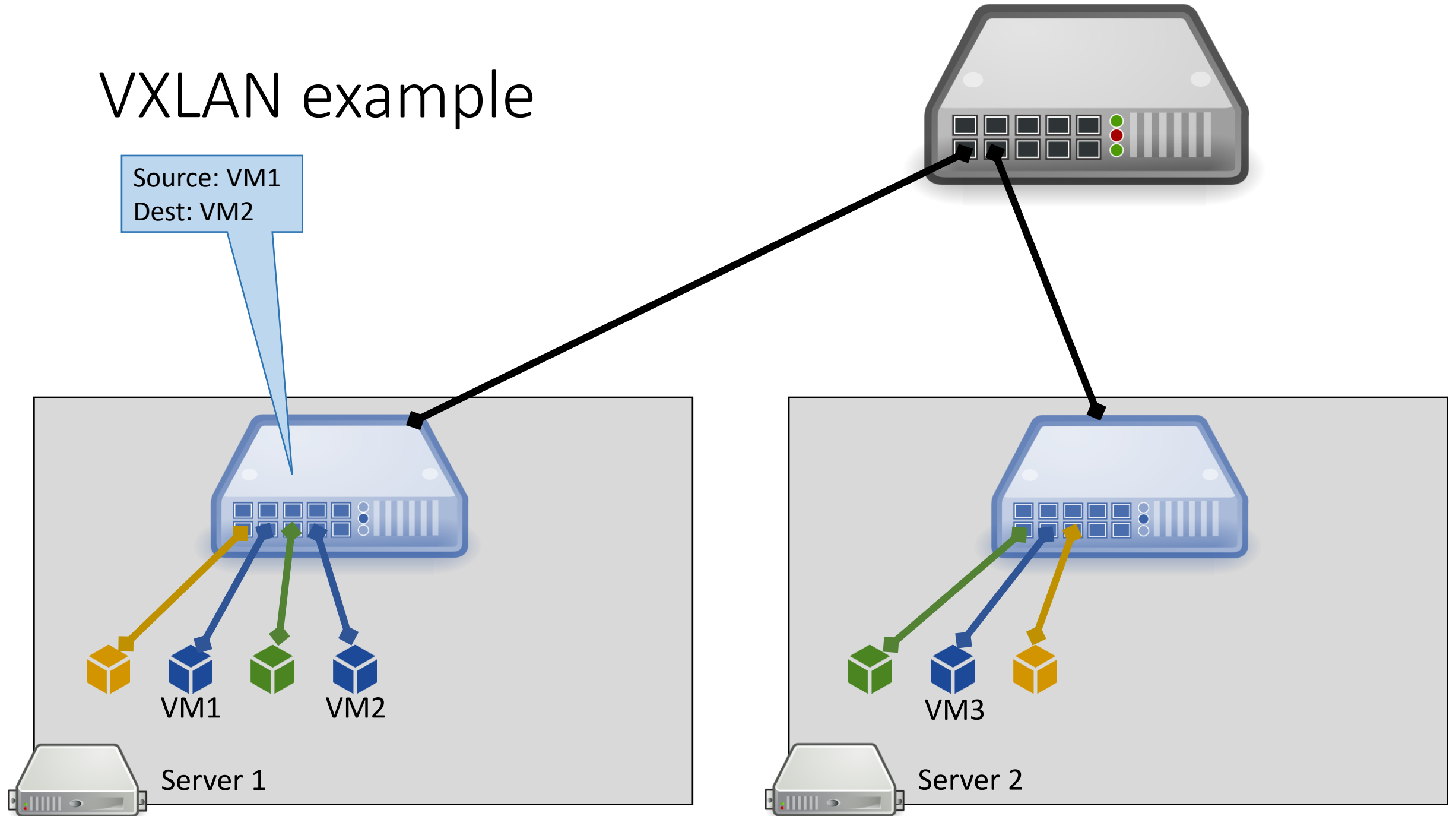
Ethernet packet encapsulating another **Ethernet packet** using **VXLAN**



