FUJITSU

shaping tomorrow with you

FloatingIP Enhancement For Public Cloud Infrastructure

June 4, 2015

Yushiro Furukawa
Fujitsu Limited

Who am I ?

FUJITSU

- Yushiro Furukawa (Speaker)
  - Software Engineer of Fujitsu from 2011
    - Developer of OpenStack Neutron
  - Characteristics
    - Red glasses frame

Please remember me

Agenda

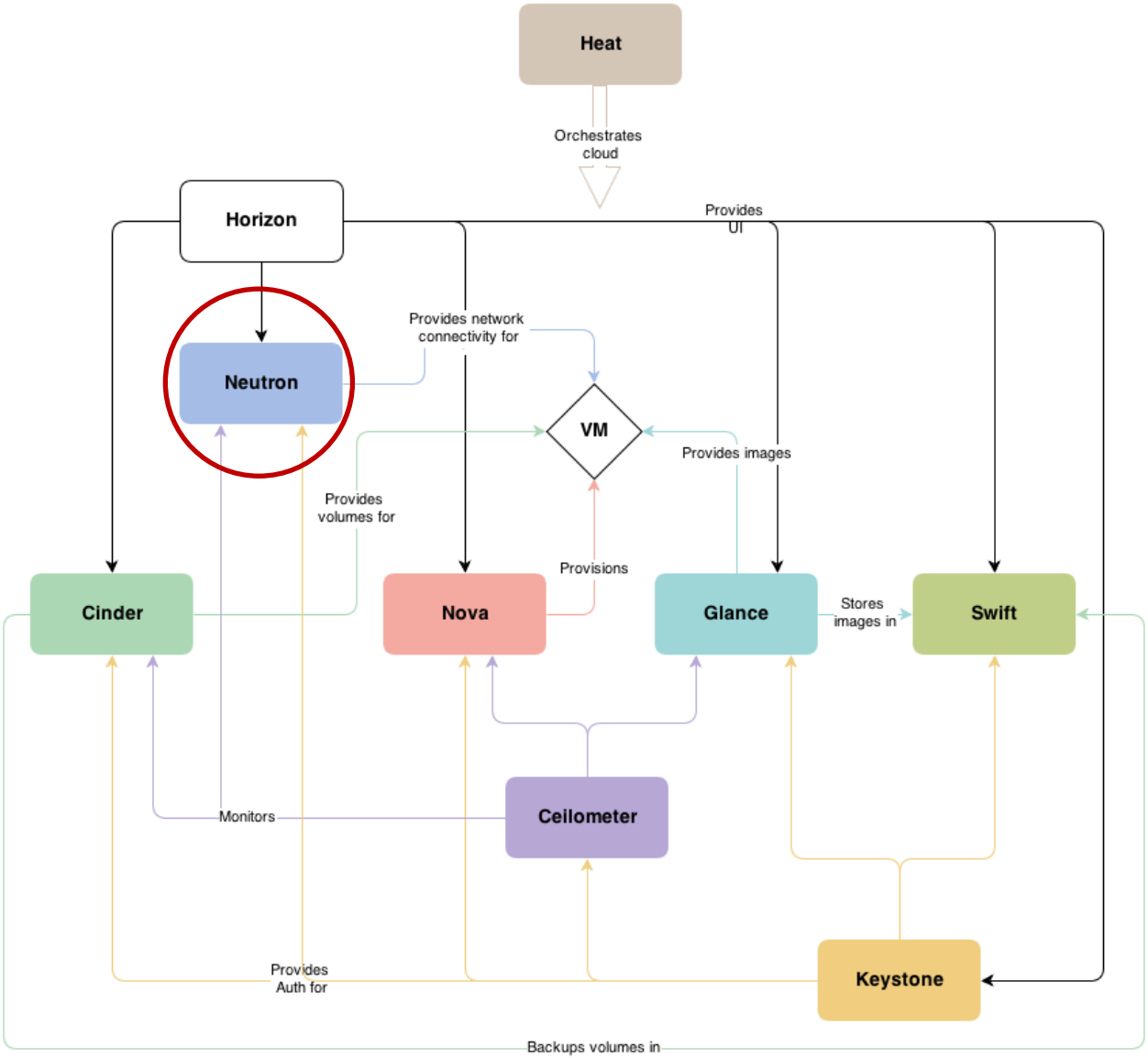
FUJITSU

1. OpenStack Neutron Overview
2. FloatingIP allocation with public cloud infrastructure
3. Legacy Router and DVR

FUJITSU

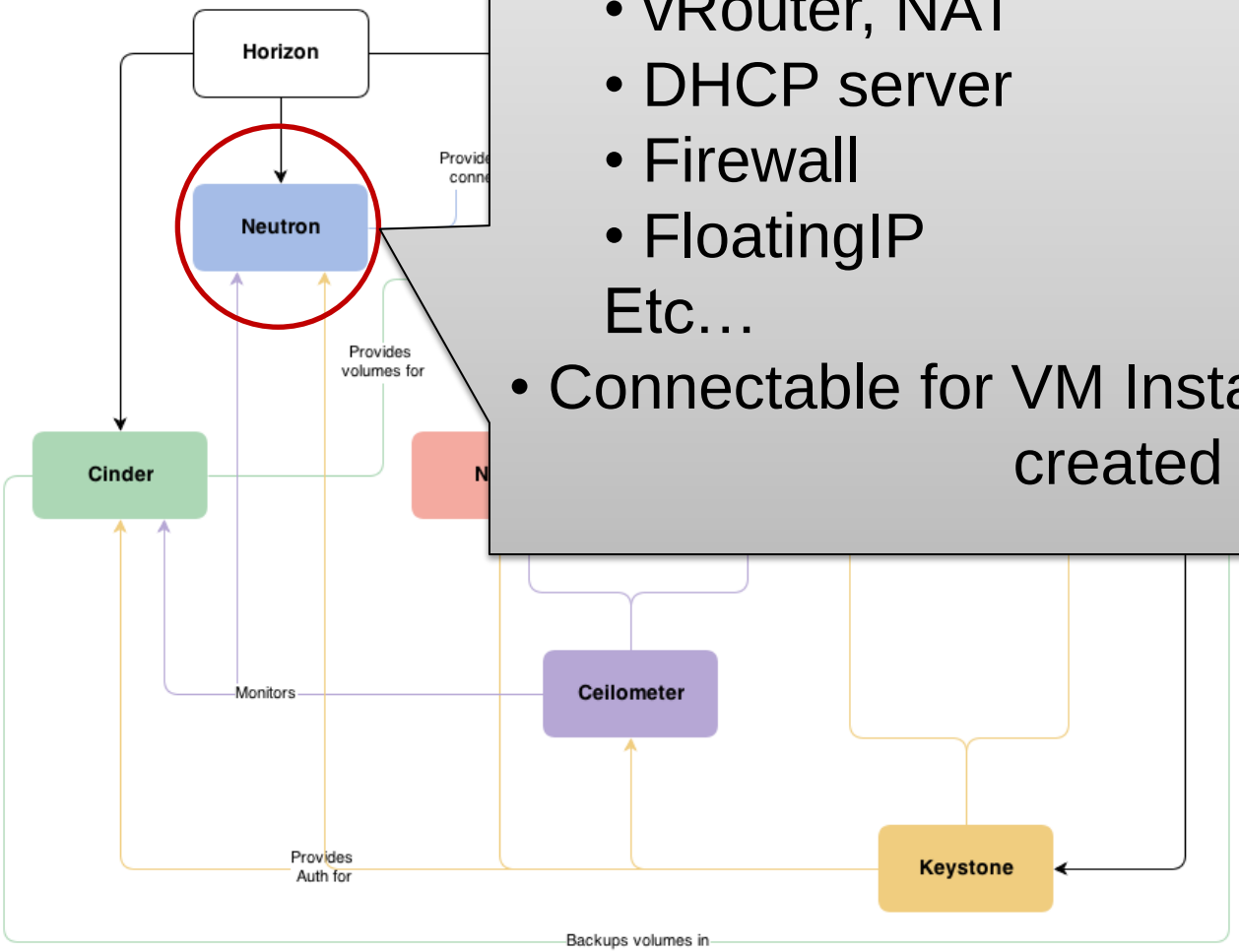
OpenStack Neutron Overview

OpenStack Neutron



OpenStack Neutron

FUJITSU

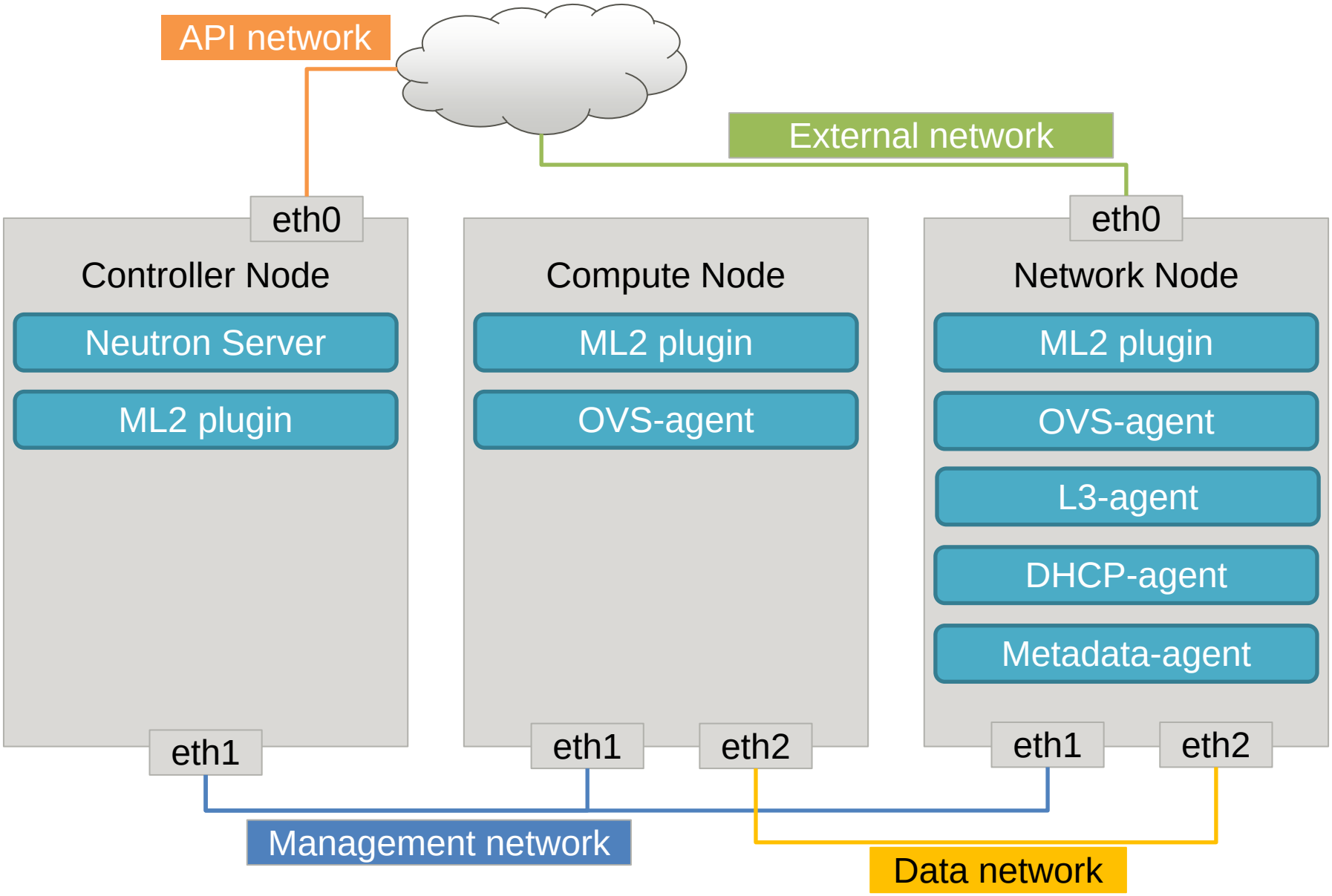


- Provide L2 / L3 networking
- Network isolation between tenants
  - vRouter, NAT
  - DHCP server
  - Firewall
  - FloatingIP