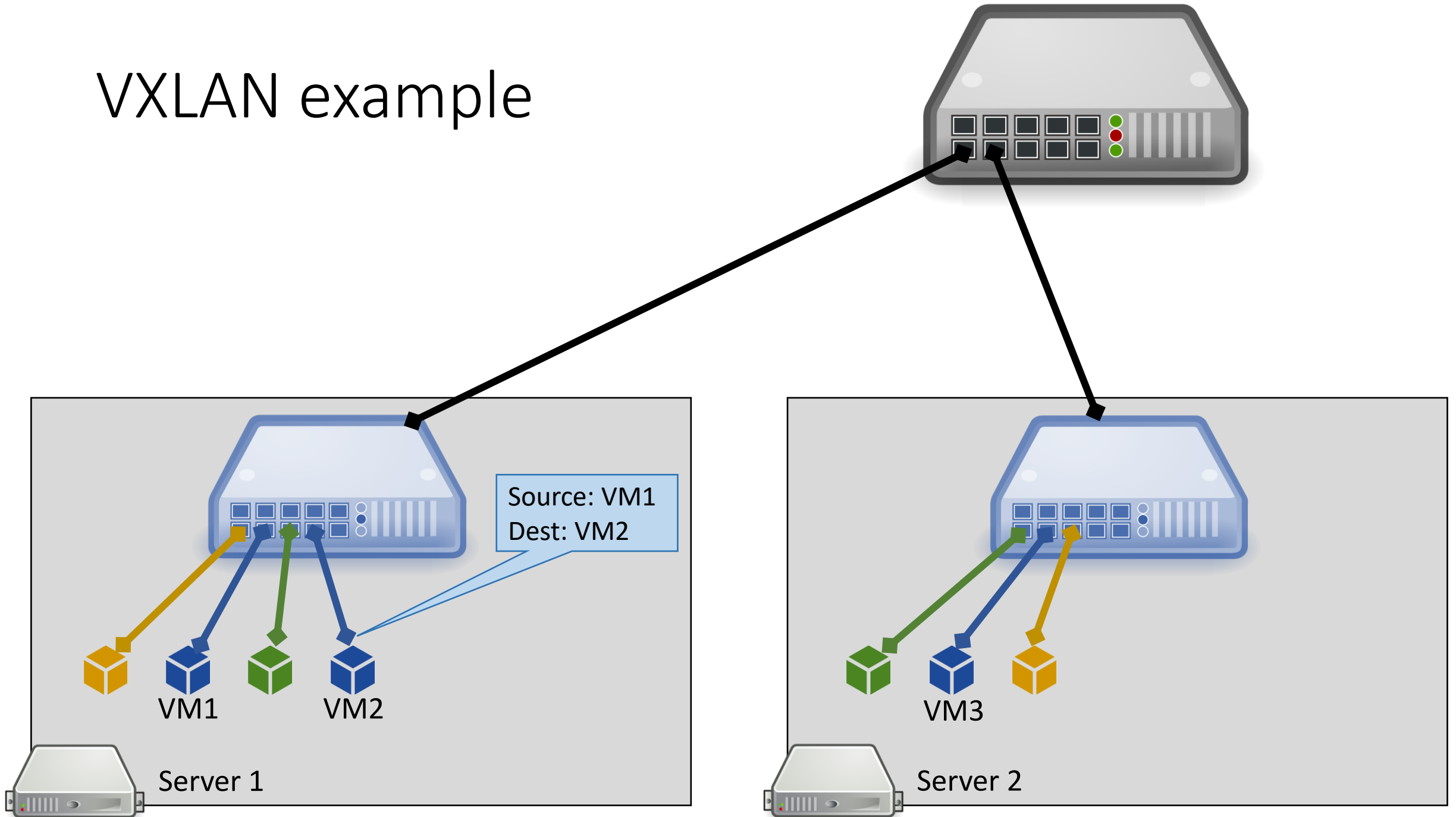
VXLAN example



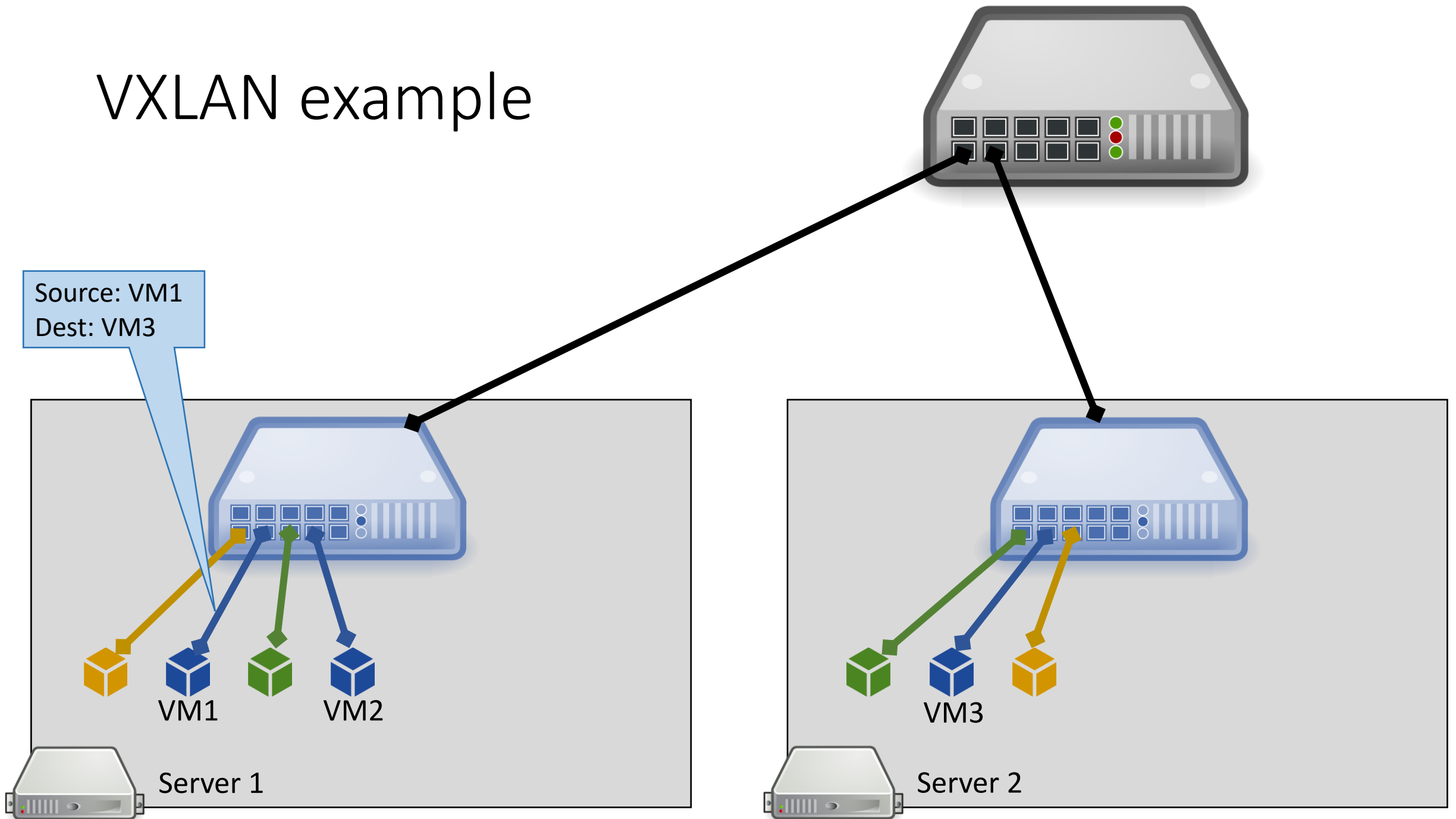
VXLAN example



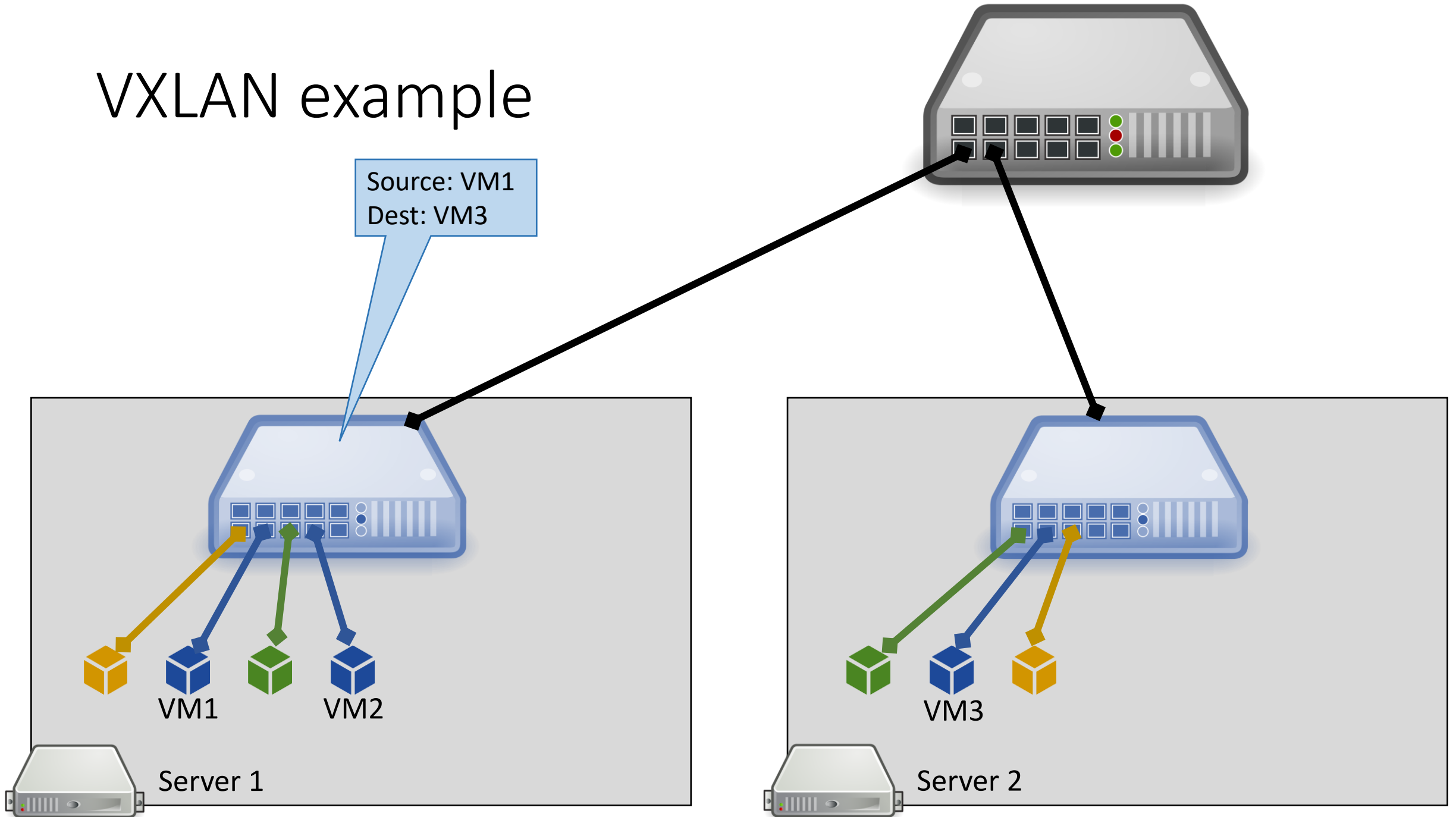
VXLAN example



VXLAN example



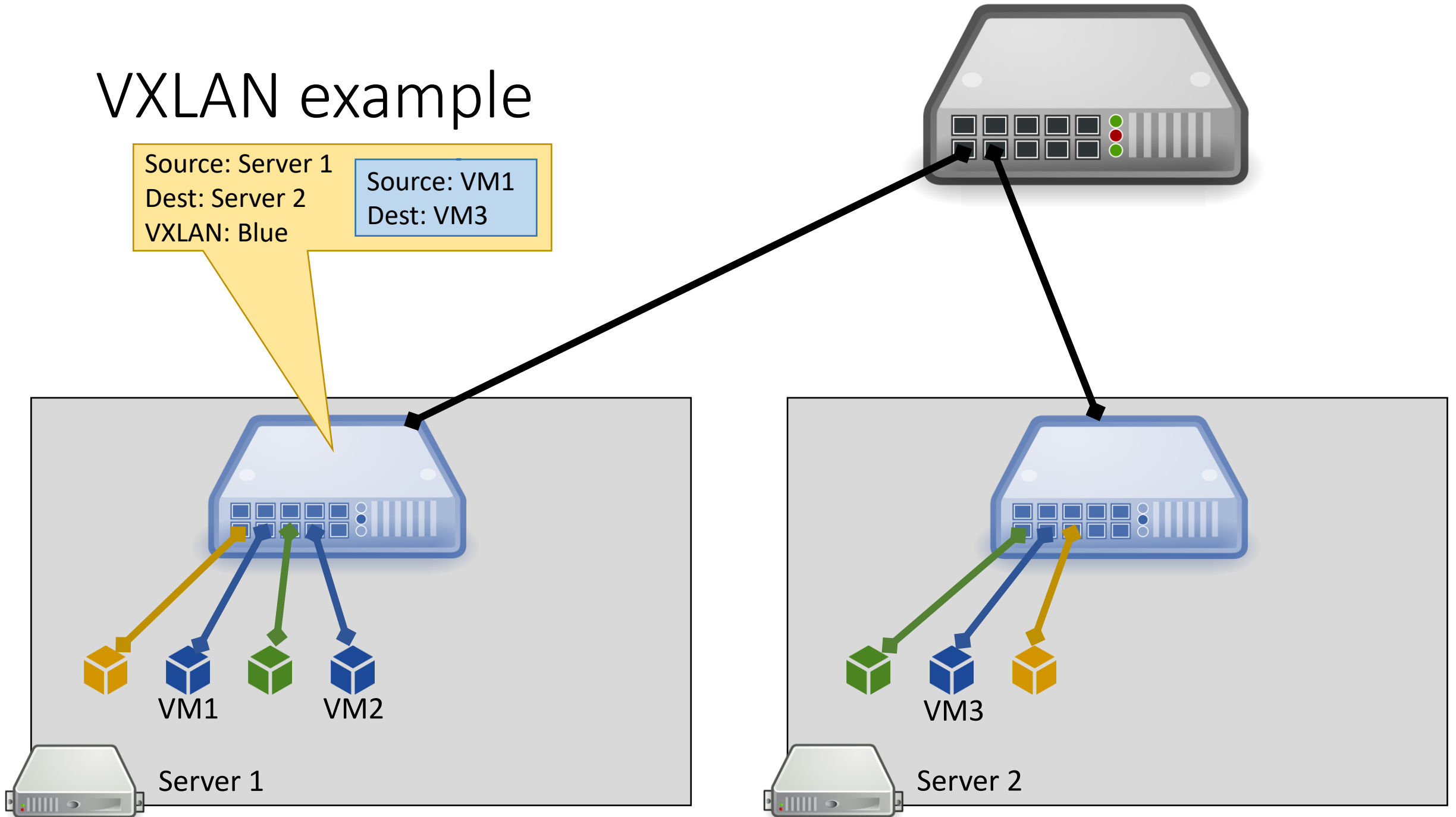
VXLAN example



VXLAN example

Source: Server 1
Dest: Server 2
VXLAN: Blue

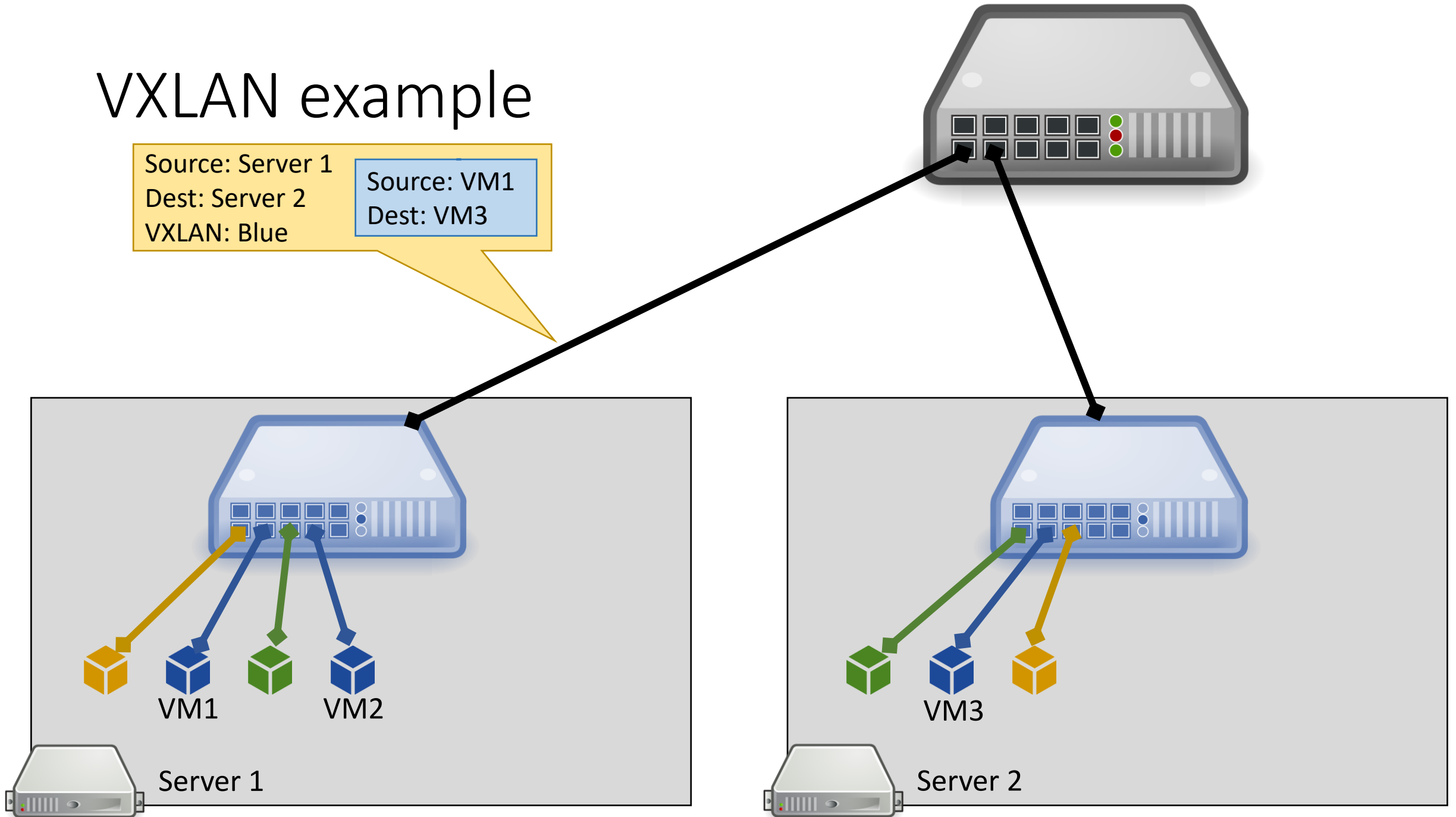
Source: VM1
Dest: VM3



VXLAN example

Source: Server 1
Dest: Server 2
VXLAN: Blue

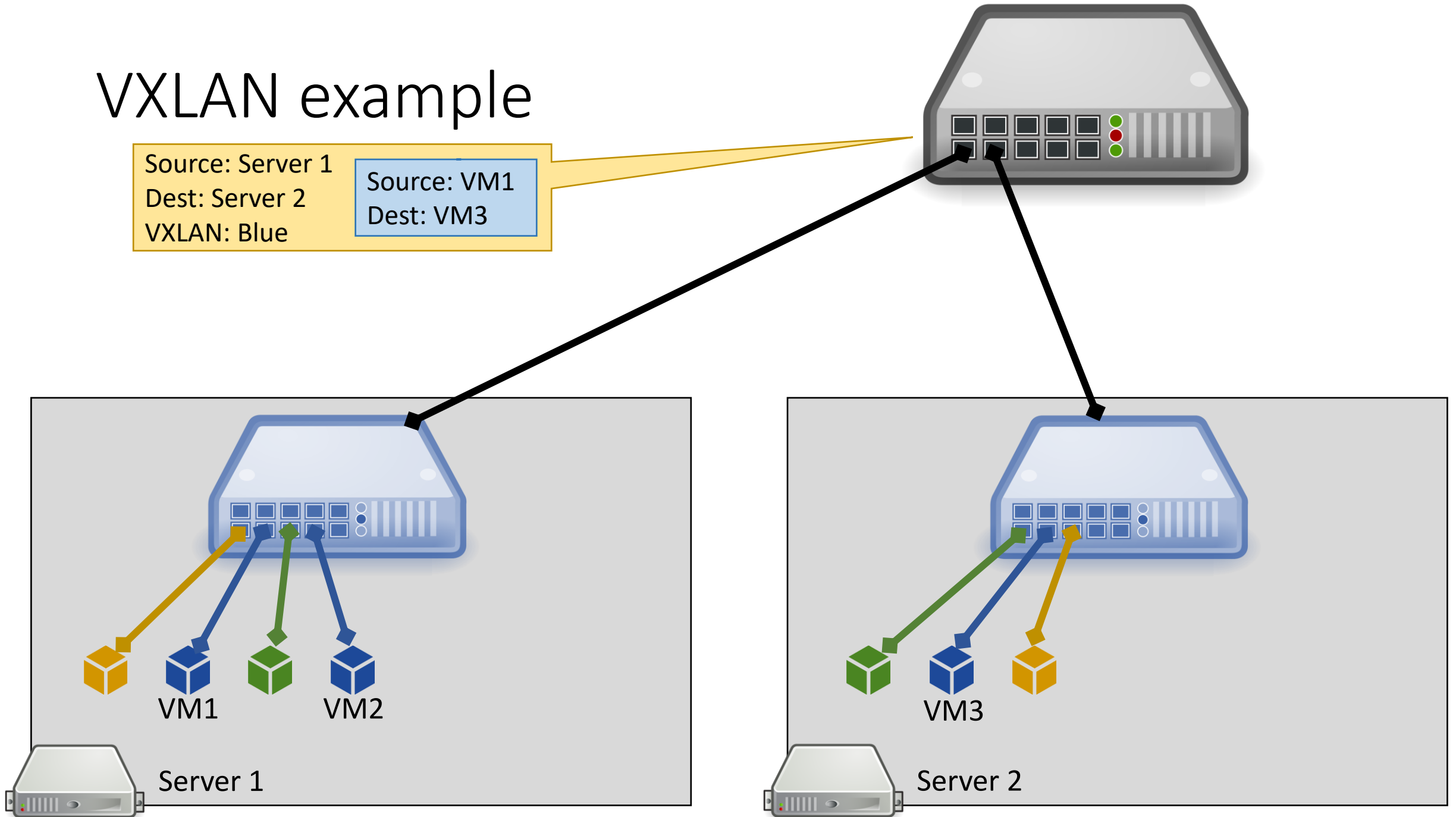
Source: VM1
Dest: VM3



VXLAN example

Source: Server 1
Dest: Server 2
VXLAN: Blue

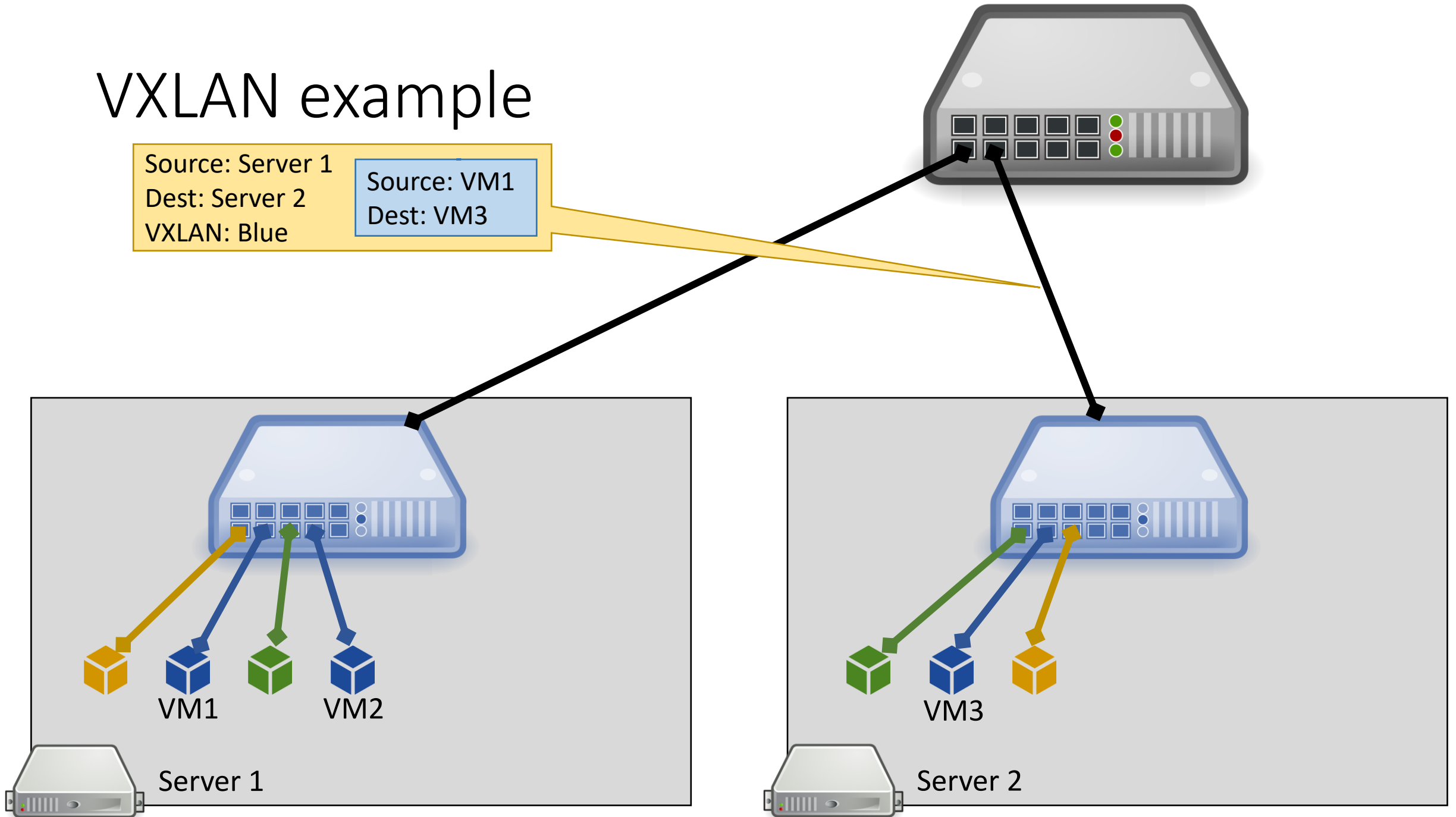
Source: VM1
Dest: VM3



VXLAN example