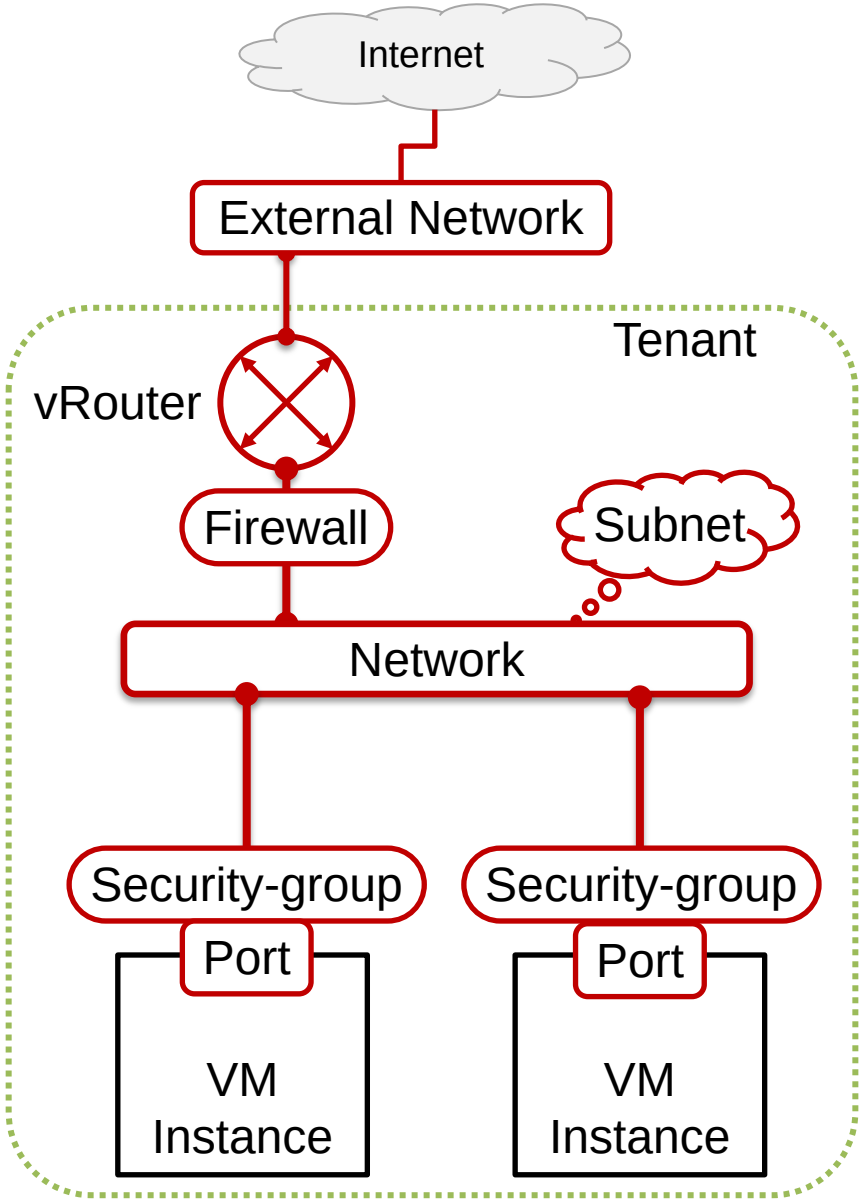
  Etc…
- Connectable for VM Instances created by Nova.

Neutron Components (Legacy Router)

FUJITSU

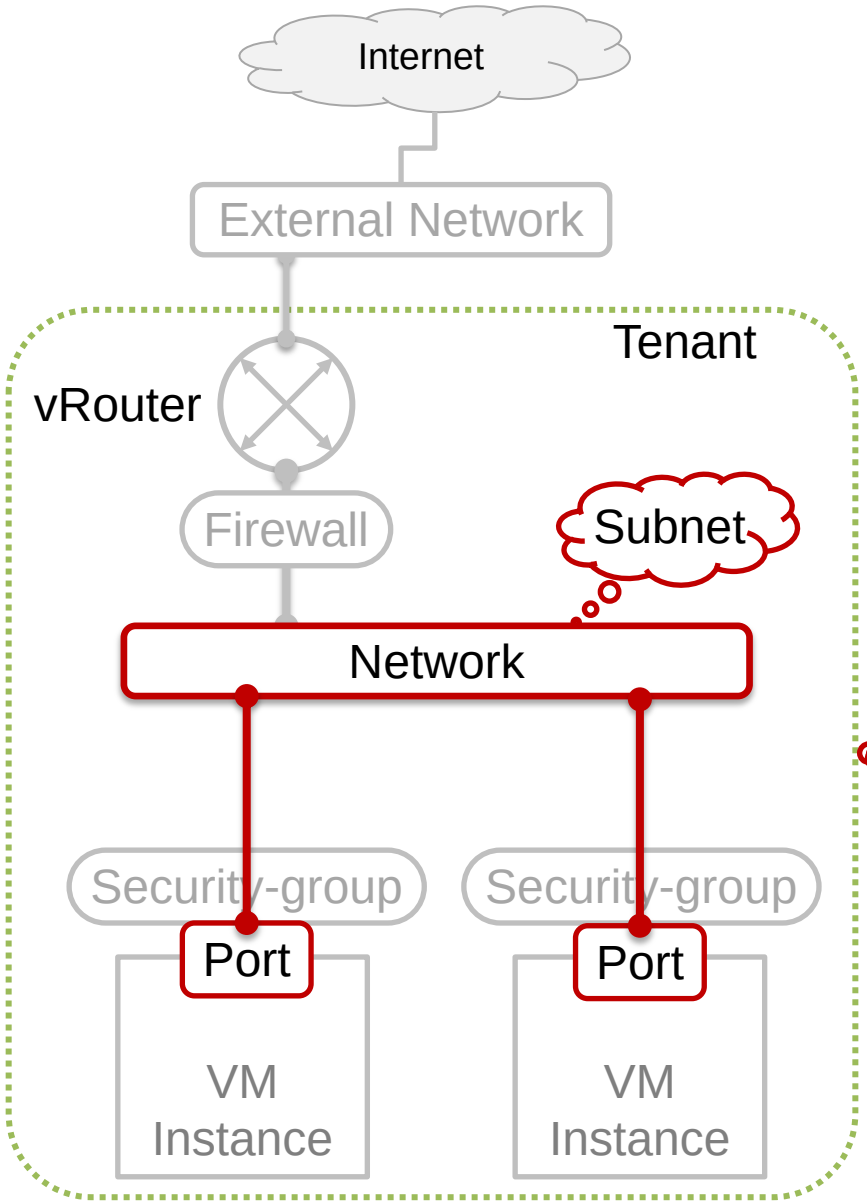


Neutron services



Neutron virtual networking services

FUJITSU



Network

- Virtual L2 network

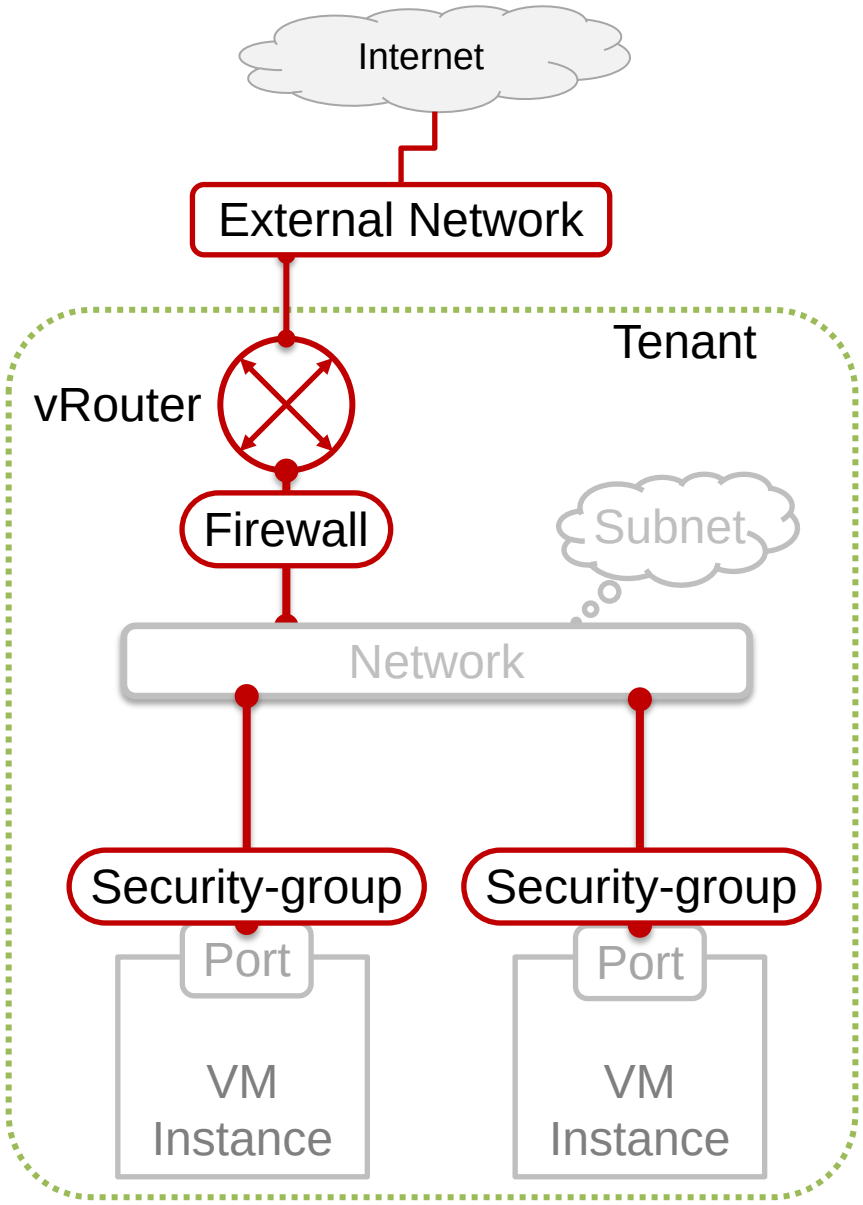
Port

- Connects a VM instance and Network
- Able to attach Security-Group

Subnet

- IP address pool
- Provides an IP address for Port

Neutron extension services



vRouter

- Connects Networks, also Network and External network.