Source: Server 1
Dest: Server 2
VXLAN: Blue

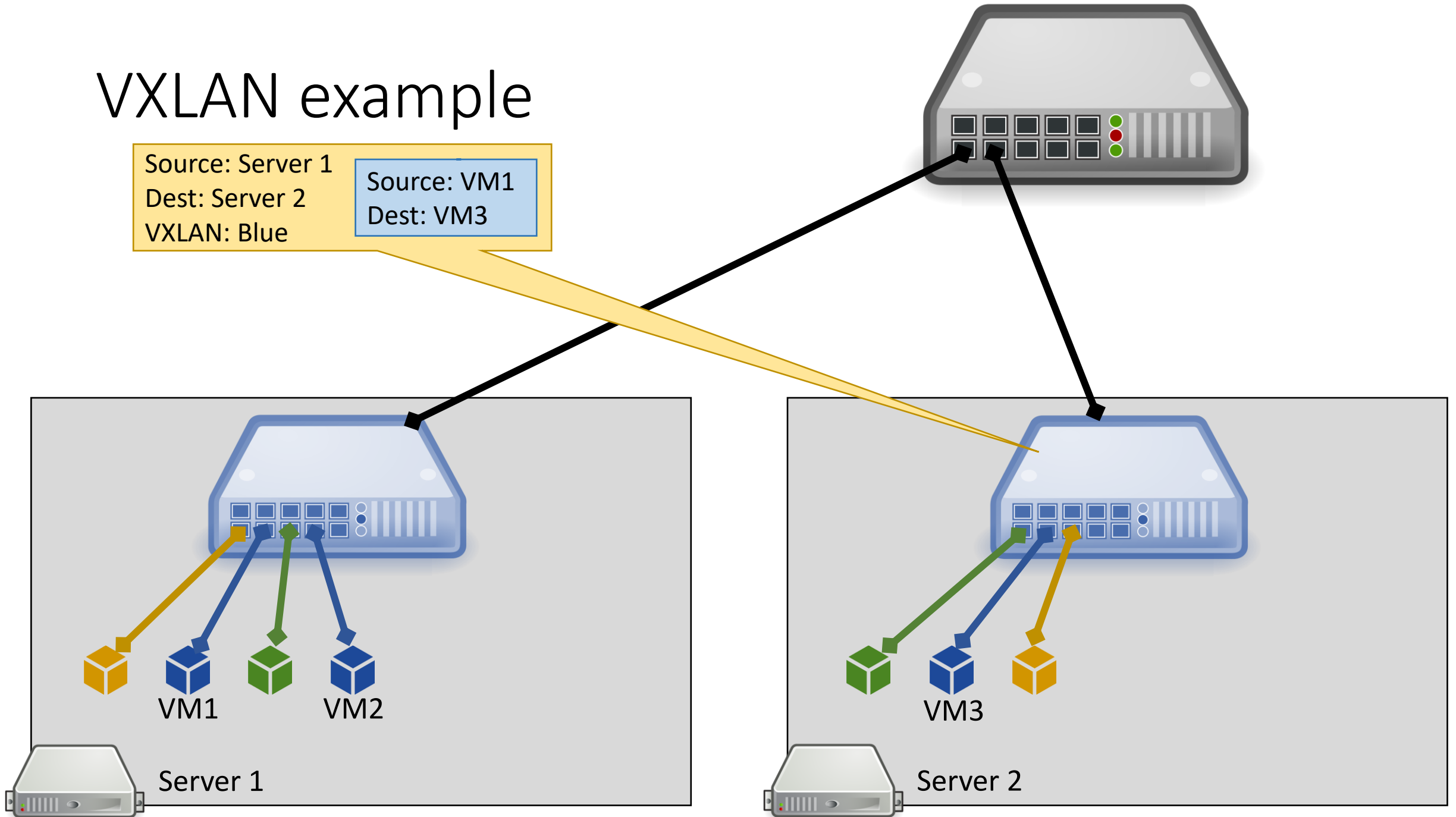
Source: VM1
Dest: VM3



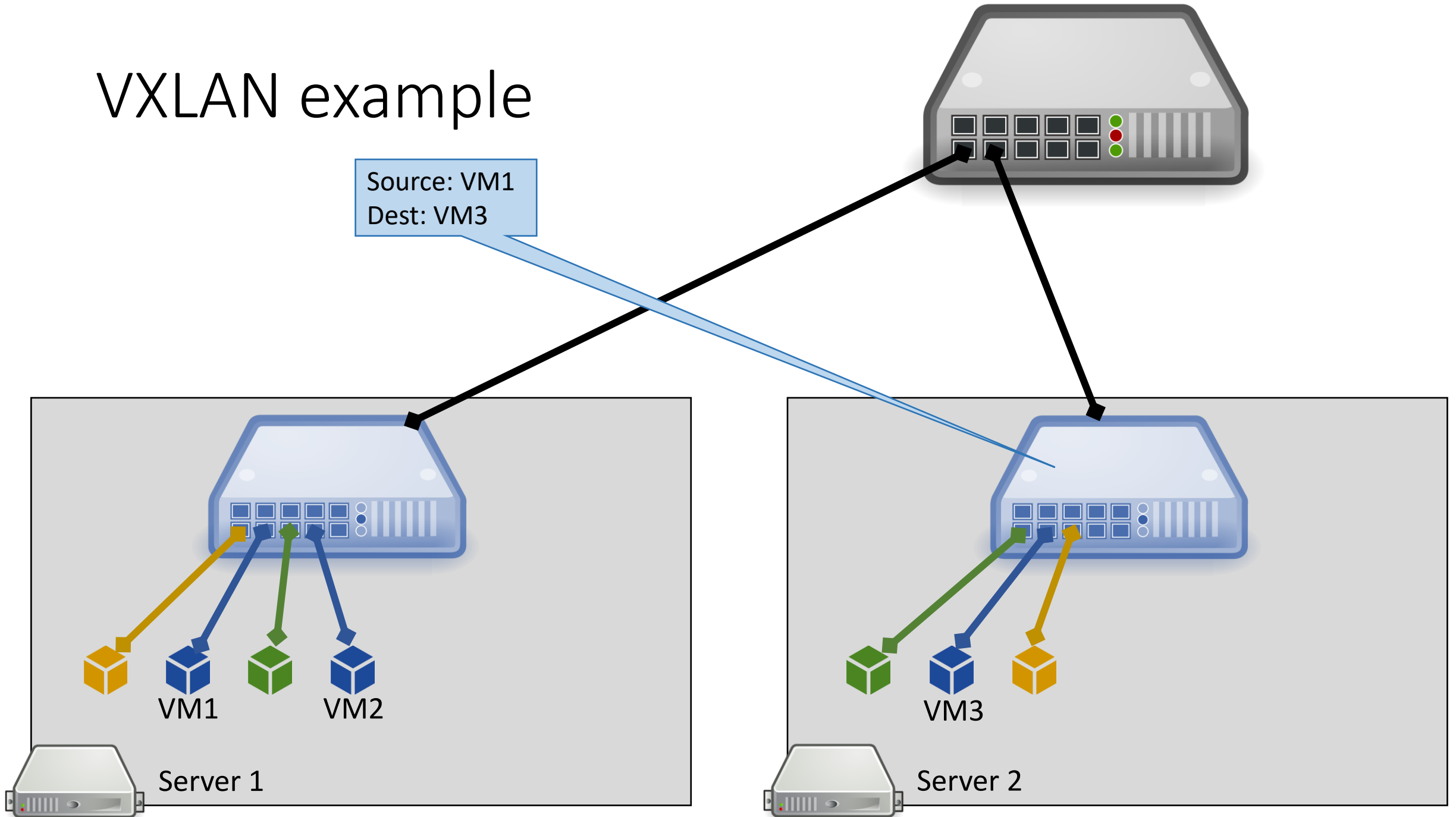
VXLAN example

Source: Server 1
Dest: Server 2
VXLAN: Blue

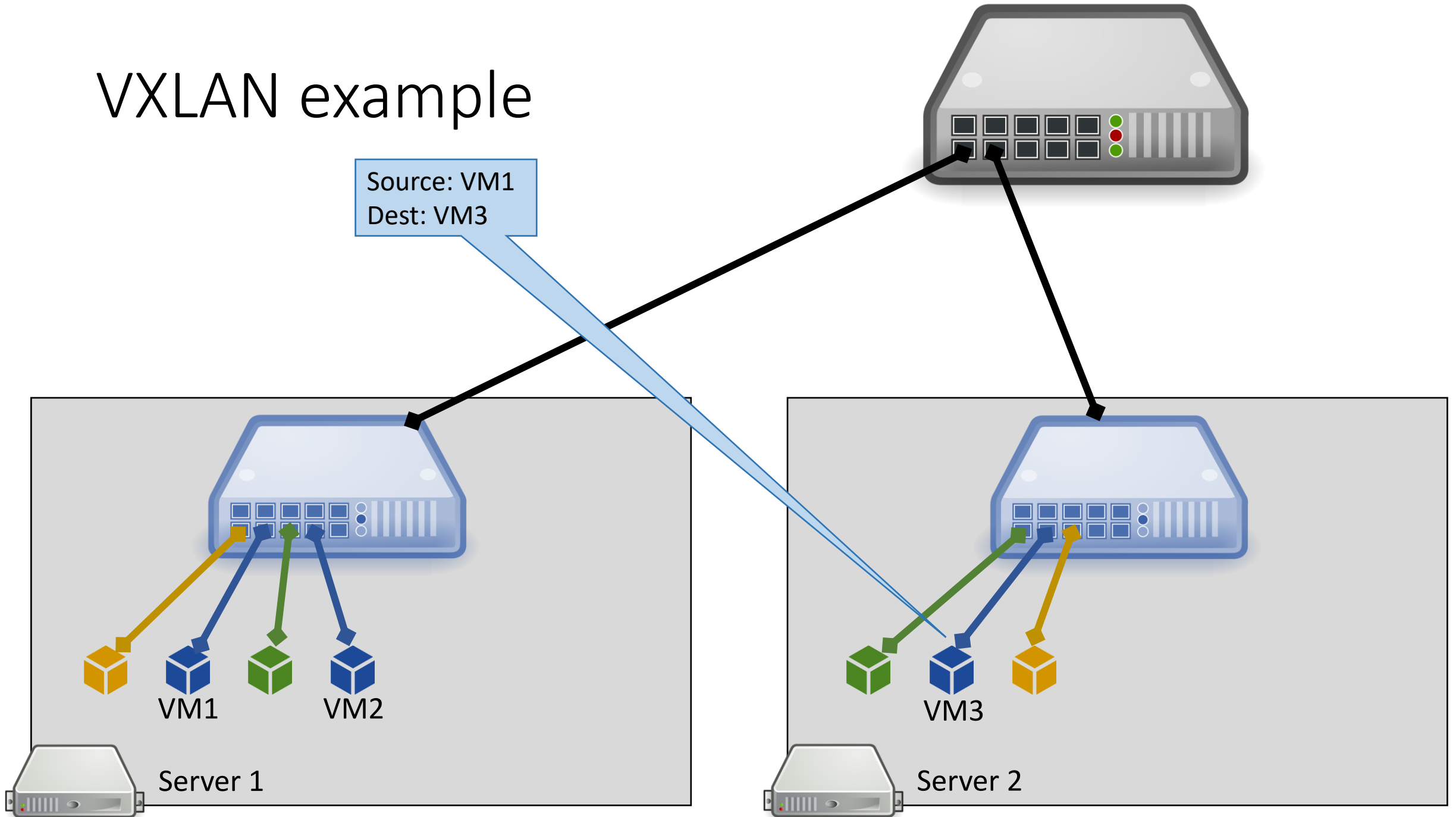
Source: VM1
Dest: VM3



VXLAN example



VXLAN example





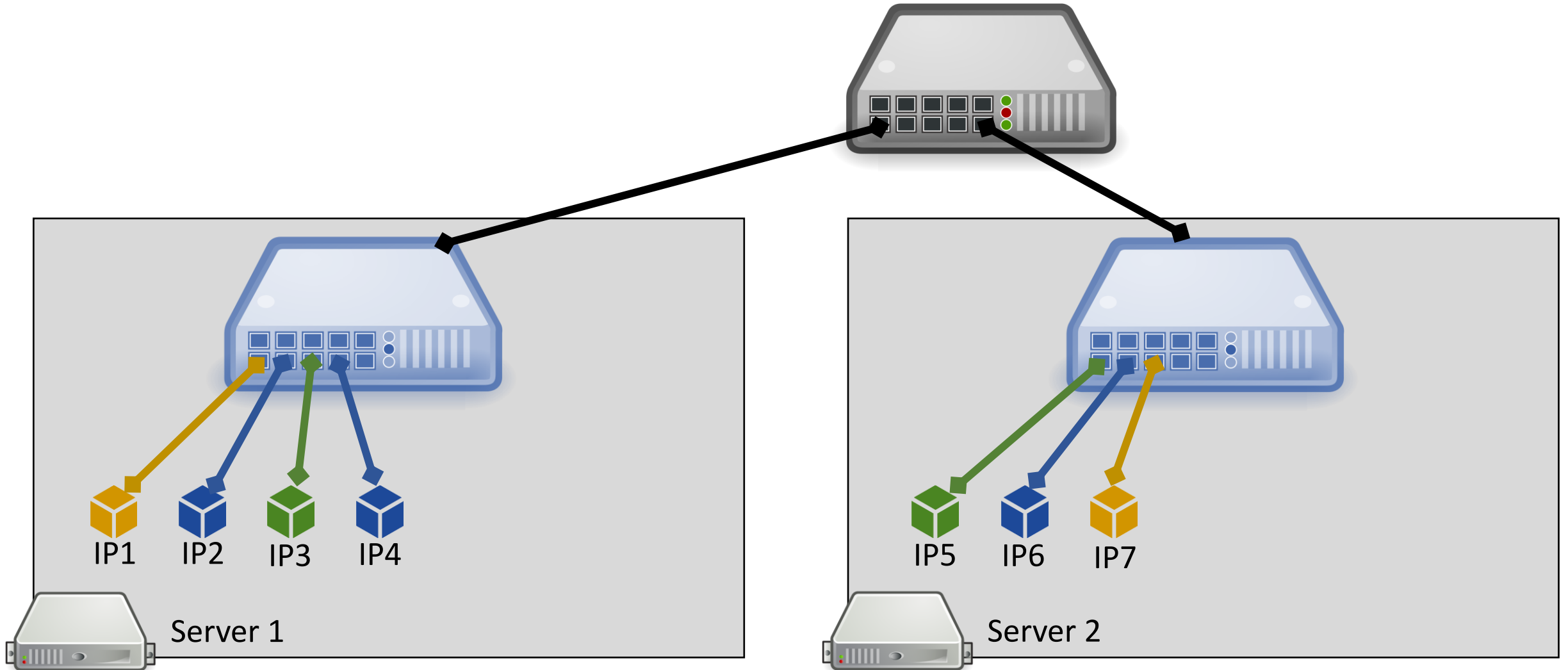
CompSci 401: Cloud Computing

Network Address Translation

Prof. Ítalo Cunha

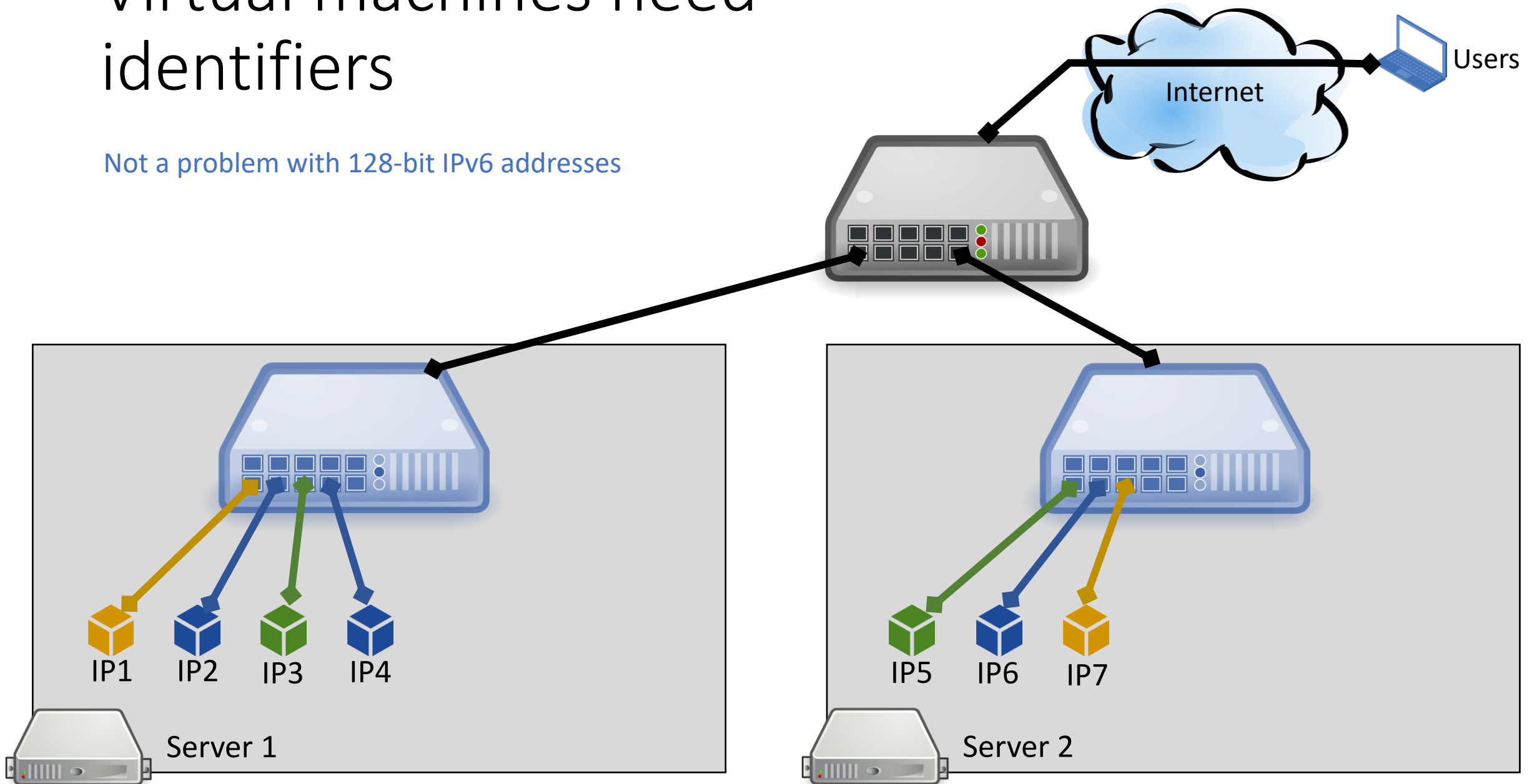


Virtual machines need identifiers



Virtual machines need identifiers

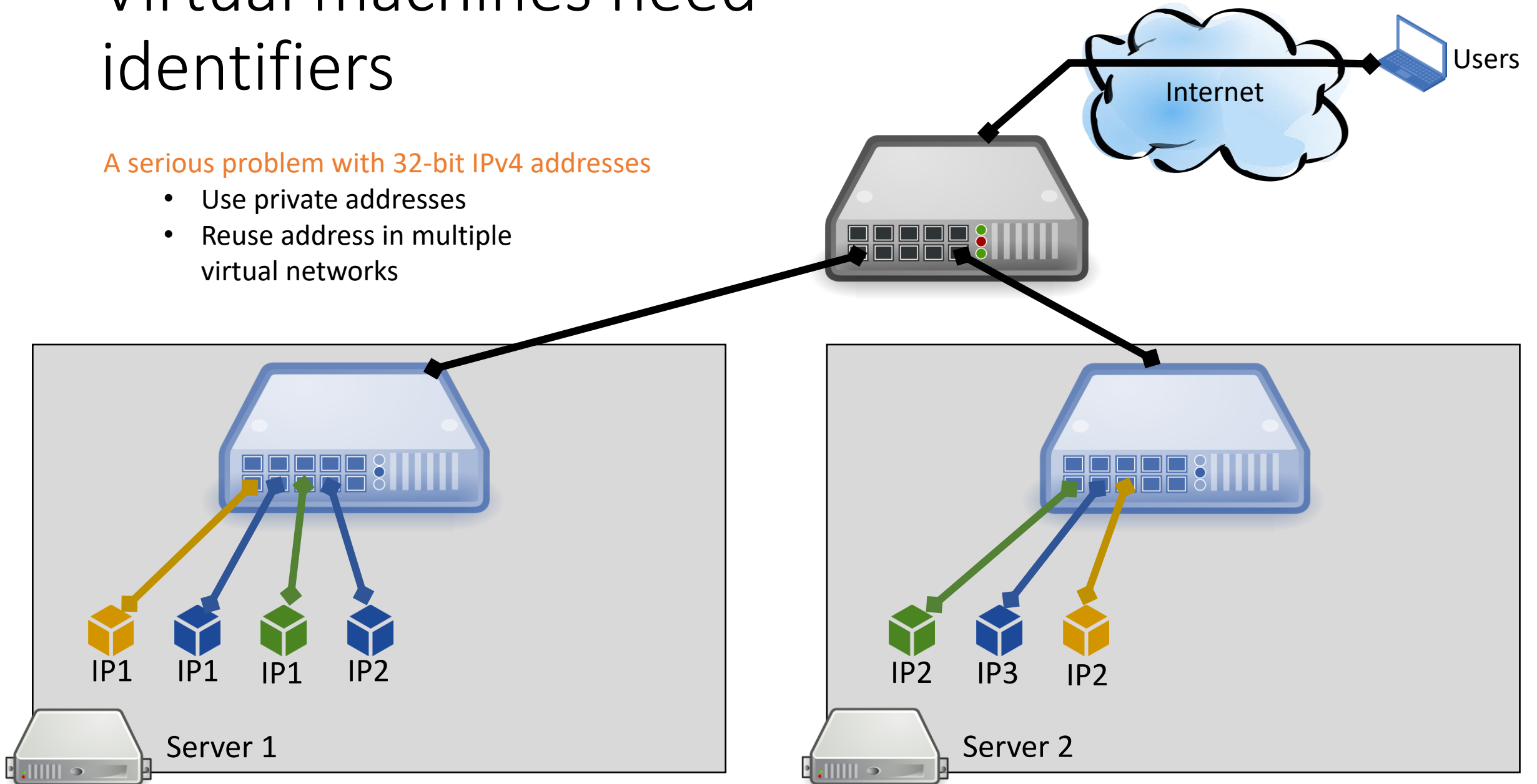
Not a problem with 128-bit IPv6 addresses



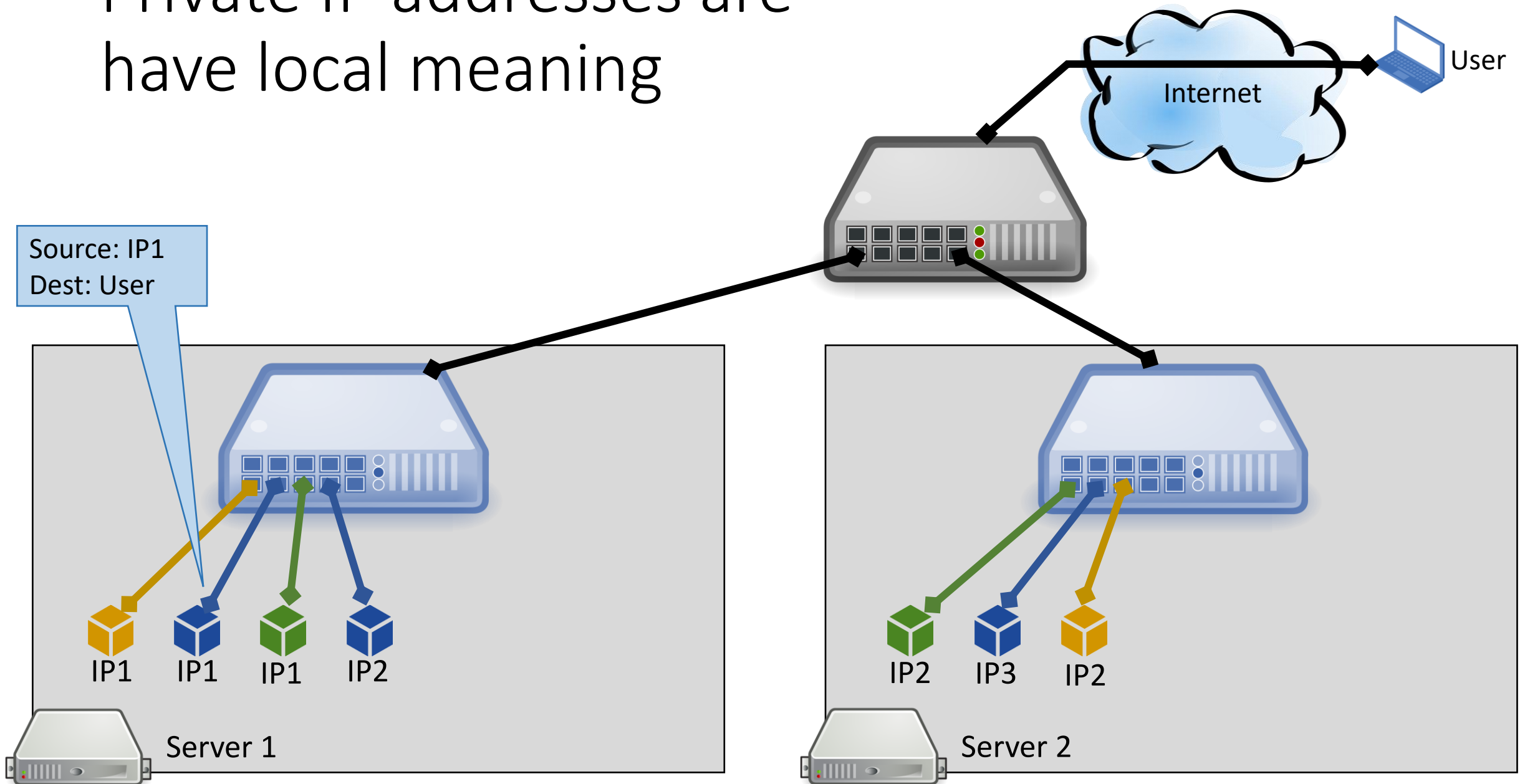
Virtual machines need identifiers

A serious problem with 32-bit IPv4 addresses

- Use private addresses
- Reuse address in multiple virtual networks

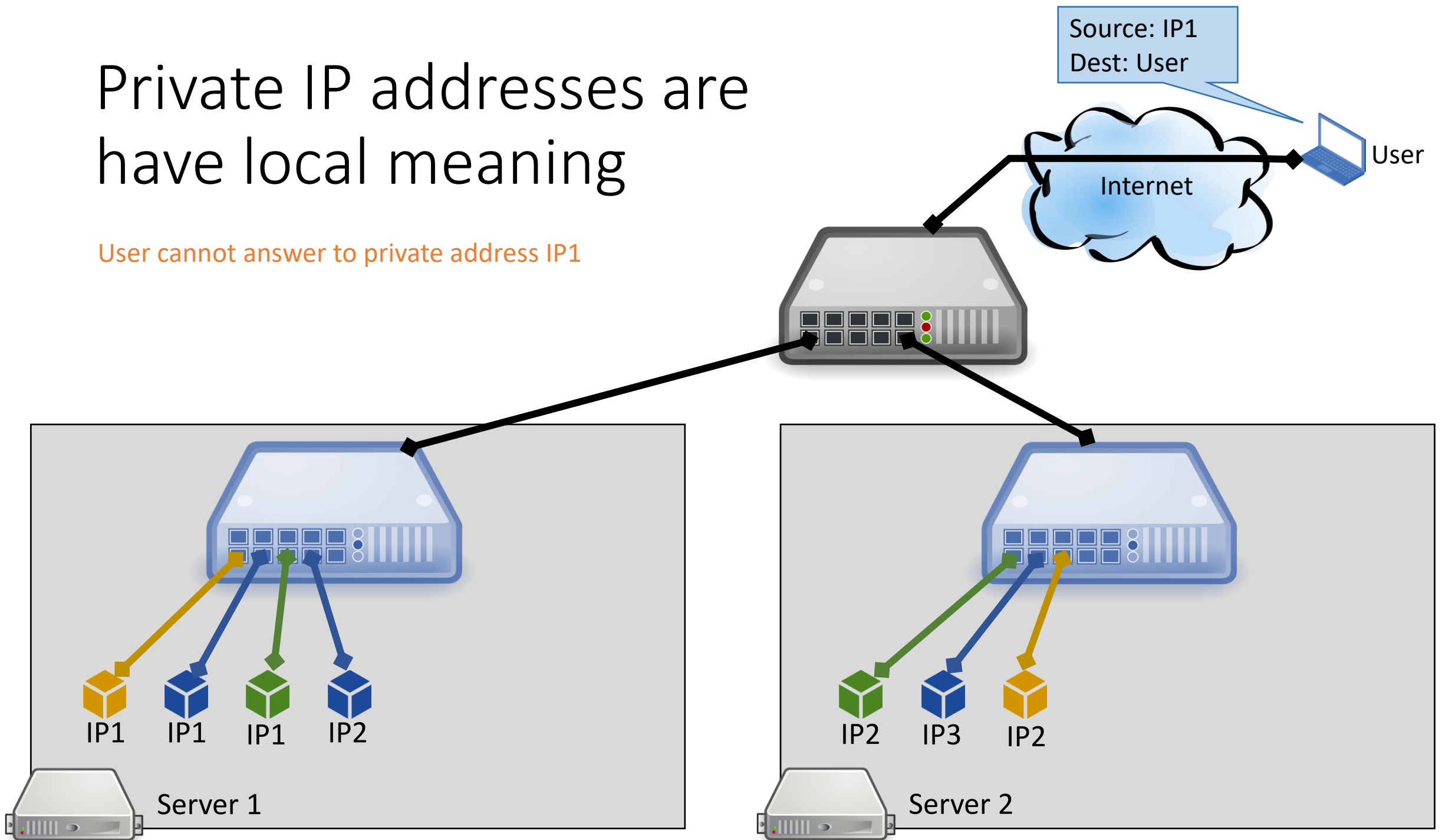


Private IP addresses are have local meaning

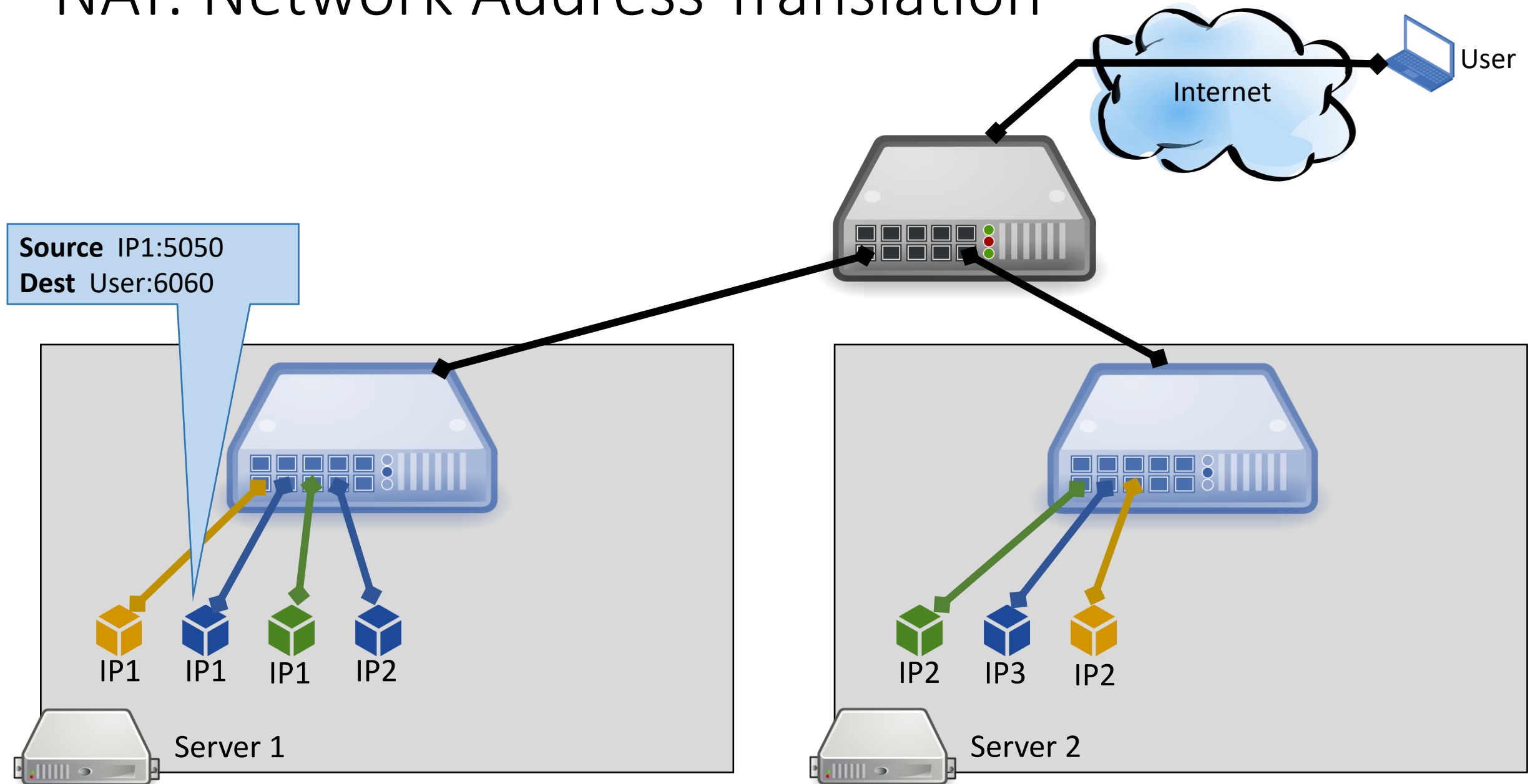


Private IP addresses are have local meaning

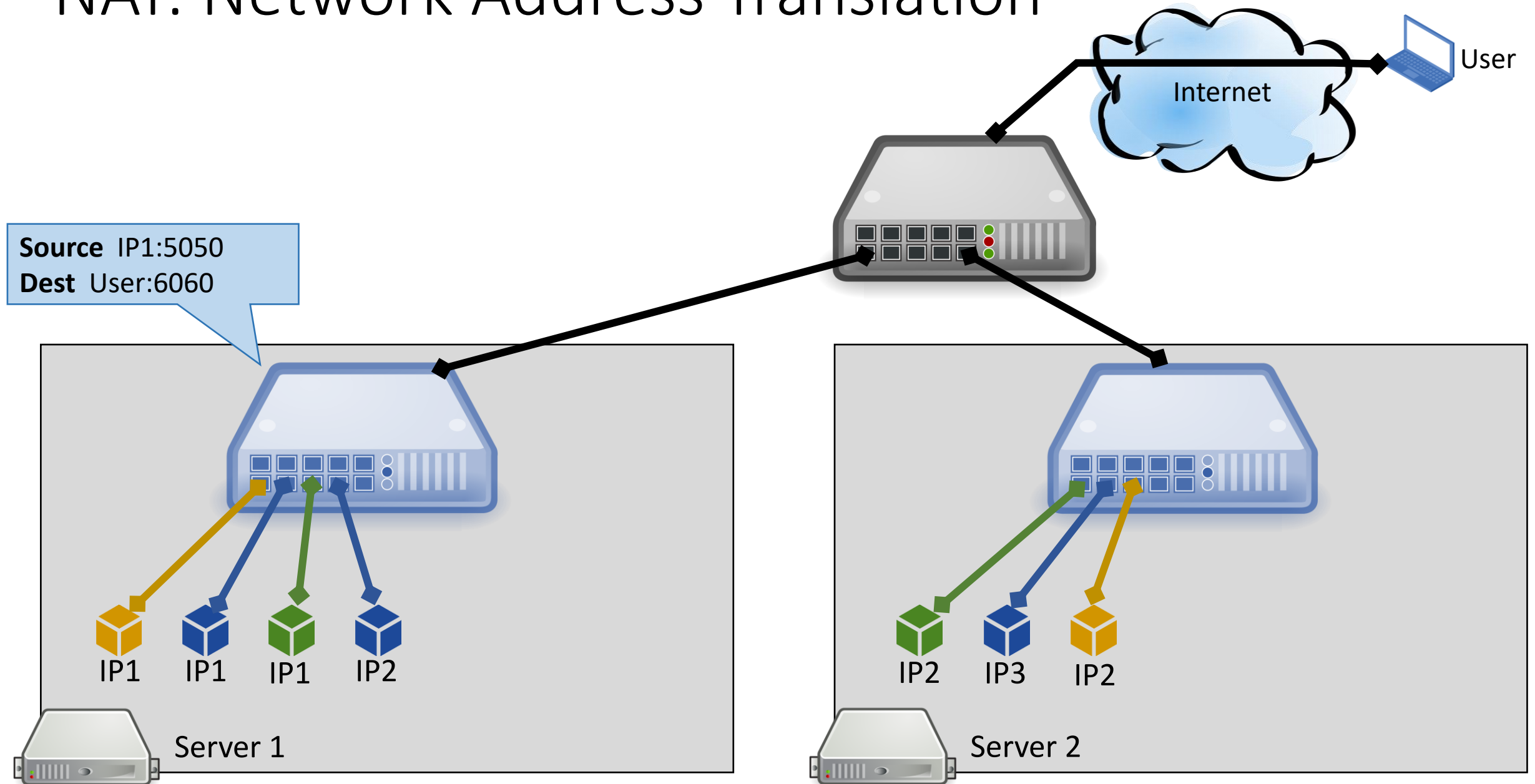
User cannot answer to private address IP1