External Network

- Virtual L2 network between the Internet and tenants

FloatingIP

- Will be explained later

Security-group

- Works on Port
- Filters ingress/egress packets
- Uses a White-list for filtering

Firewall

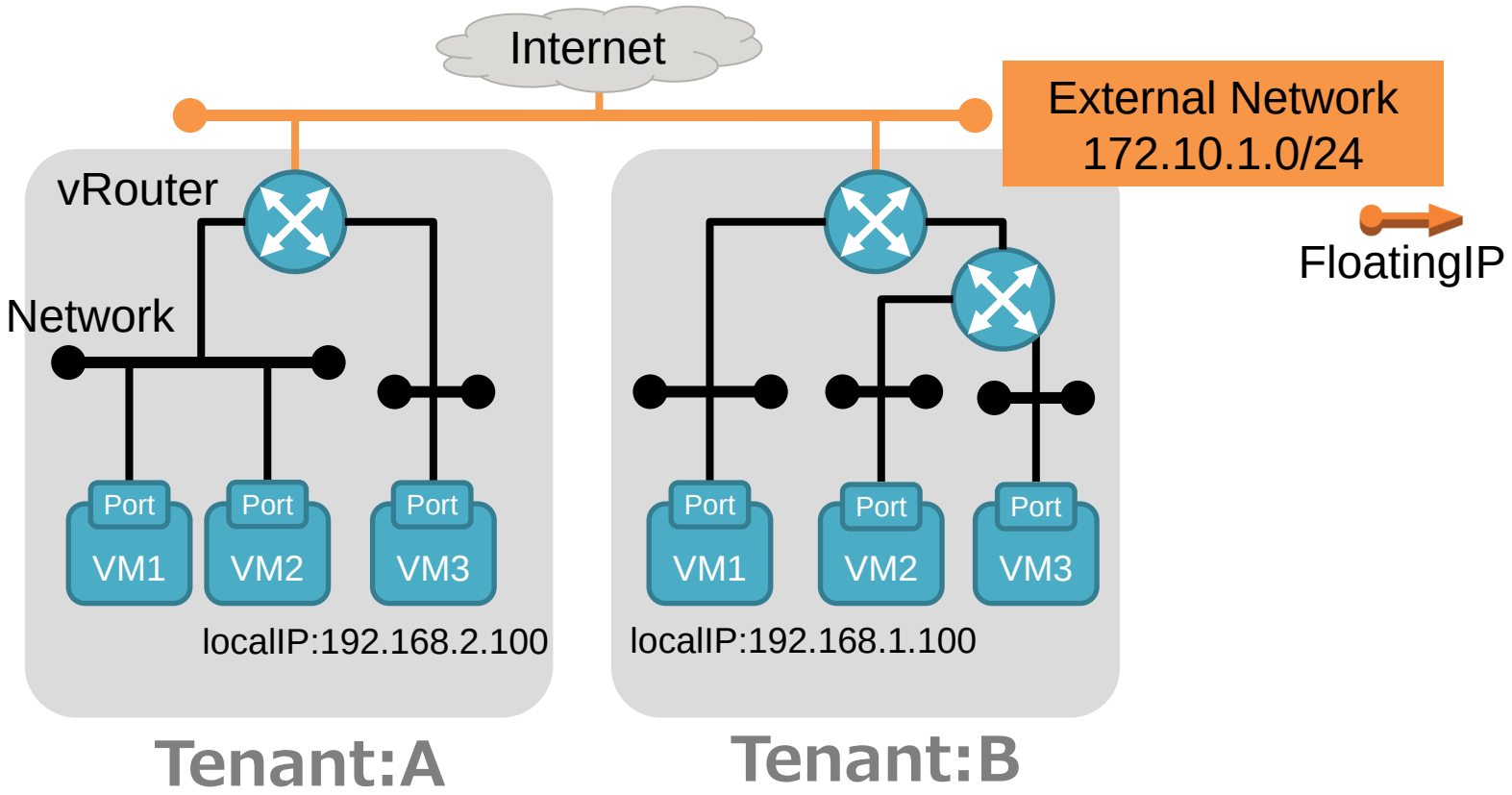
- Works on vRouter
- Filters packets

FUJITSU

FloatingIP Allocation For Public Cloud Infrastructure

What is FloatingIP?

- In public cloud, GlobalIP is usually used as FloatingIP.
- We can associate a FloatingIP with a specific Port.



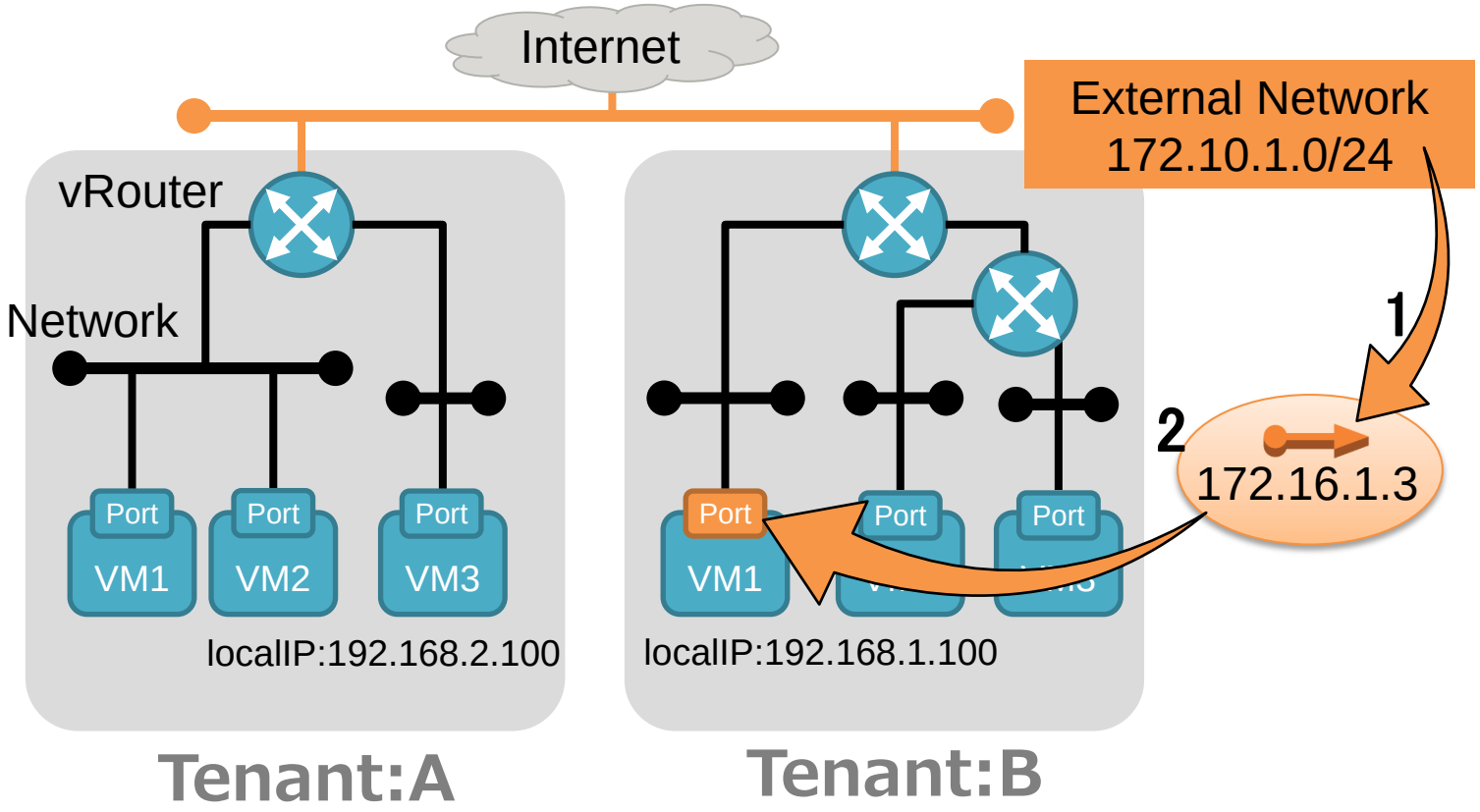
Setup steps

1. Create a FloatingIP

   $ neutron floatingip-create *FLOATING_NETWORK*

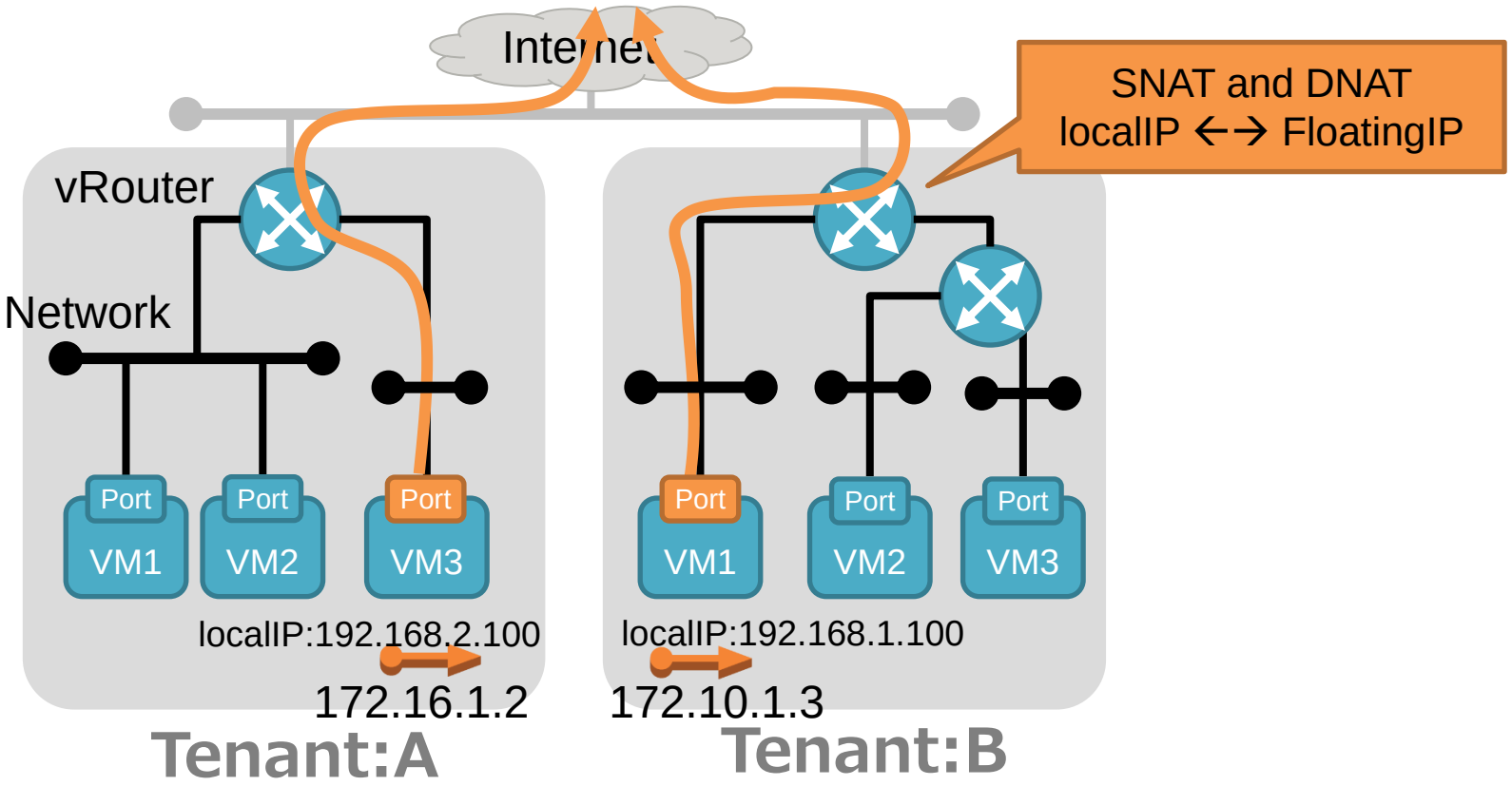
2. Associate the FloatingIP with a Port of a VM instance.