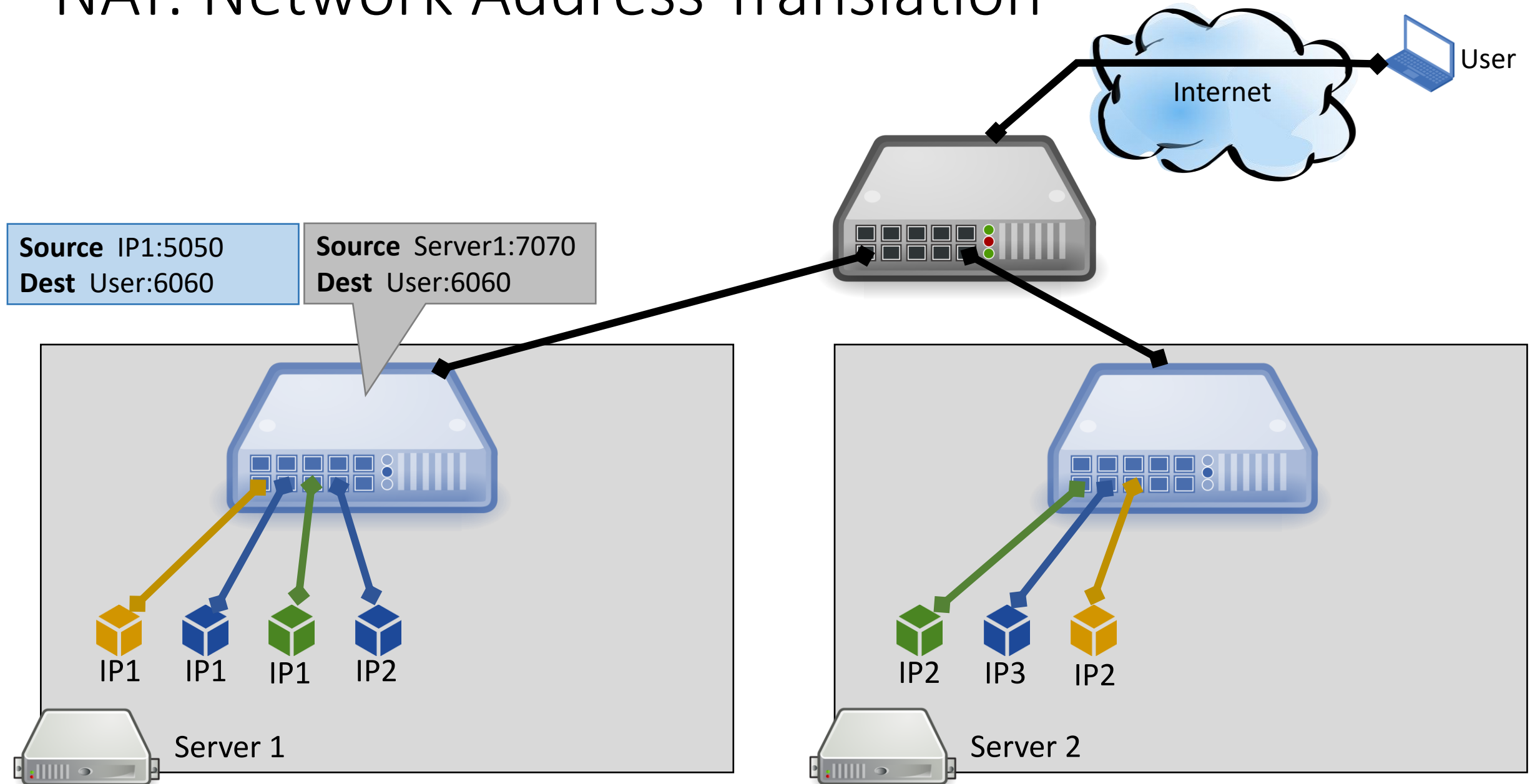
NAT: Network Address Translation



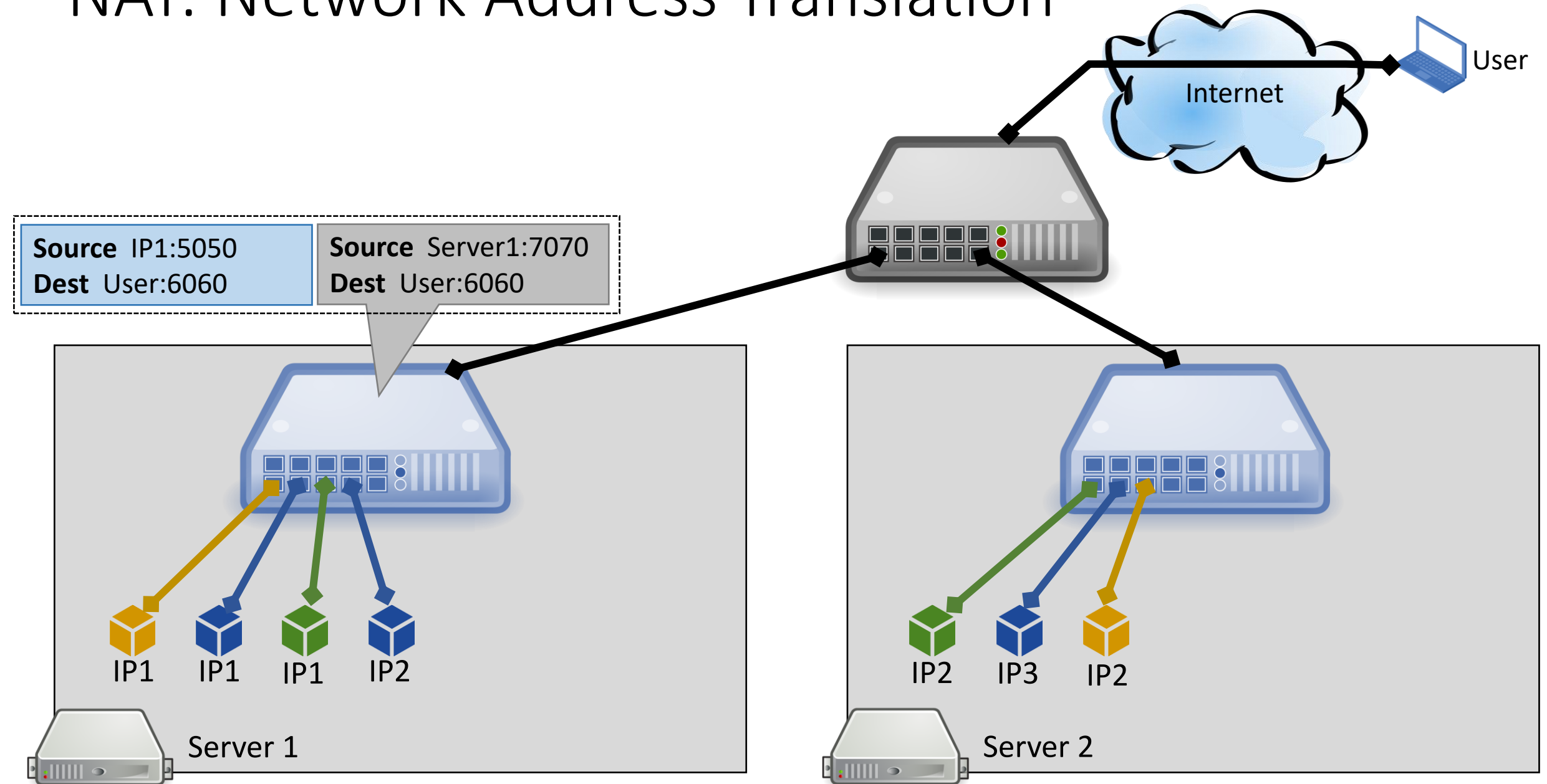
NAT: Network Address Translation



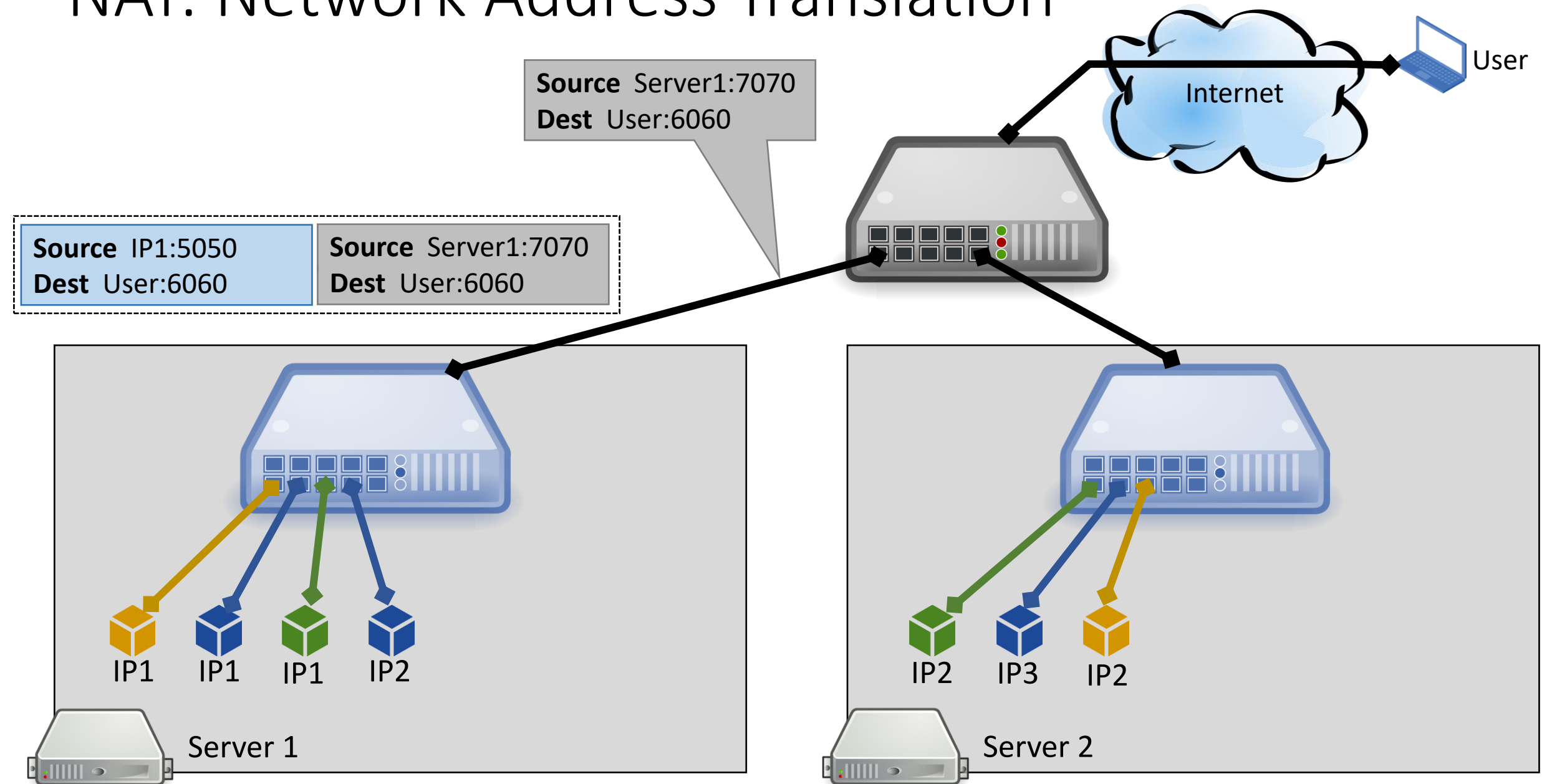
NAT: Network Address Translation



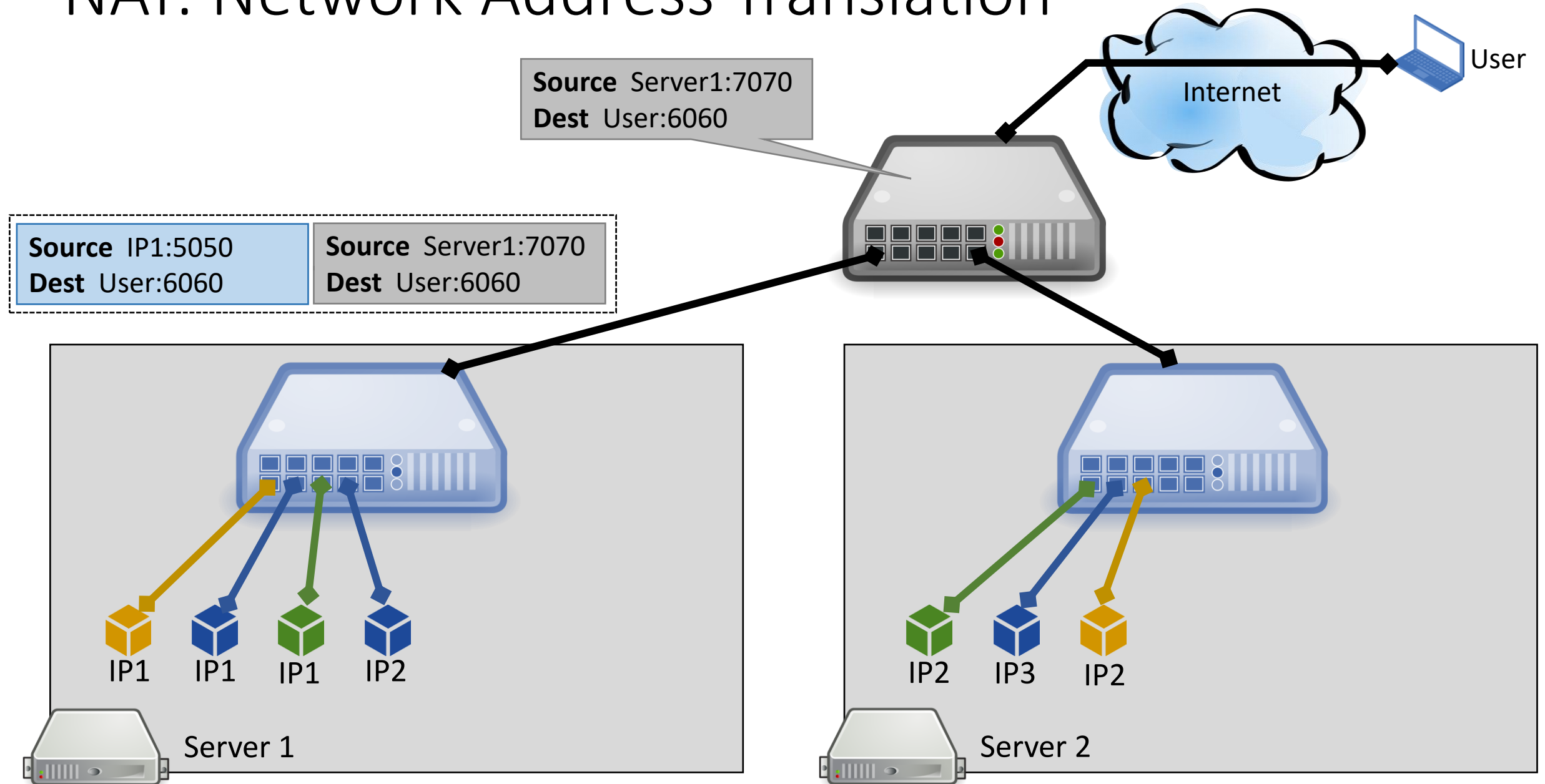
NAT: Network Address Translation



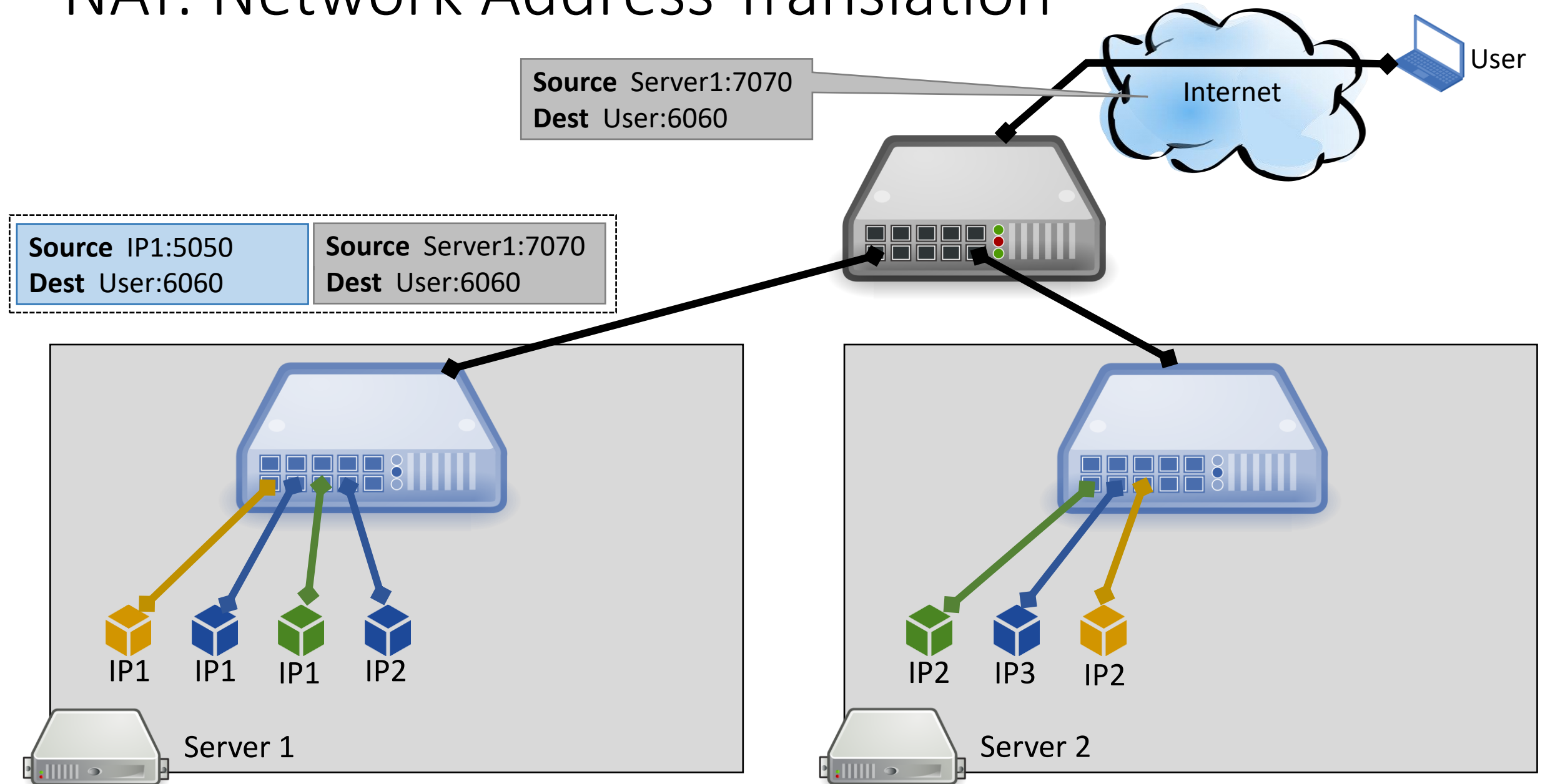
NAT: Network Address Translation



NAT: Network Address Translation

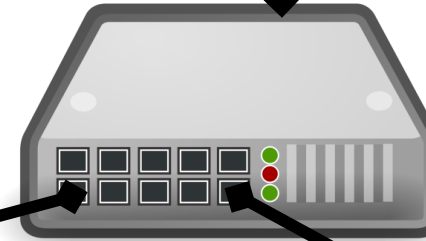
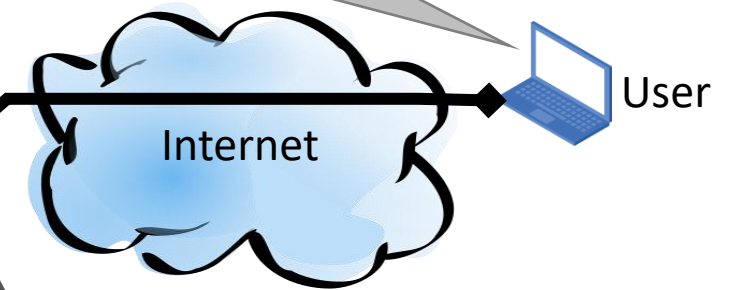


NAT: Network Address Translation



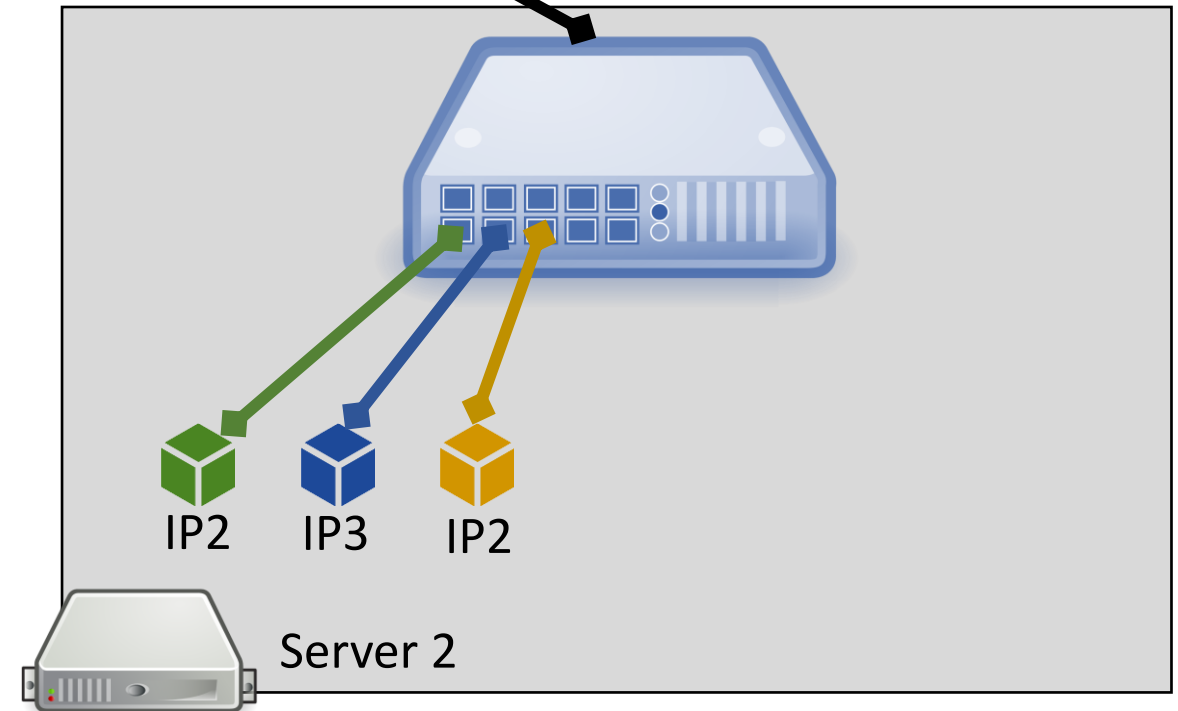
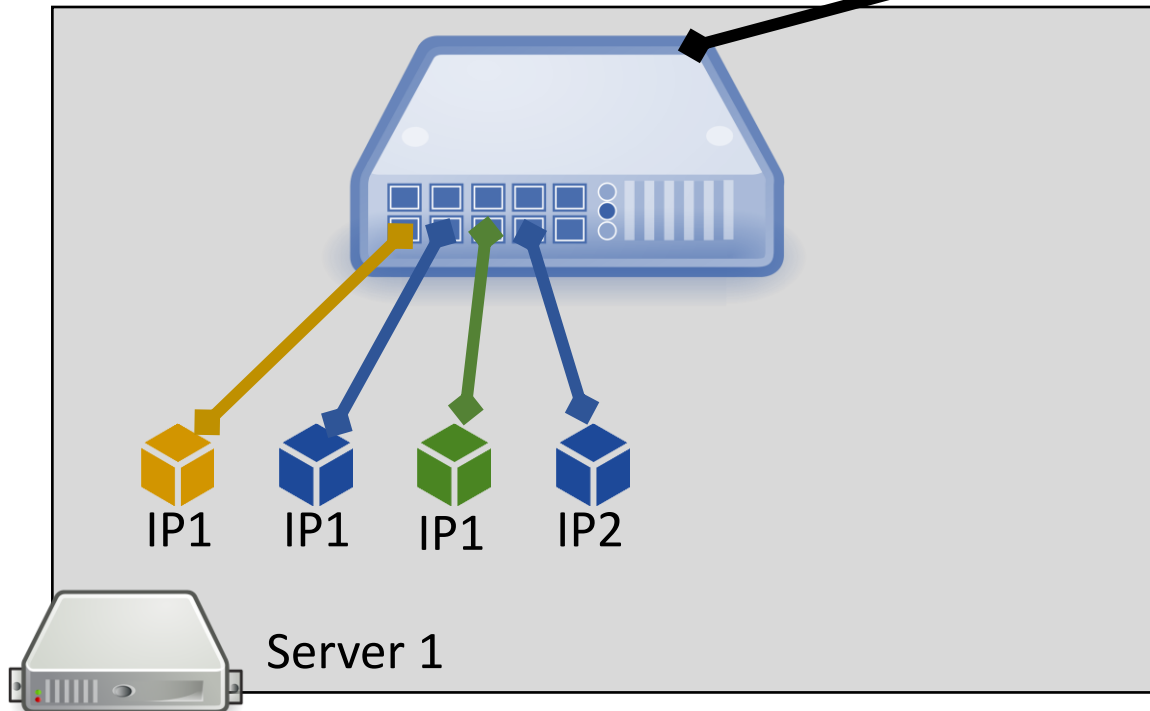
NAT: Network Address Translation

Source Server1:7070
Dest User:6060



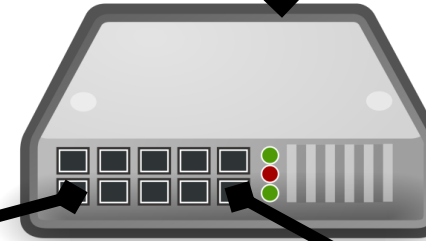
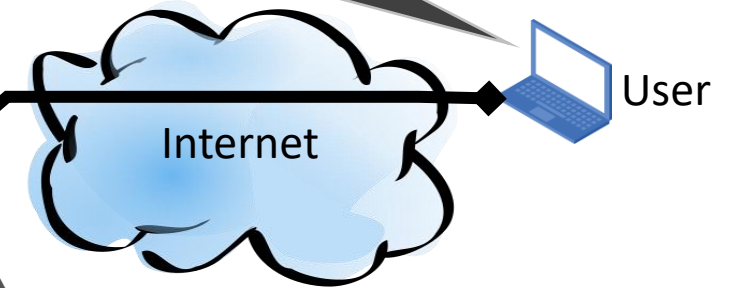
Source IP1:5050
Dest User:6060

Source Server1:7070
Dest User:6060



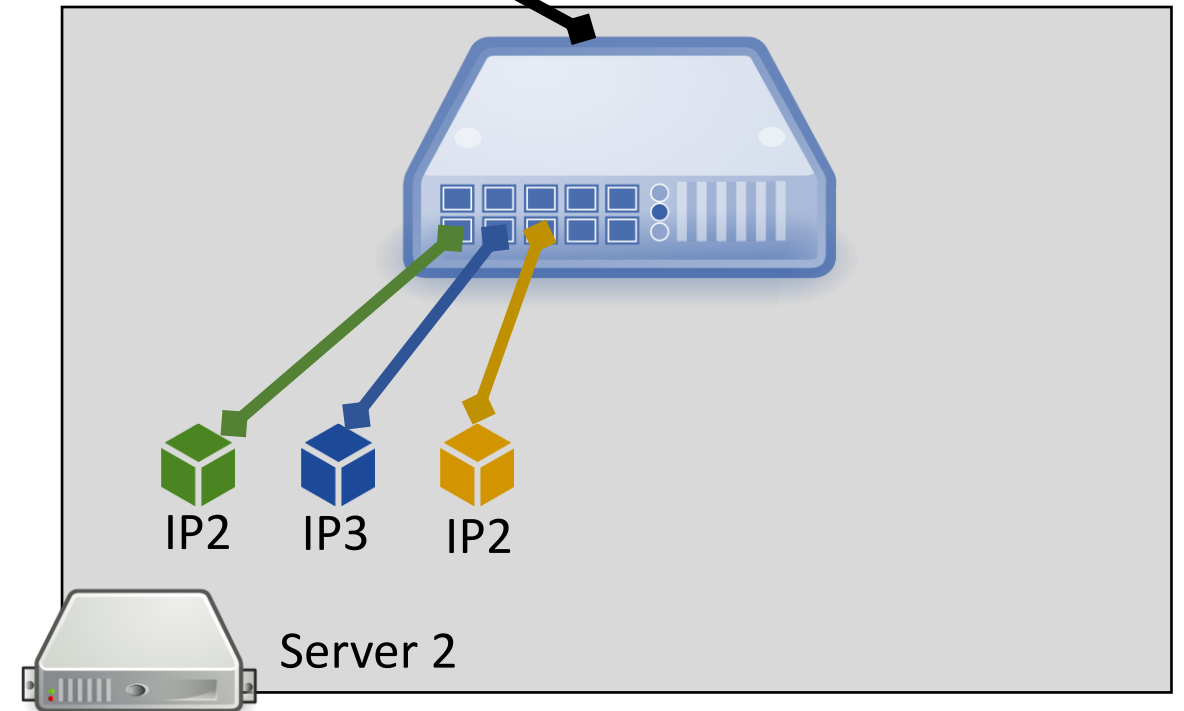
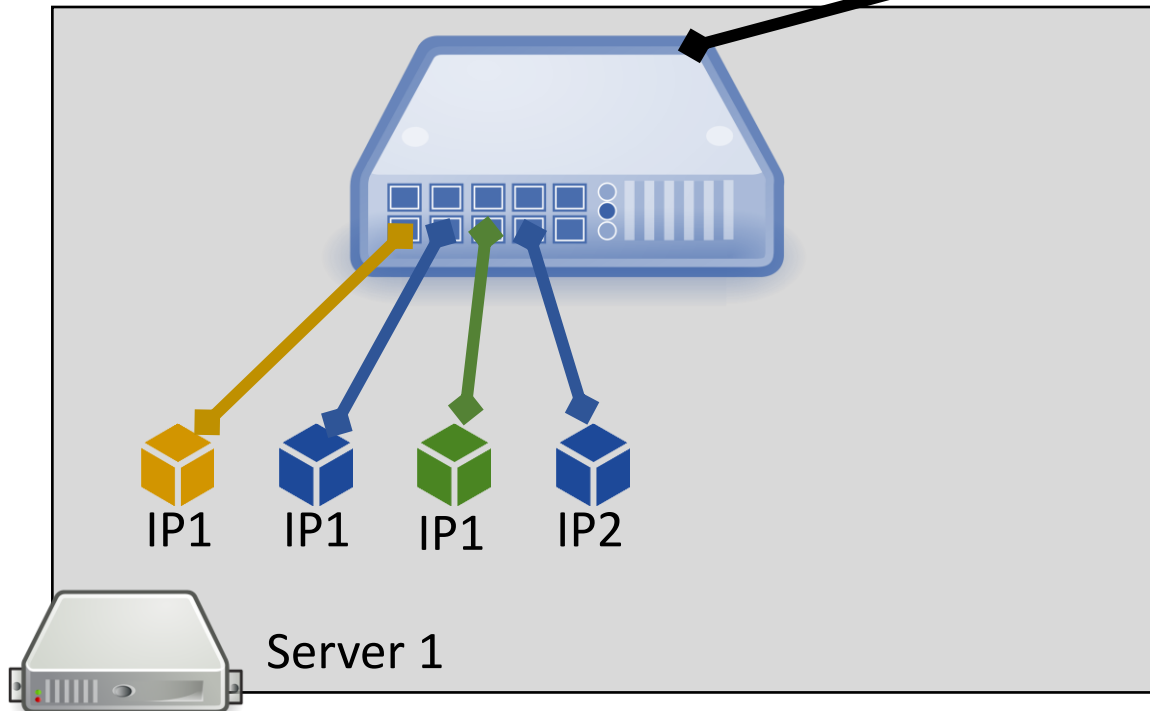
NAT: Network Address Translation

Dest Server1:7070
Source User:6060



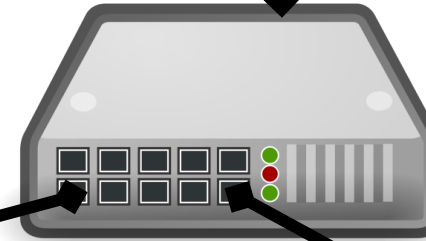
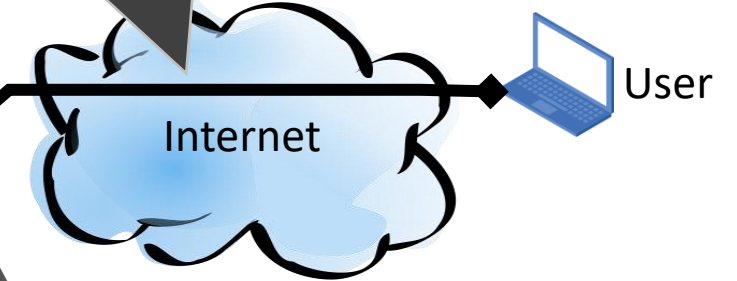
Source IP1:5050
Dest User:6060