   $ neutron floatingip-associate *FLOATINGIP_ID PORT*



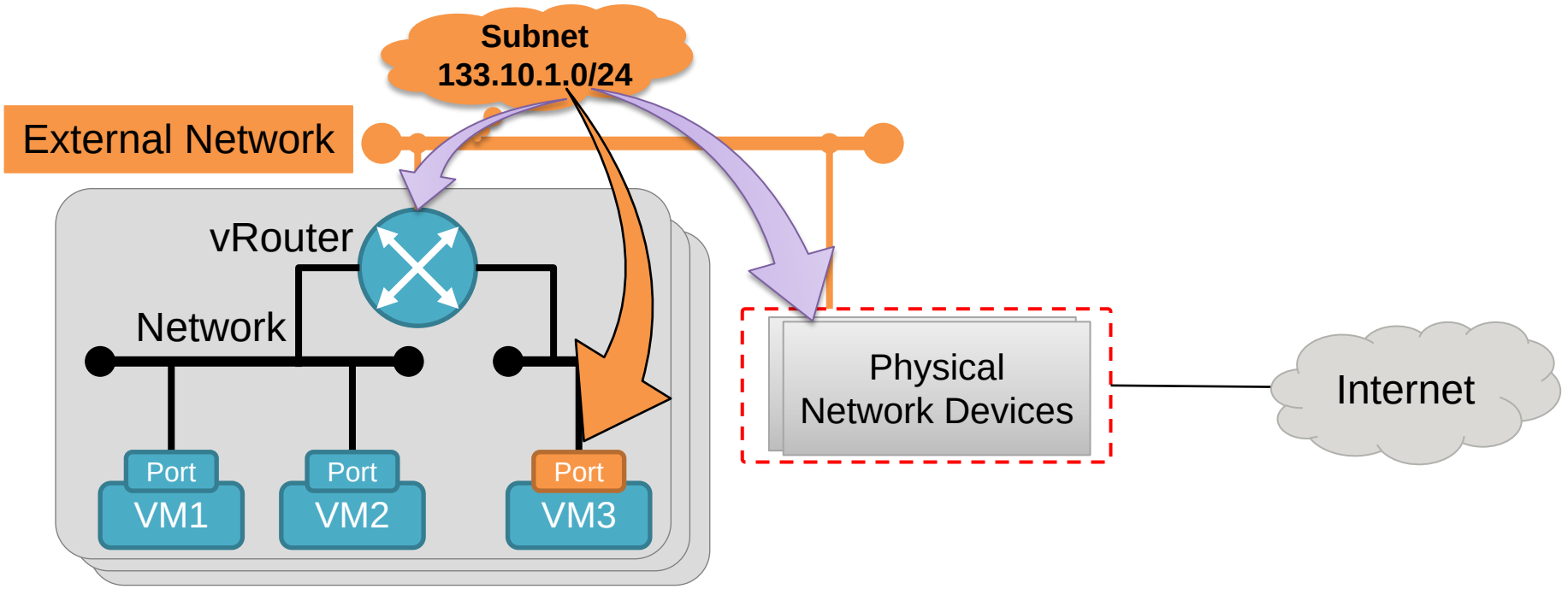
How FloatingIP works?

- SNAT and DNAT rule are added into vRouters.



Case-1: Single External Network

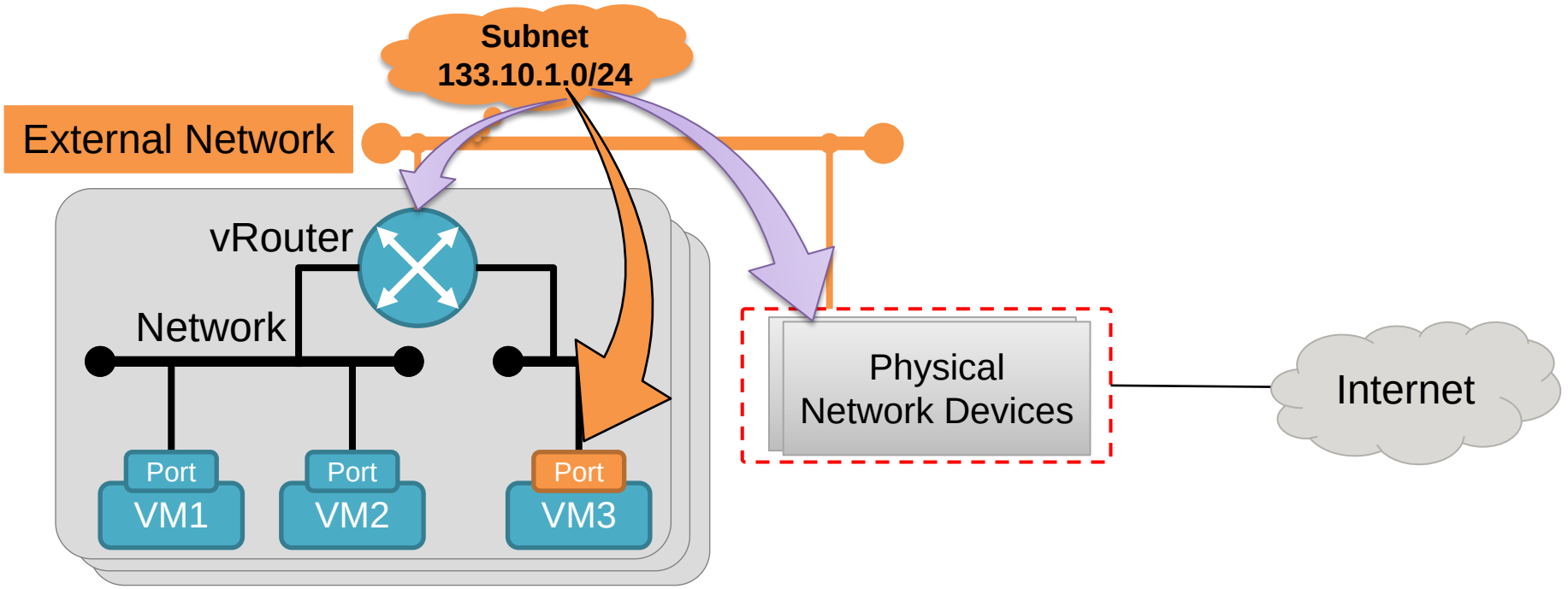
- GlobalIP is used as FloatingIP.
- FloatingIP address is allocated from the Subnet.
- IP address for physical network devices is manually picked up from the IP addresses in the Subnet.
  - Meaning the cloud provider has to make sure to avoid overlapping



Case-1: Single External Network

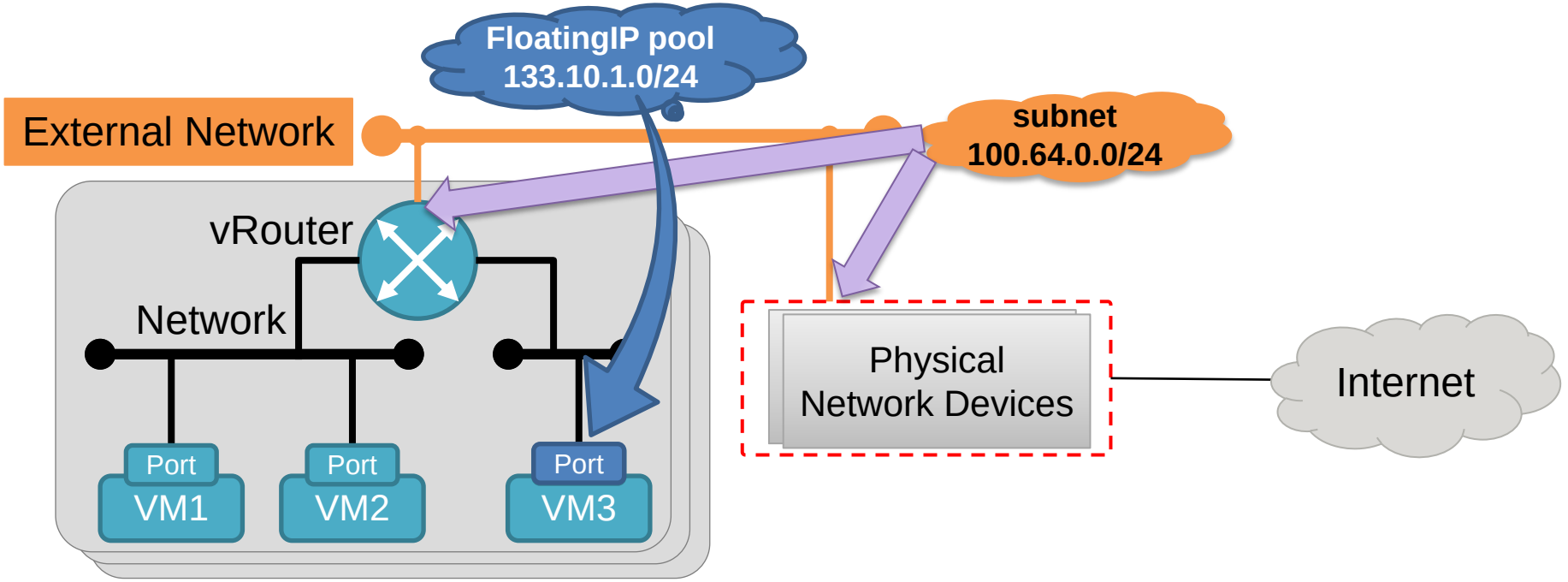
- GlobalIP is used as FloatingIP.
- FloatingIP address is allocated from the Subnet.
- IP address for physical network devices is manually picked up from the IP addresses in the Subnet.

This increases complexity of address allocation algorithm



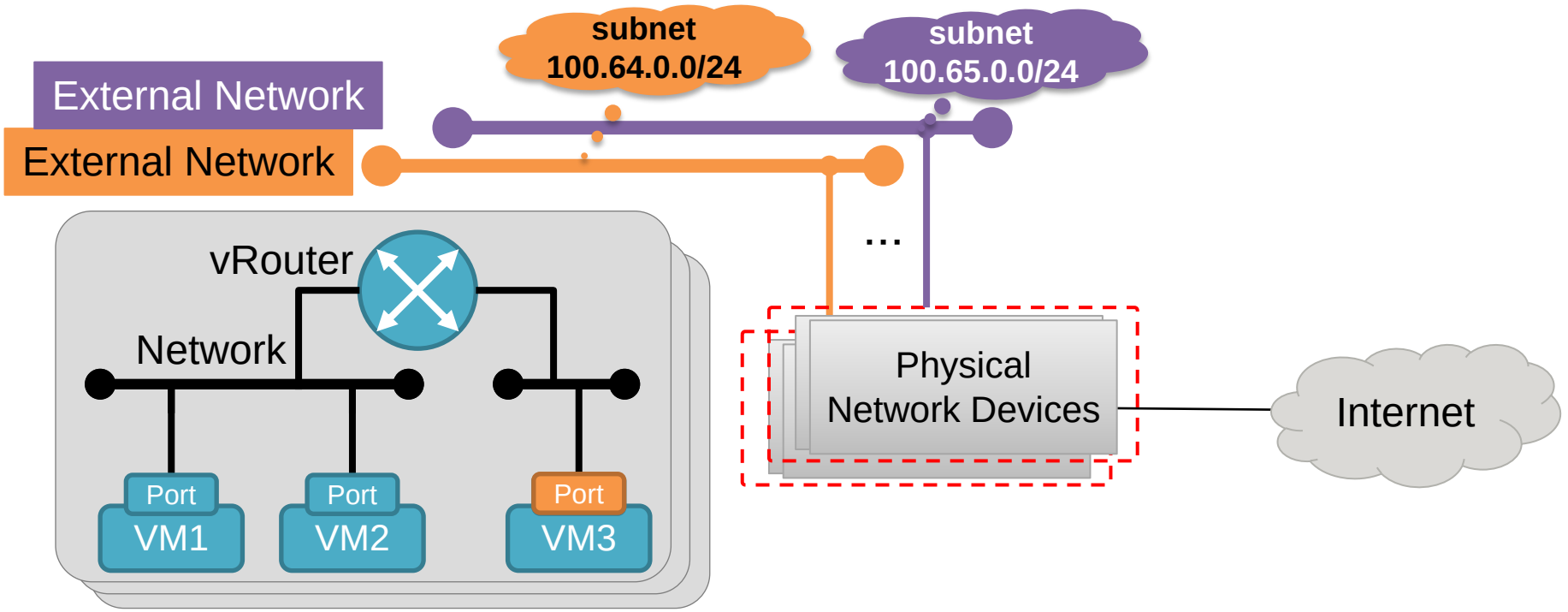
Proposal of Case-1

- GlobalIP is used as FloatingIP.
- Use PrivateIP for vRouters and physical routers.
- Create “FloatingIP Pool” for FloatingIP allocation.
  - The cloud provider no longer has to be worried about overlapping



Case-2: Multiple External Networks

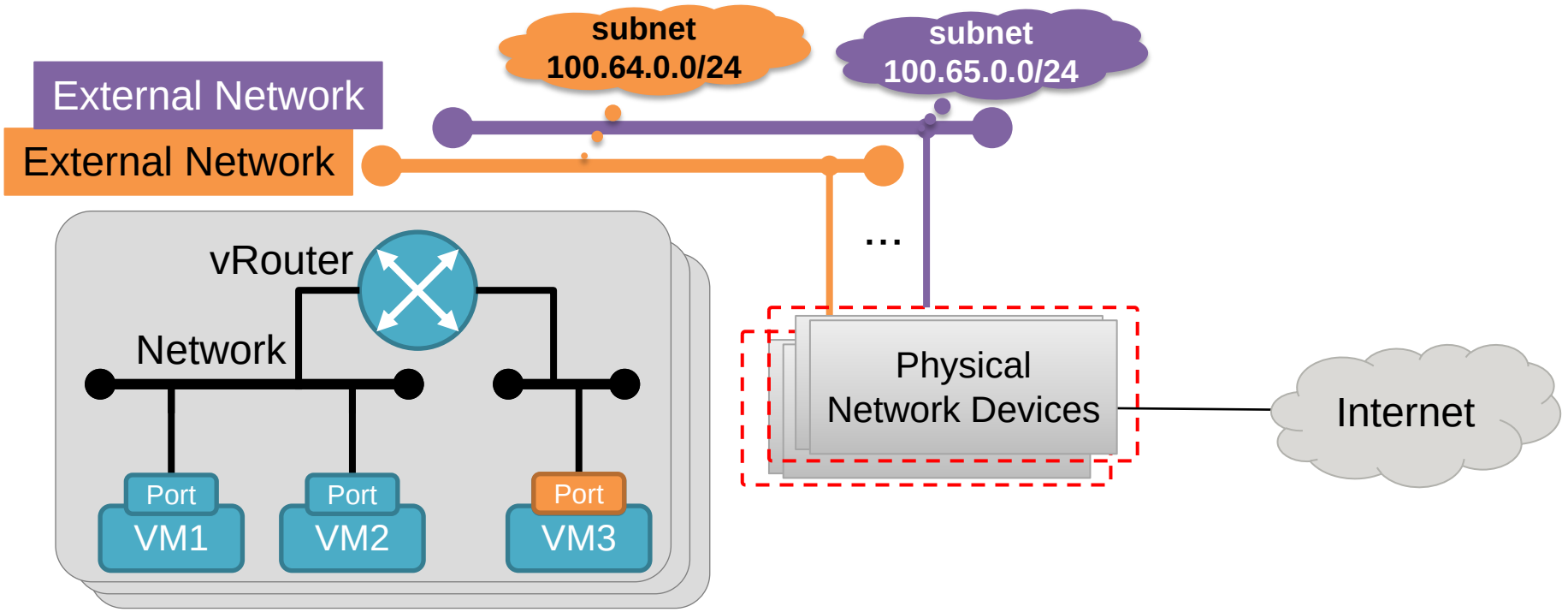
- GlobalIP is used as FloatingIP.
- There can be a case where several external networks exist in the infrastructure for some reasons



Case-2: Multiple External Networks

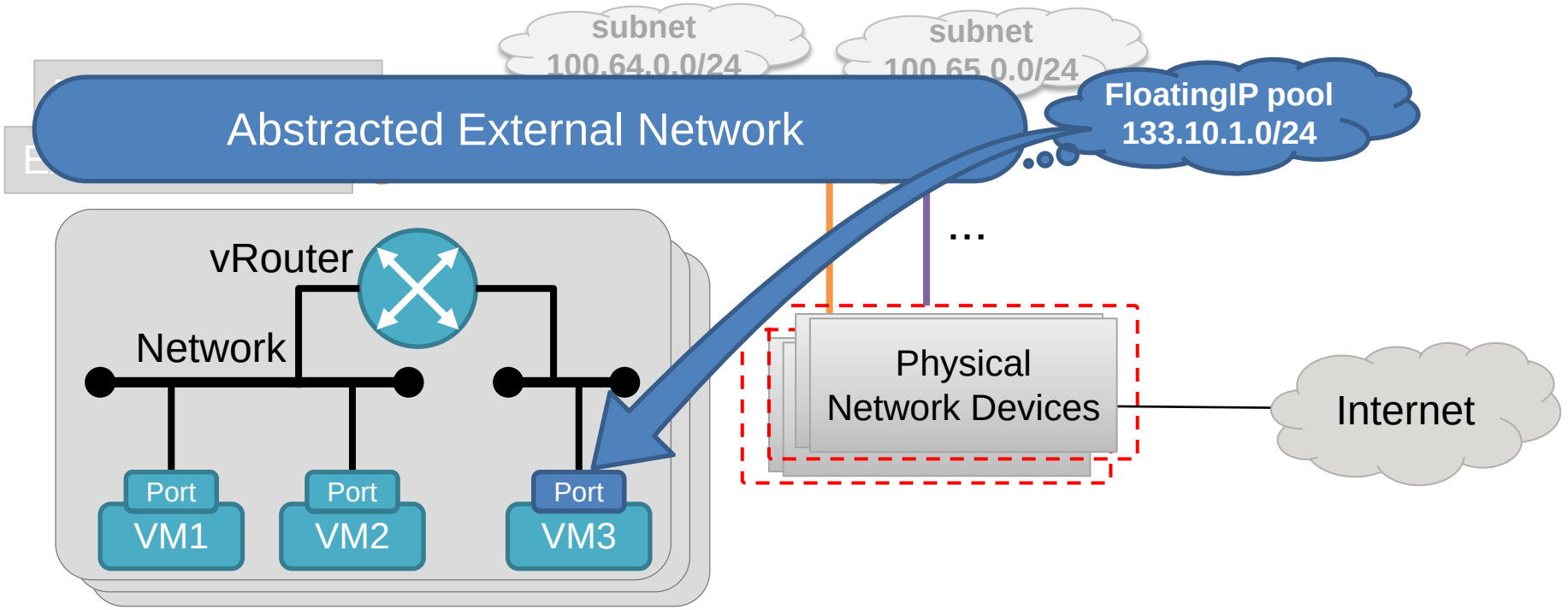
- GlobalIP is used as FloatingIP.
- There can be a case where several external networks exist in the infrastructure for some reasons

Tenant-user have to select which external network to connect to, but it's just a burden tenant users shouldn't be take



Proposal of Case-2

- Abstract the External Network
  - Tenant-users can see only one abstracted external network
- FloatingIP pool simplifies the mechanism of the Abstracted External Network.
  - Without FloatingIP pool, each External network has a Subnet, and the Abstracted External Network needs to select which Subnet to use...



However….

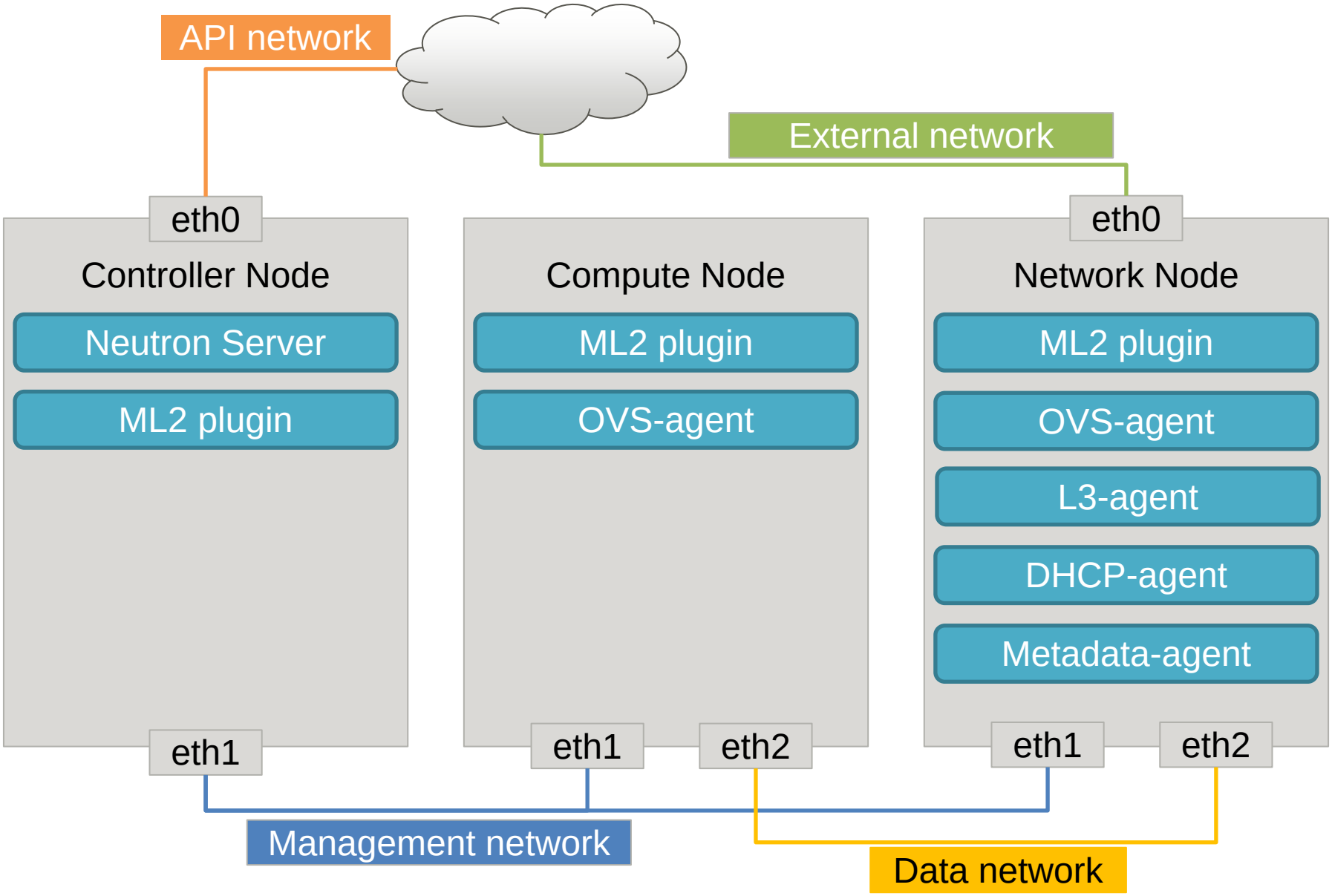
- I have been thinking about FloatingIP enhancement for legacy router configuration.
- DVR is becoming the de facto standard configuration, and now I also should consider to develop the enhancement on DVR.