Source Server1:7070
Dest User:6060



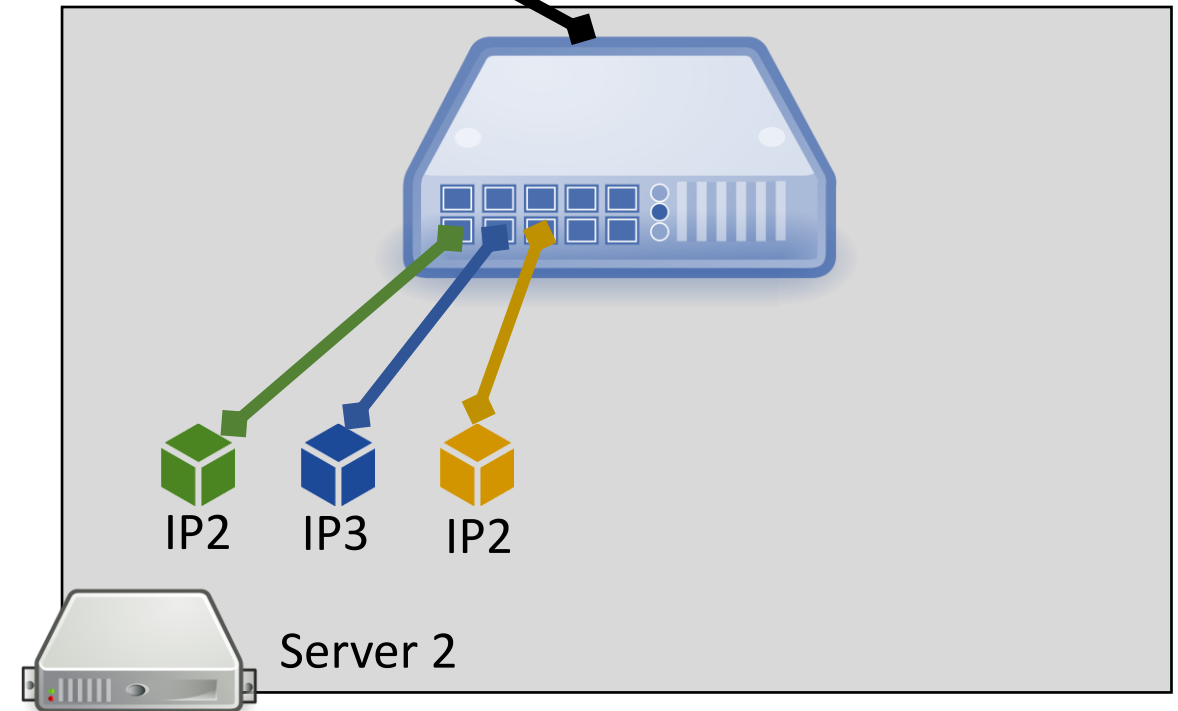
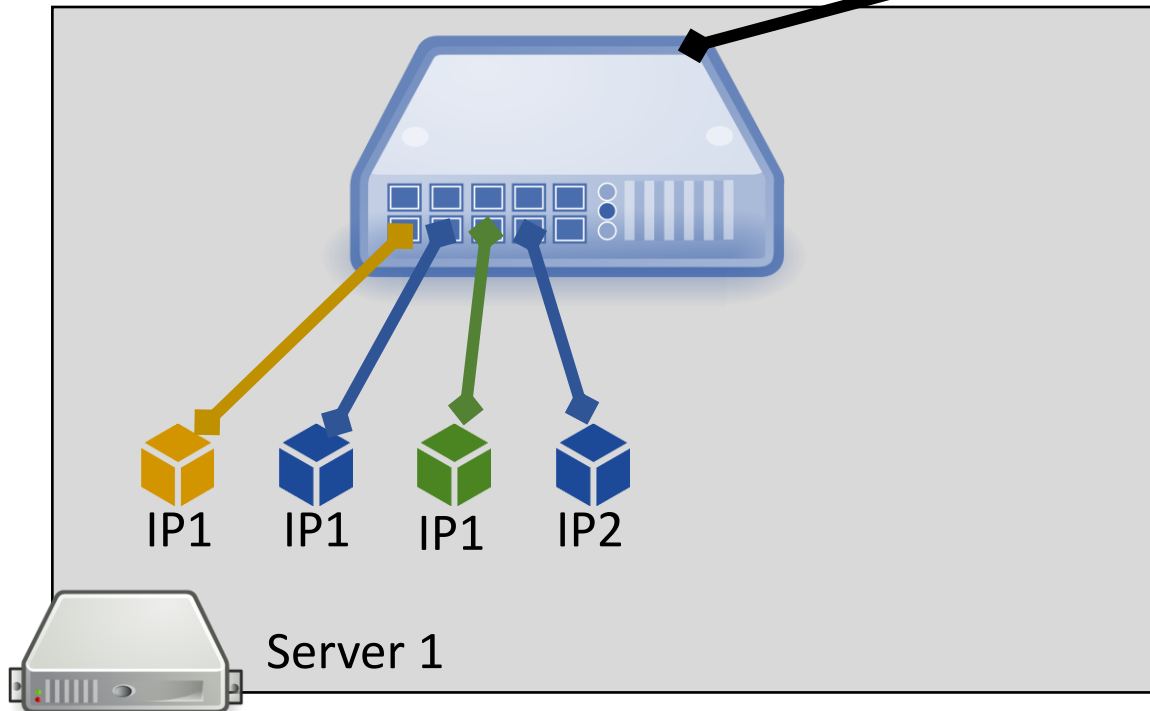
NAT: Network Address Translation