FUJITSU

DVR (**D**istributed **V**irtual **R**outer) Enhancement

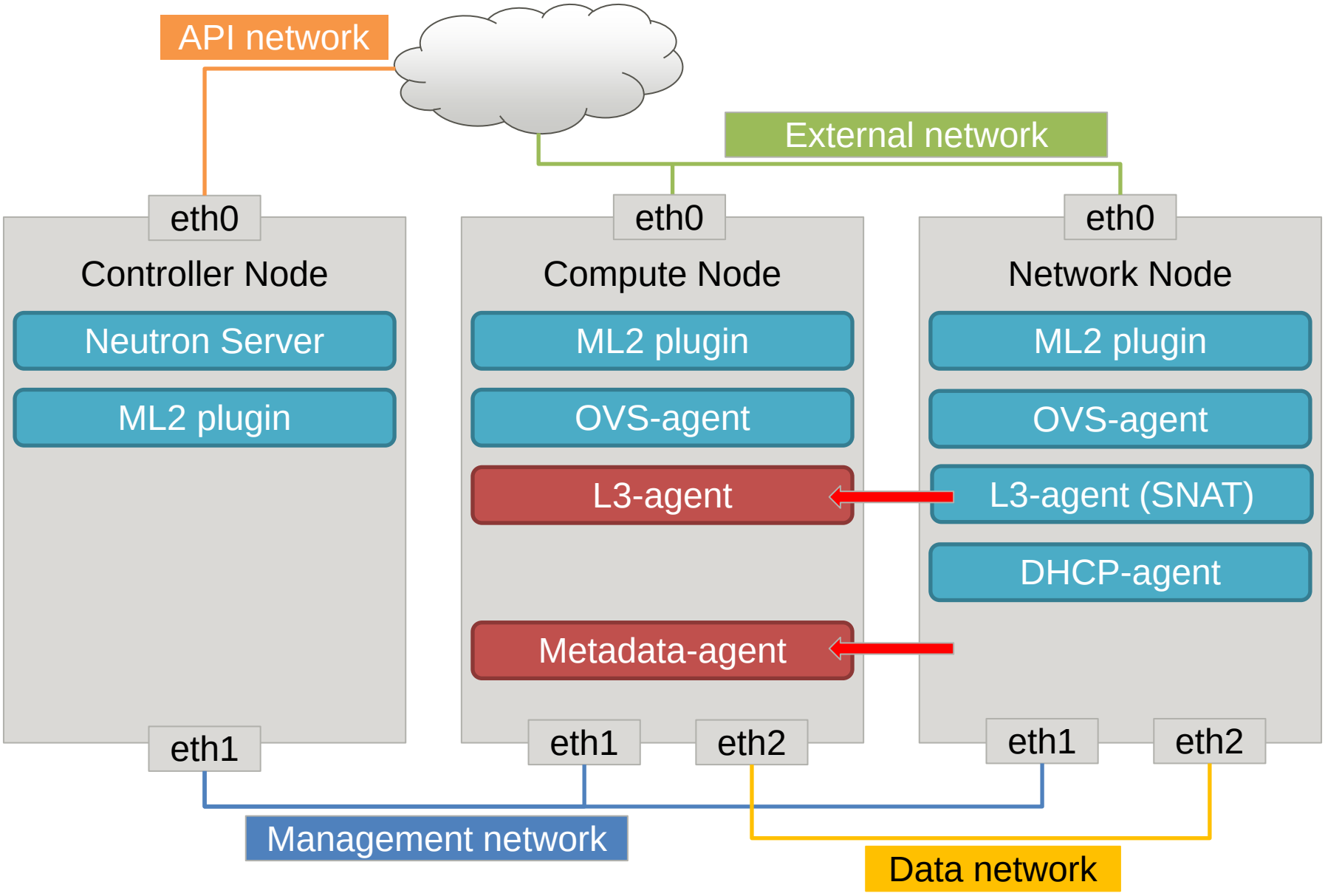
Neutron Components (Legacy-Router)

FUJITSU

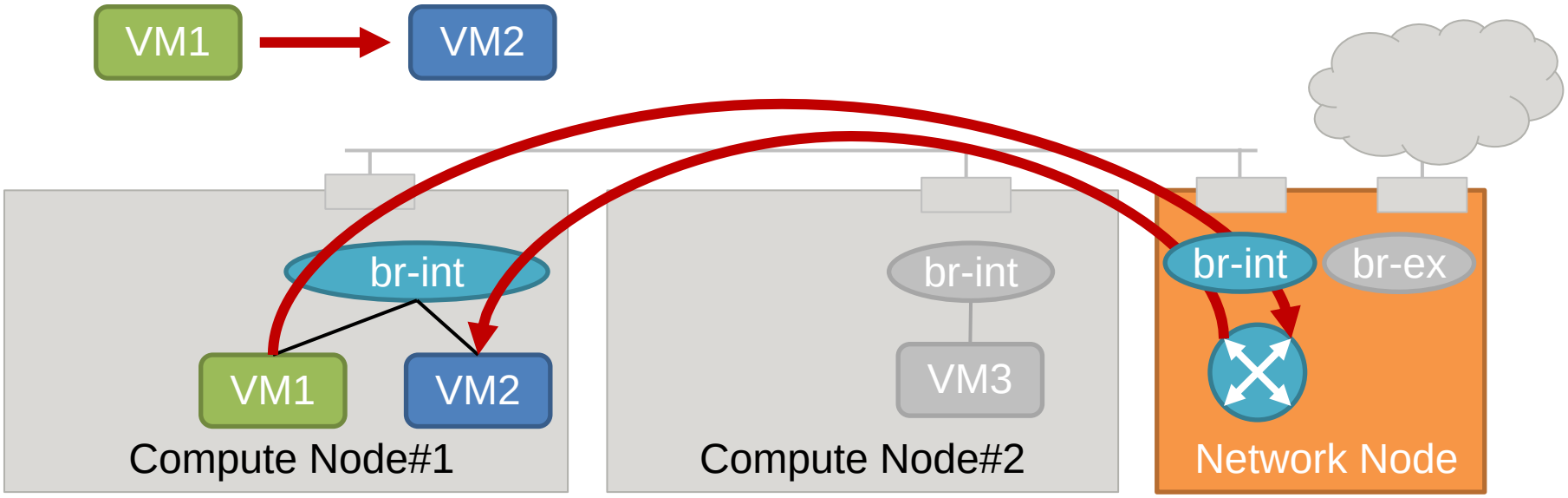


Neutron Components (DVR)

FUJITSU



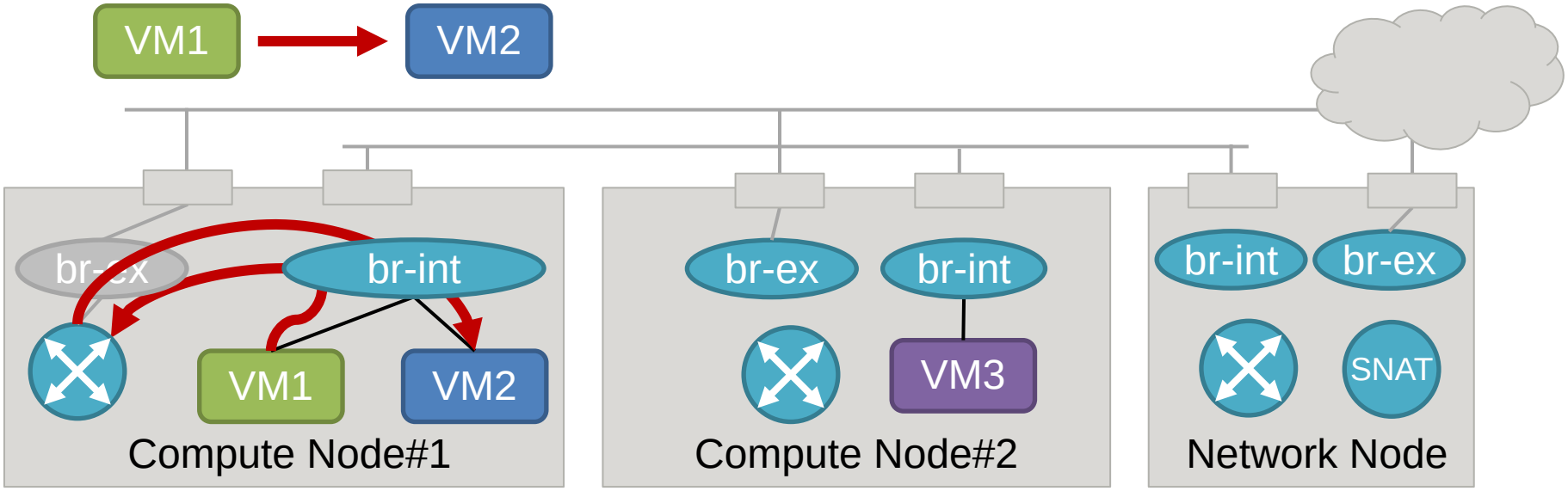
Network Traffic on Legacy Router



- Main characteristic:
  - vRouter only exists on Network Node.
  - All network traffic must go through Network Node.
    - East-West (between different Subnets)
    - North-South (between the Internet and tenants using FloatingIP or SNAT)

    => Can be a performance bottle neck.
  - Network Node is also Single-Point-of-Failure.

Network Traffic on DVR



- Main characteristic:
  - vRouter exists on all Compute Nodes.
  - Basically, Network traffic only has to go through Network Node when the traffic goes to the Internet using SNAT

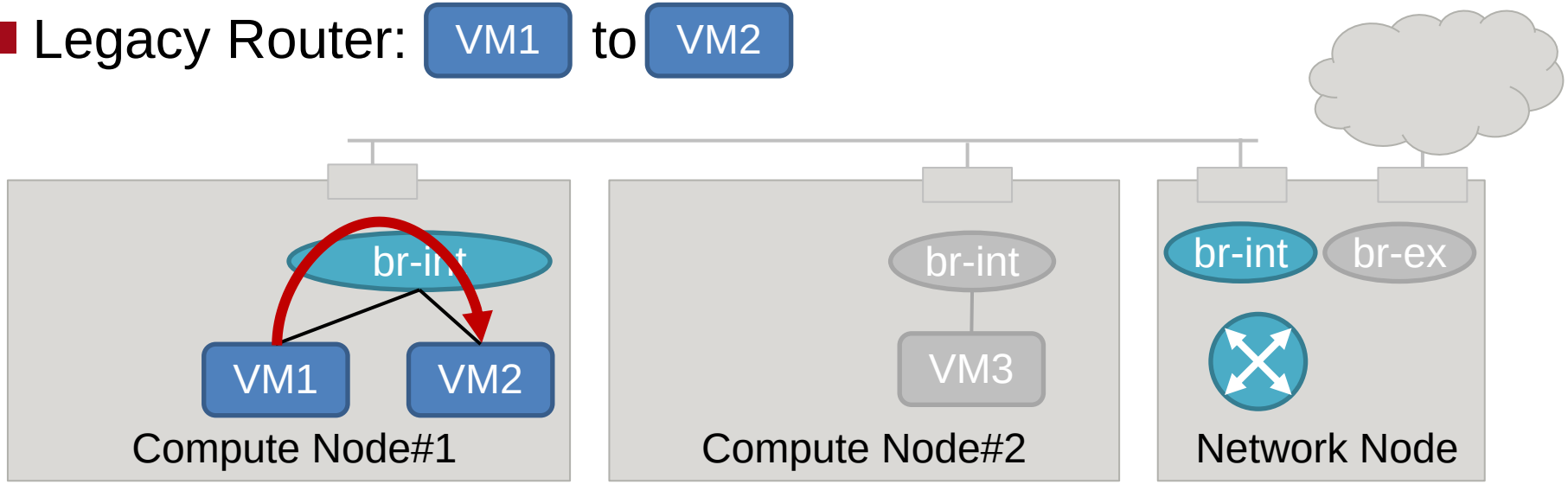
    => Performance can scale more.