Dest Server1:7070
Source User:6060

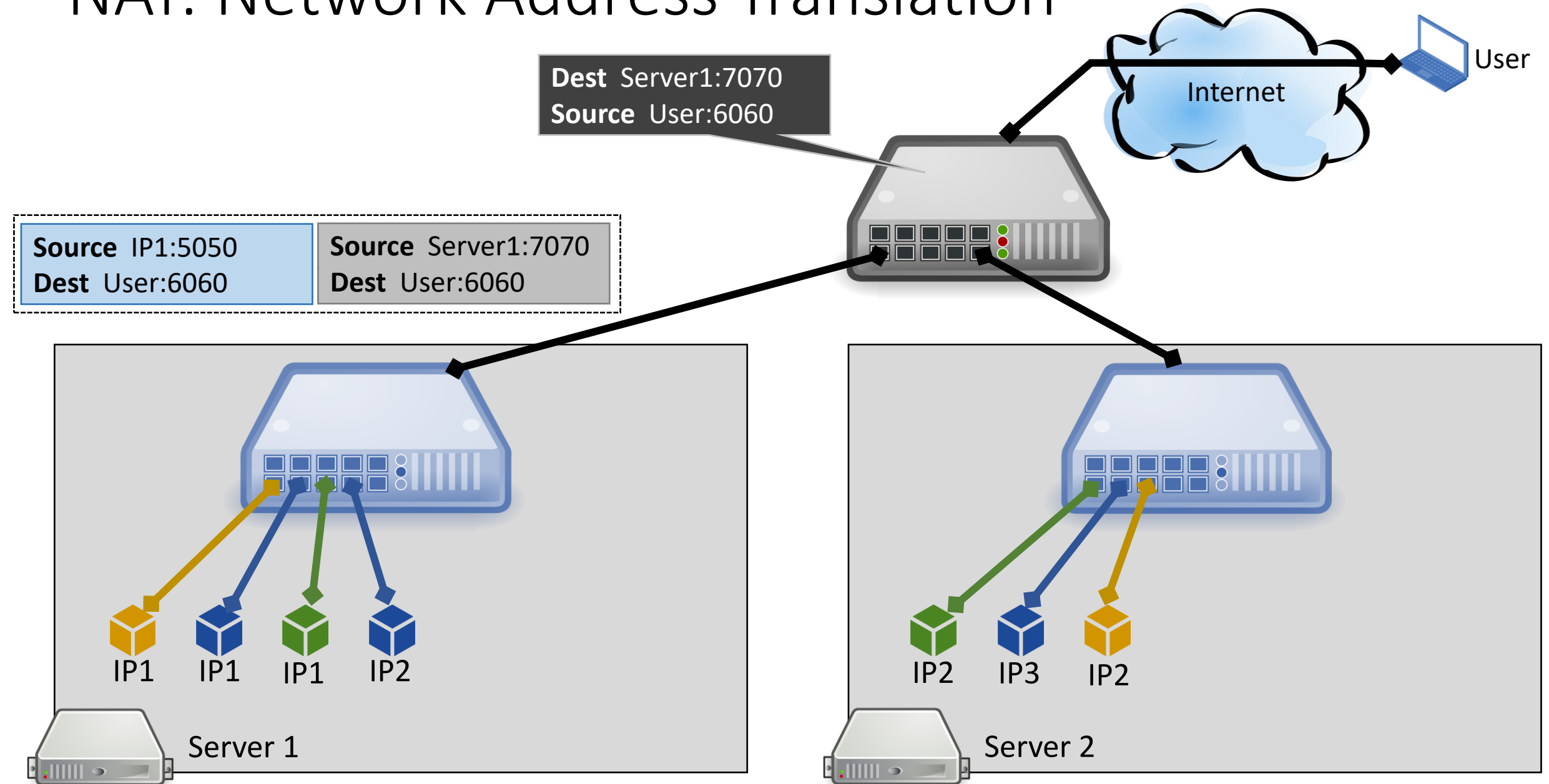


Source IP1:5050
Dest User:6060

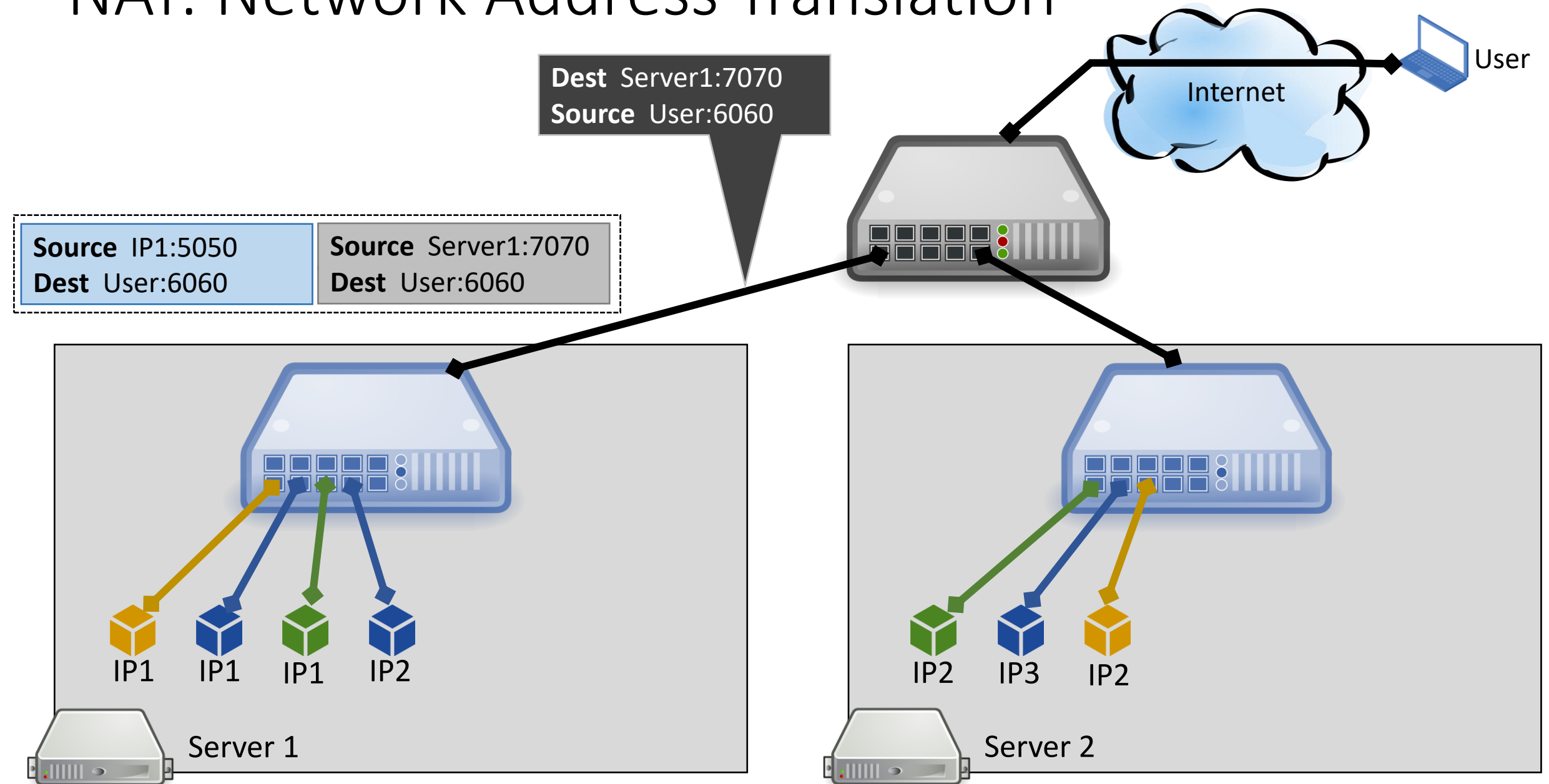
Source Server1:7070
Dest User:6060



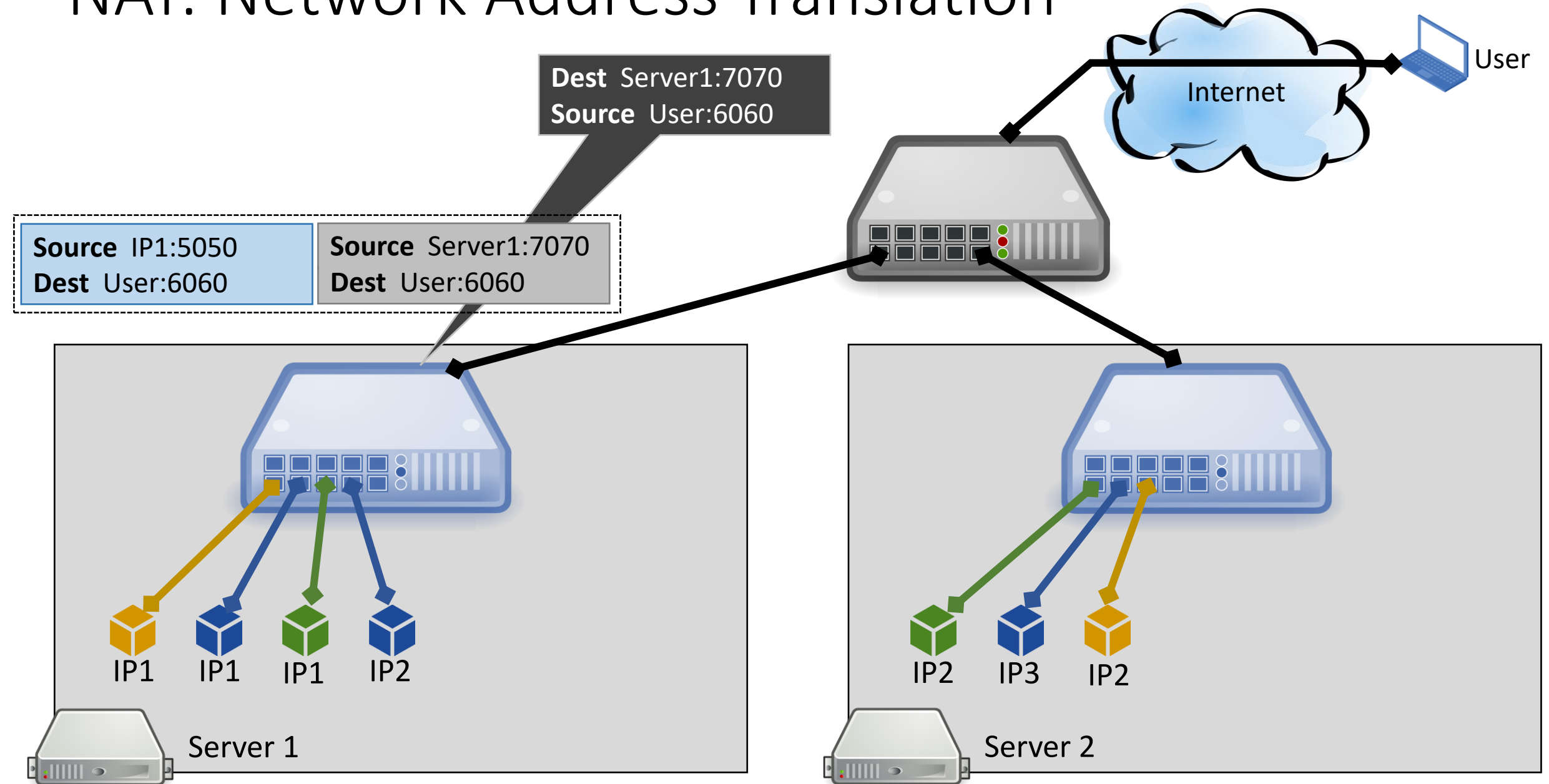
NAT: Network Address Translation



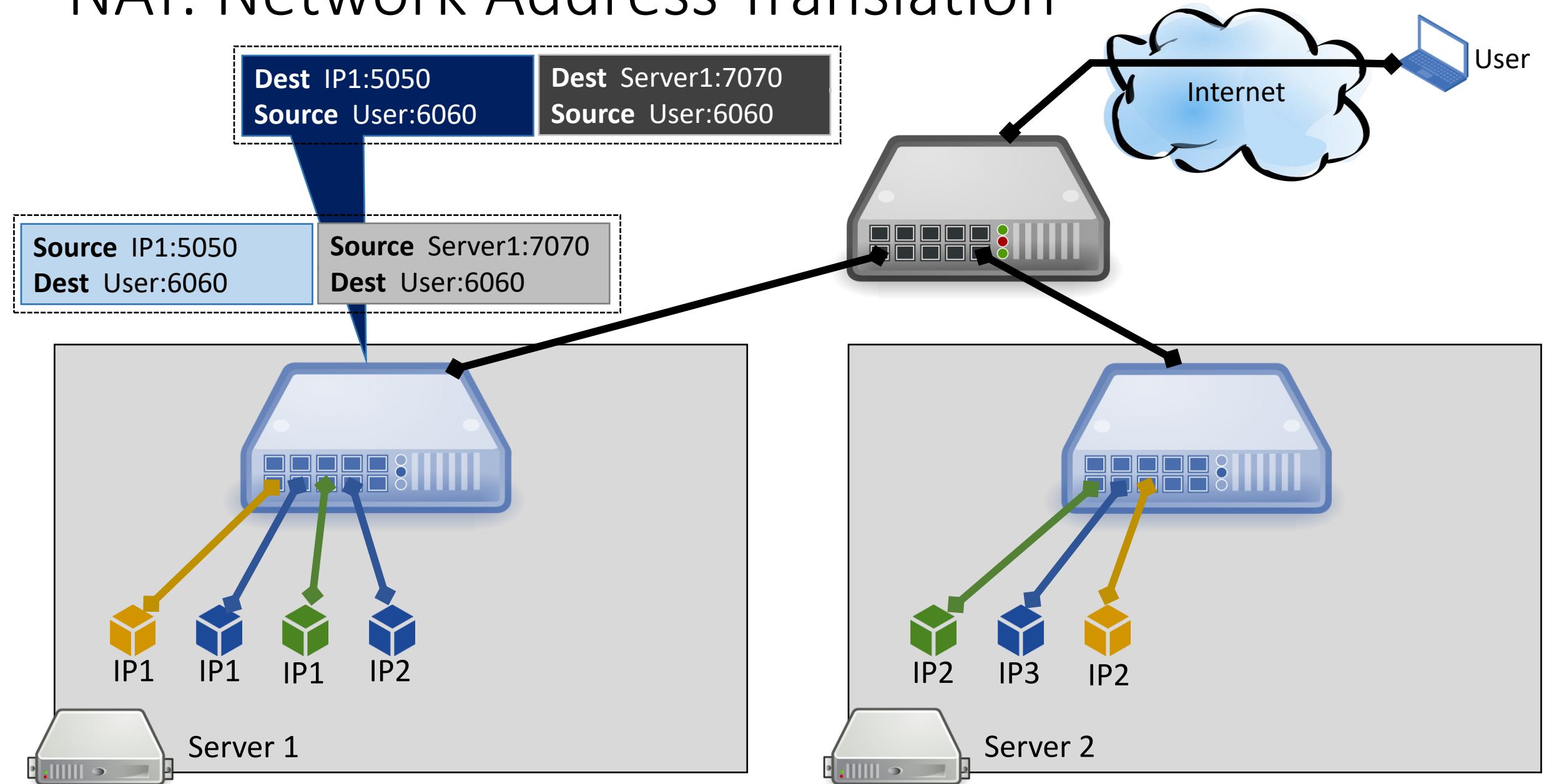
NAT: Network Address Translation



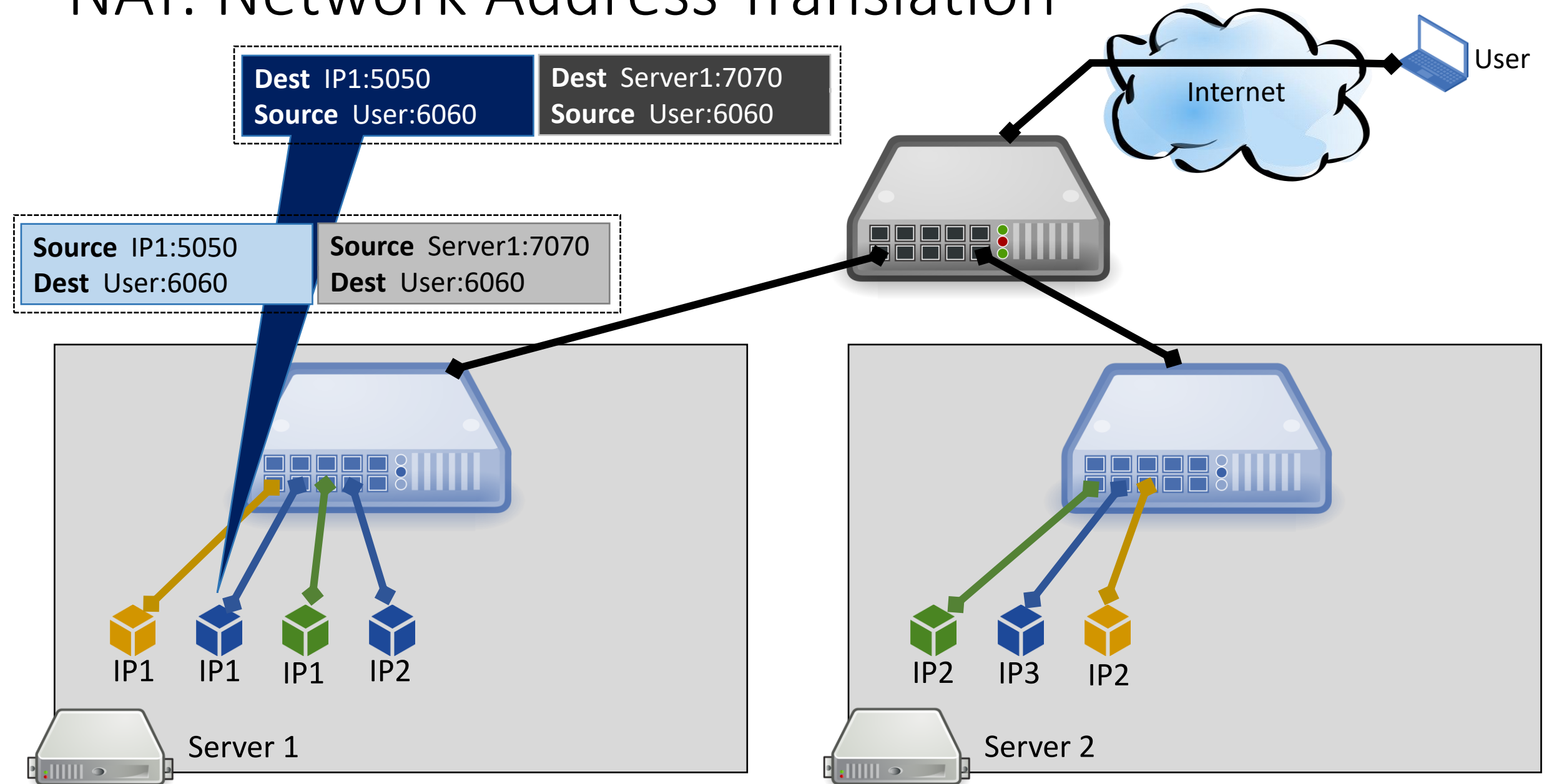
NAT: Network Address Translation



NAT: Network Address Translation



NAT: Network Address Translation





CompSci 401: Cloud Computing

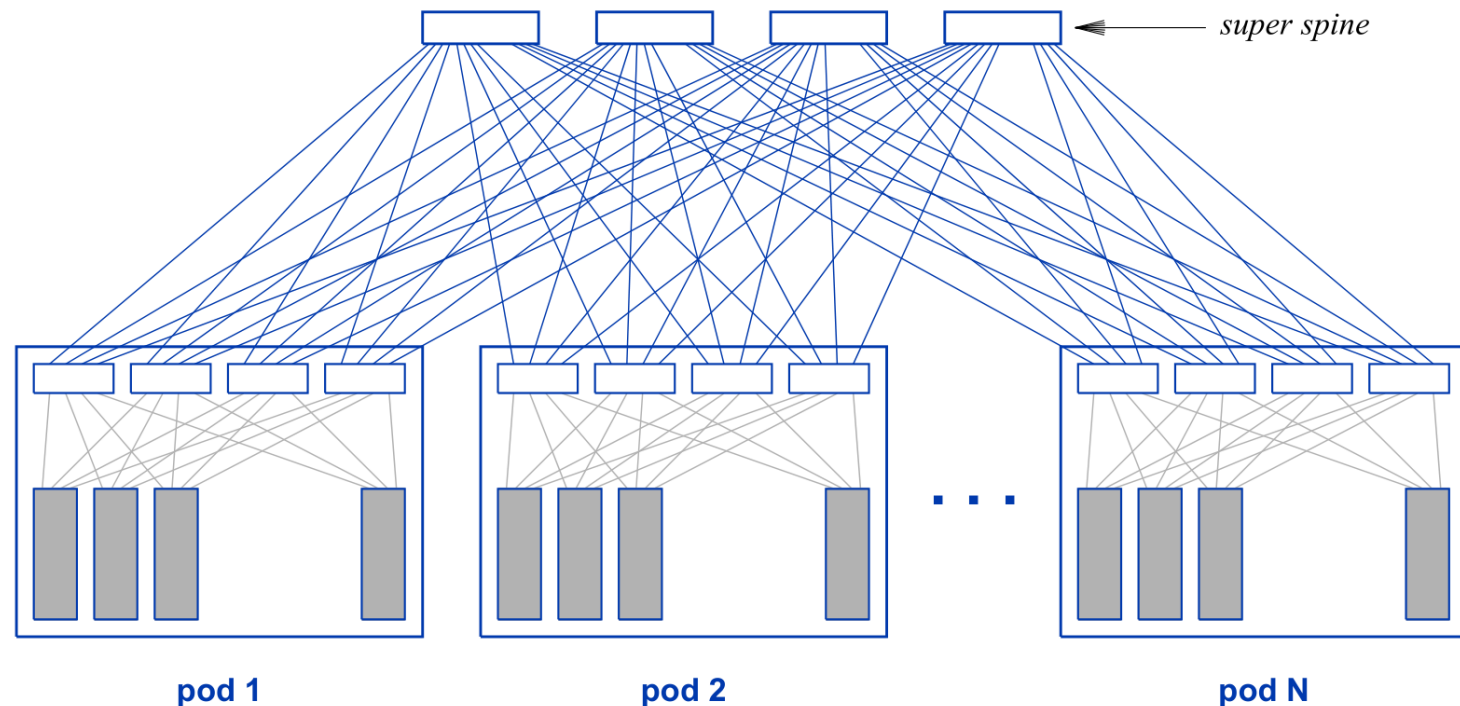
Managing Virtual Networks

Prof. Ítalo Cunha



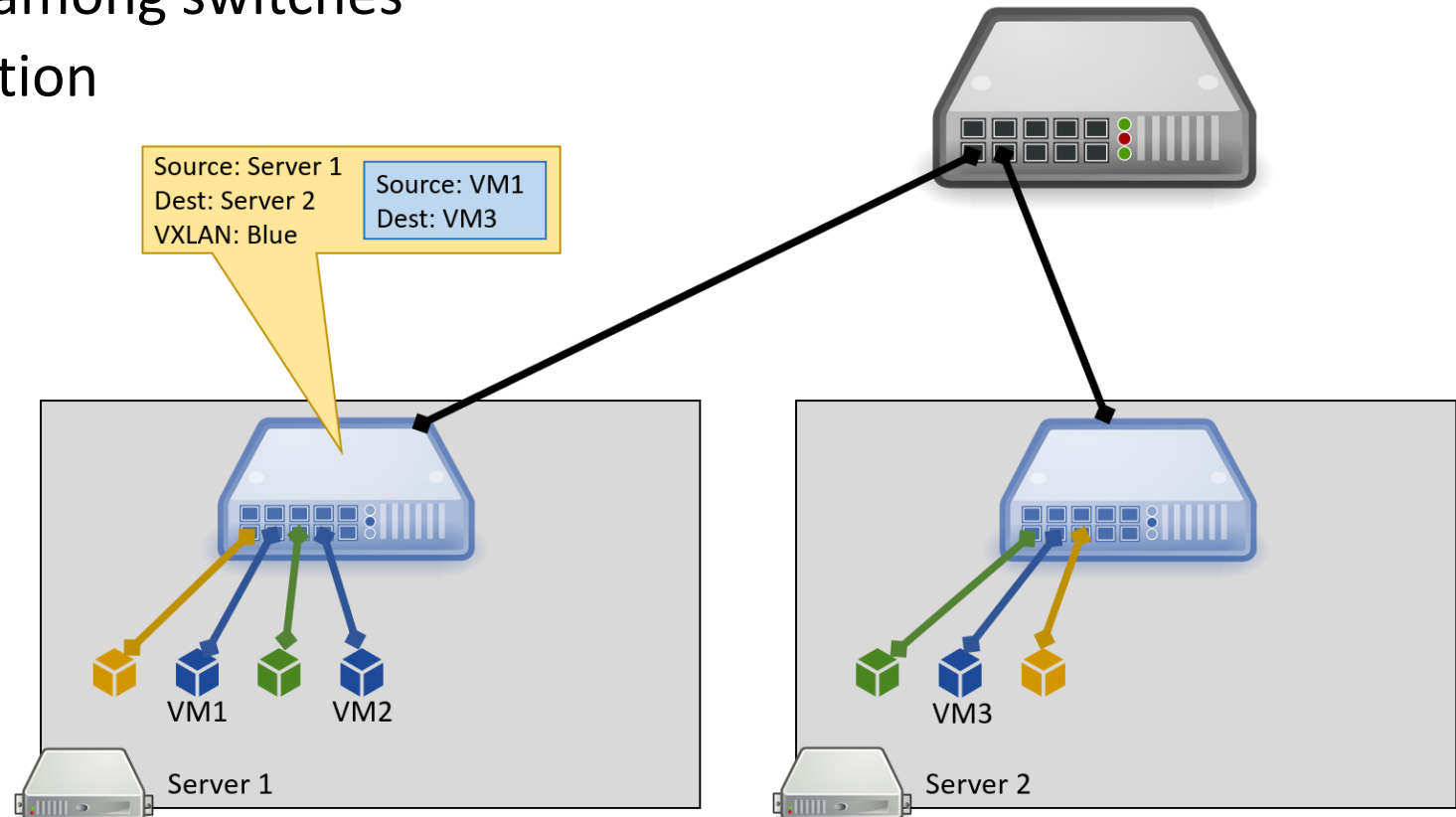
Managing virtual networks is challenging

- Three factors complicate management of virtual networks in the cloud
 - Complex interconnections among switches



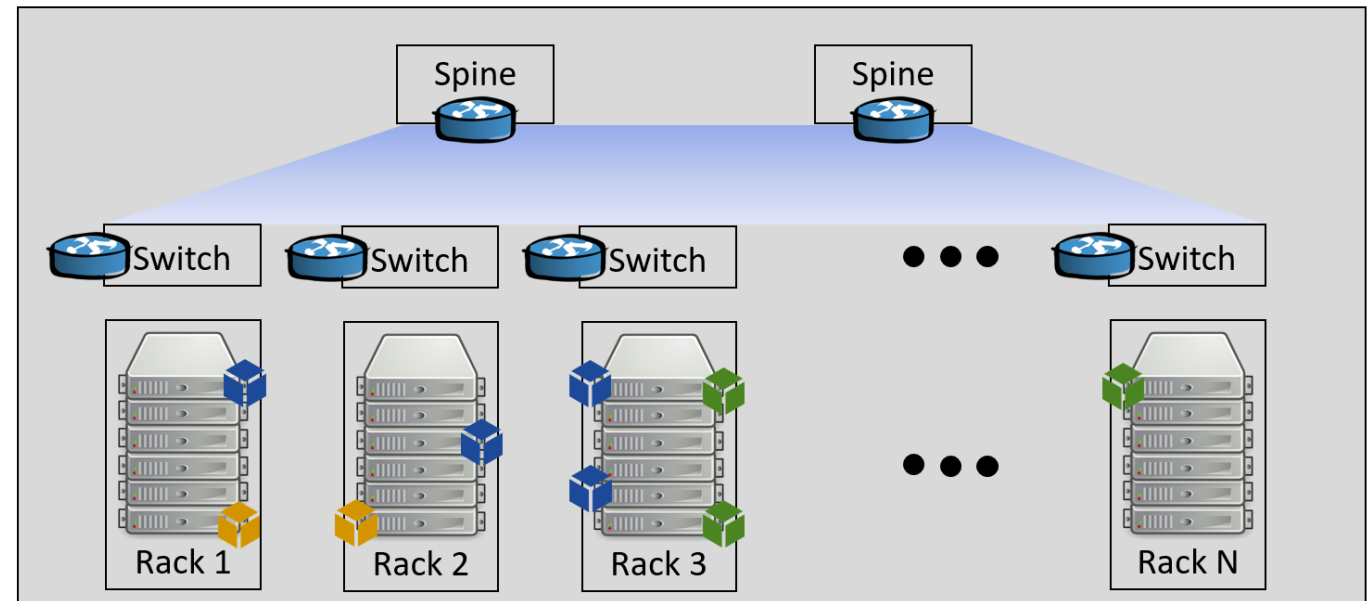
Managing virtual networks is challenging

- Three factors complicate management of virtual networks in the cloud
 - Complex interconnections among switches
 - Multiple levels of virtualization



Managing virtual networks is challenging

- Three factors complicate management of virtual networks in the cloud
 - Complex interconnections among switches
 - Multiple levels of virtualization
 - Arbitrary placement and migration of entities



Computing routes in datacenters

- Routing protocols
 - Link-state (OSPF) and distance vector (RIP)
 - Compute shortest paths
 - Policy-based (BGP)
 - Compute short, policy-compliant paths

Computing routes in datacenters

- Routing protocols
 - Link-state (OSPF) and distance vector (RIP)
 - Compute shortest paths
 - Policy-based (BGP)
 - Compute short, policy-compliant paths
- Software-defined networks
 - Centralized controller
 - Maintains state of the network
 - Configures routing rules on physical and virtual switches (OpenFlow)
 - Flexibility to configure arbitrary routes and rules