Network Traffic Case#1

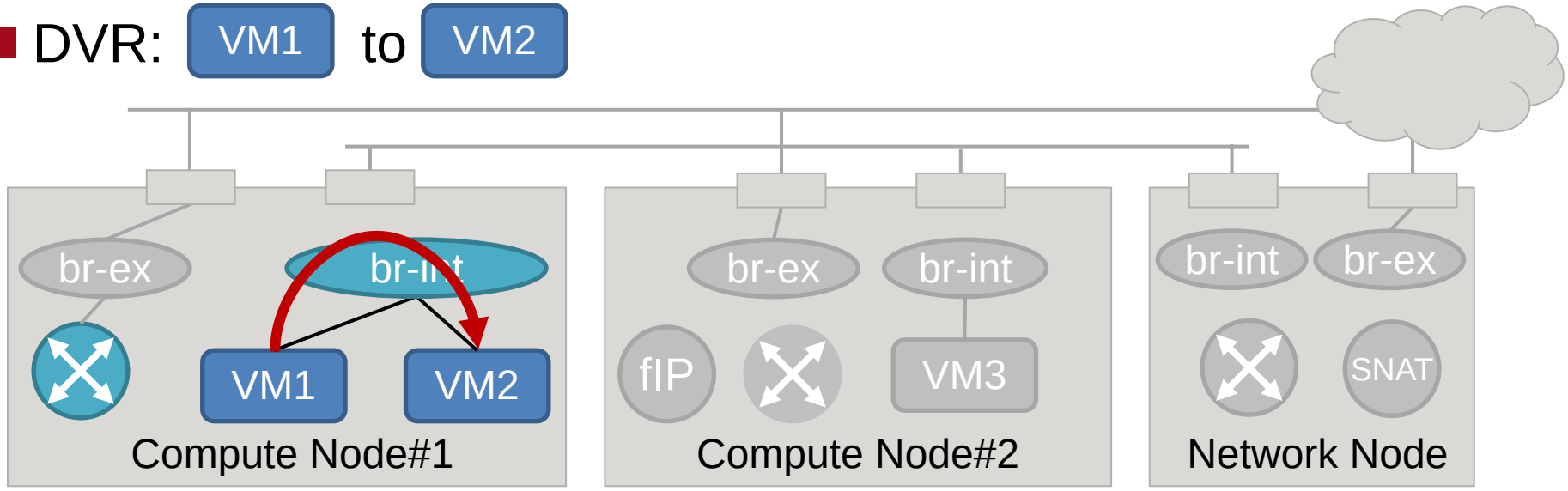
FUJITSU

Between VMs in the same Subnet and host

- Legacy Router: VM1 to VM2



- DVR: VM1 to VM2

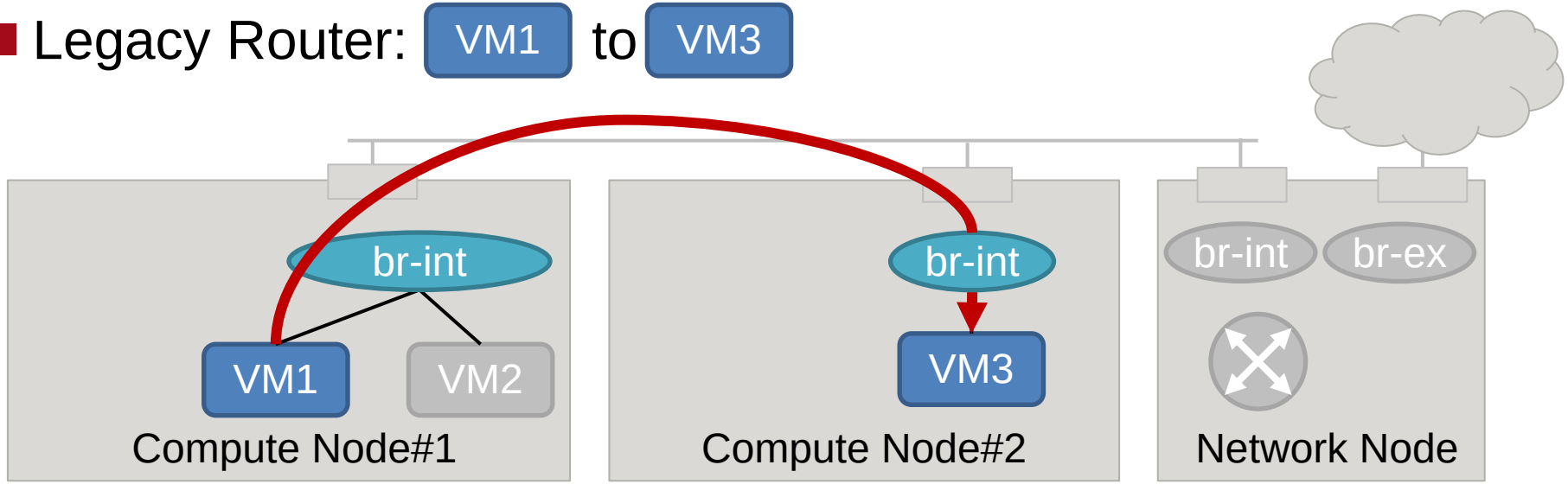


Network Traffic Case#2

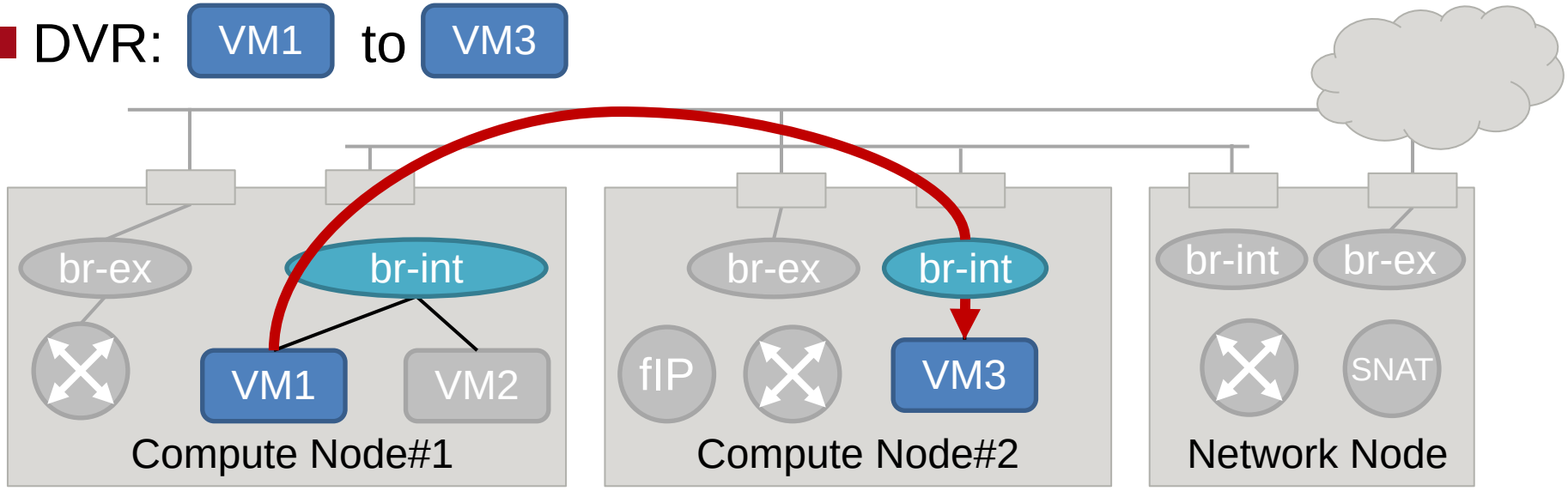
FUJITSU

Between VMs in the same Subnet, but in Different hosts

- Legacy Router: VM1 to VM3



- DVR: VM1 to VM3

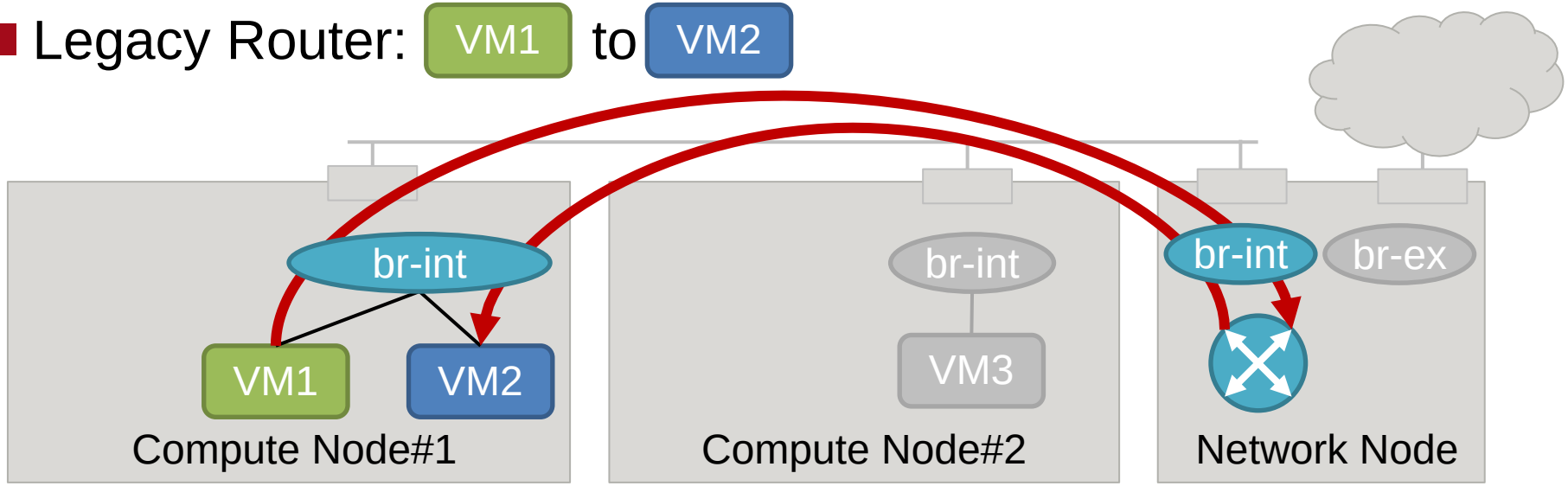


Network Traffic Case#3

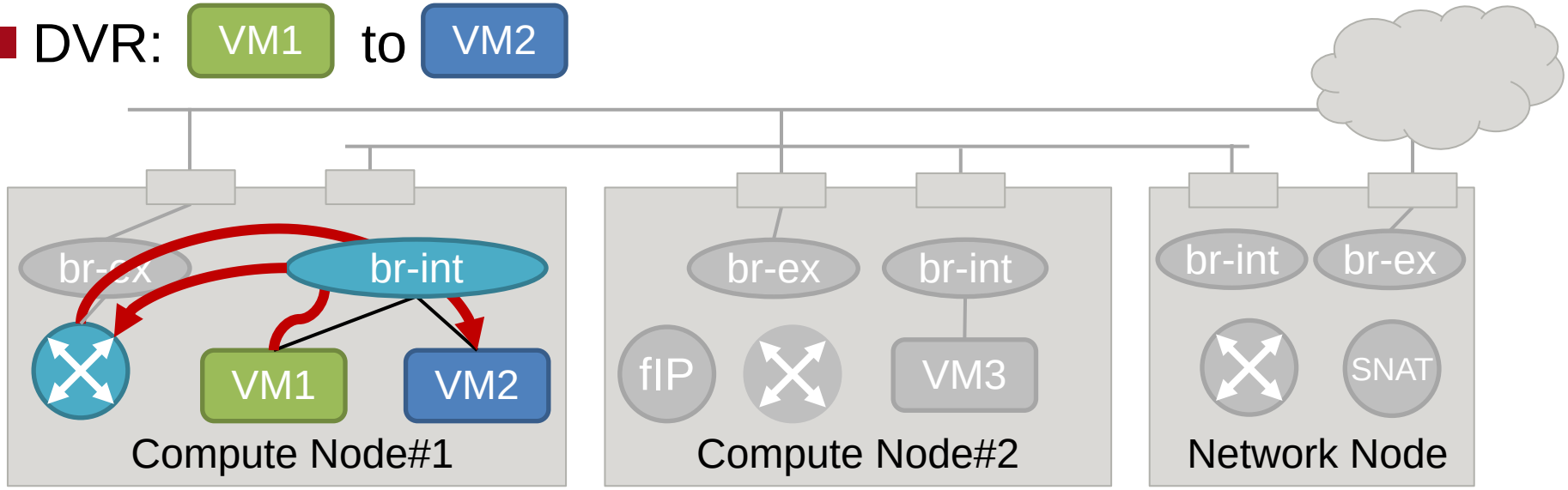
FUJITSU

Between VMs in the same hosts, but in different Subnets

- Legacy Router: VM1 to VM2



- DVR: VM1 to VM2

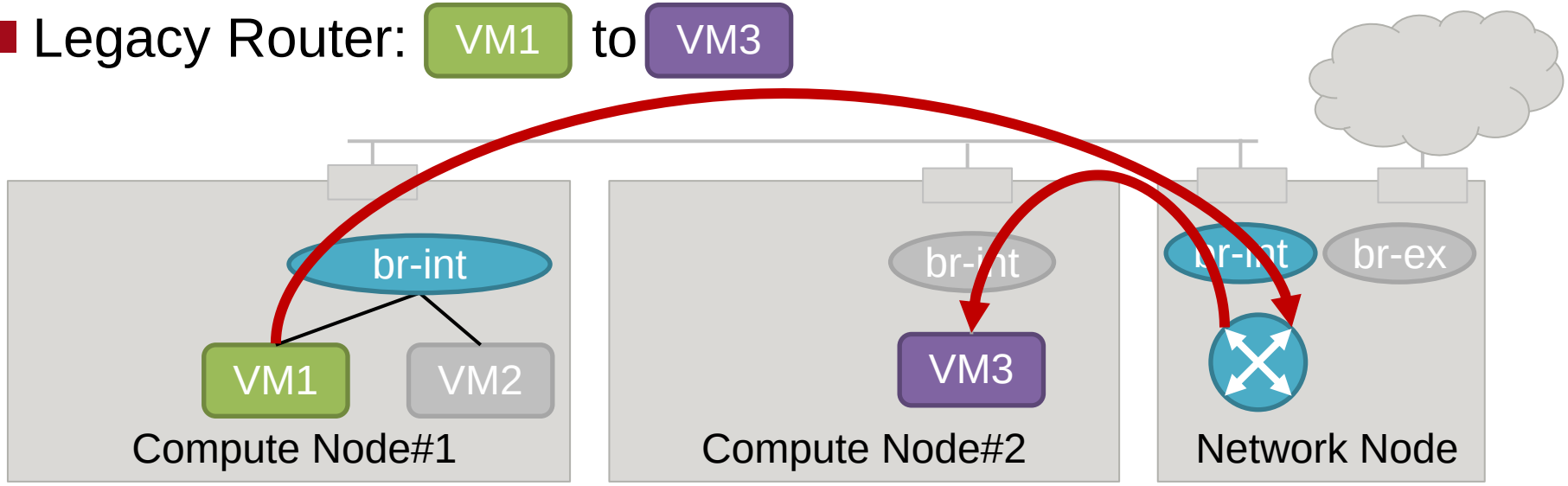


Network Traffic Case#4

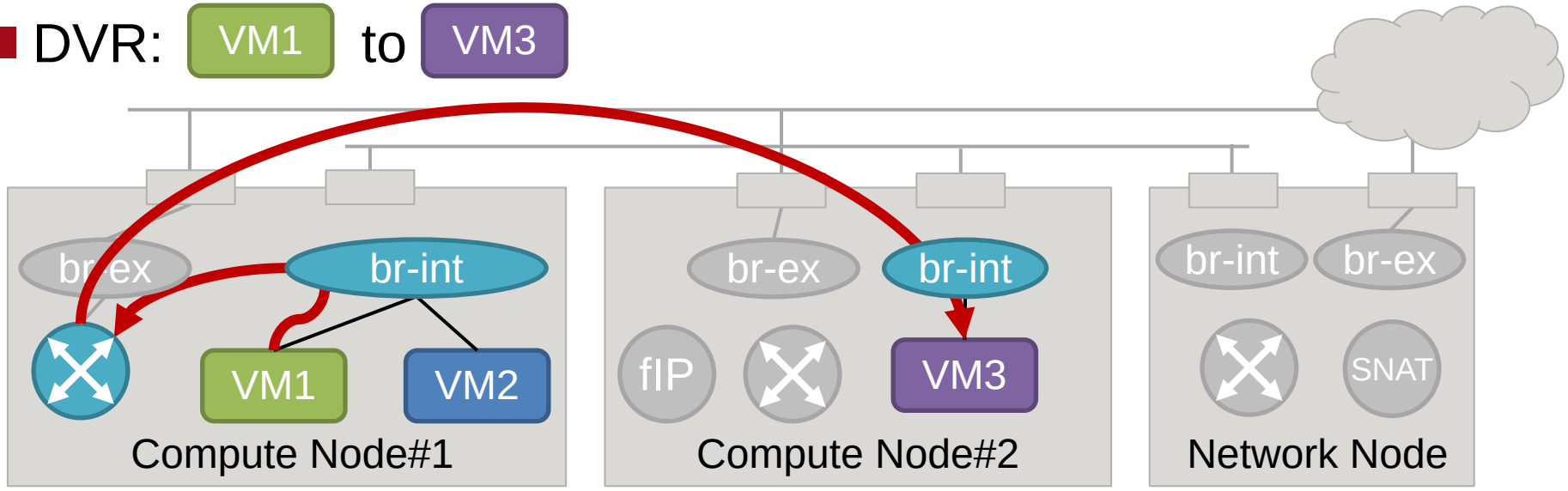
FUJITSU

Between VMs in different Subnets and hosts

- Legacy Router: VM1 to VM3



- DVR: VM1 to VM3

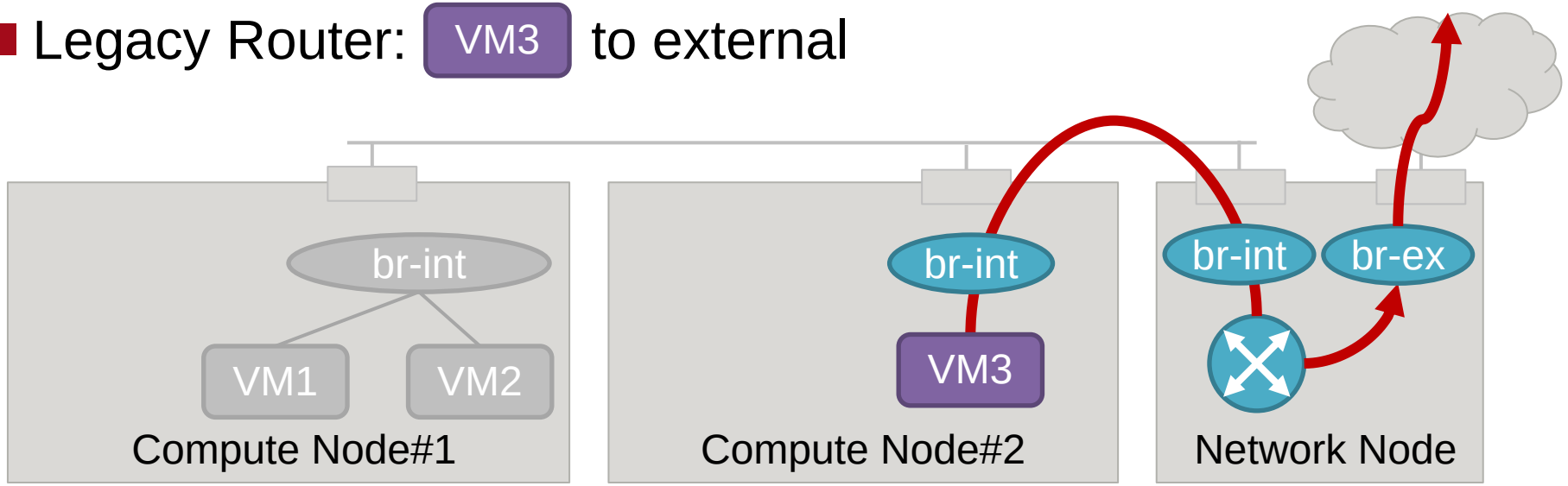


Network Traffic Case#5

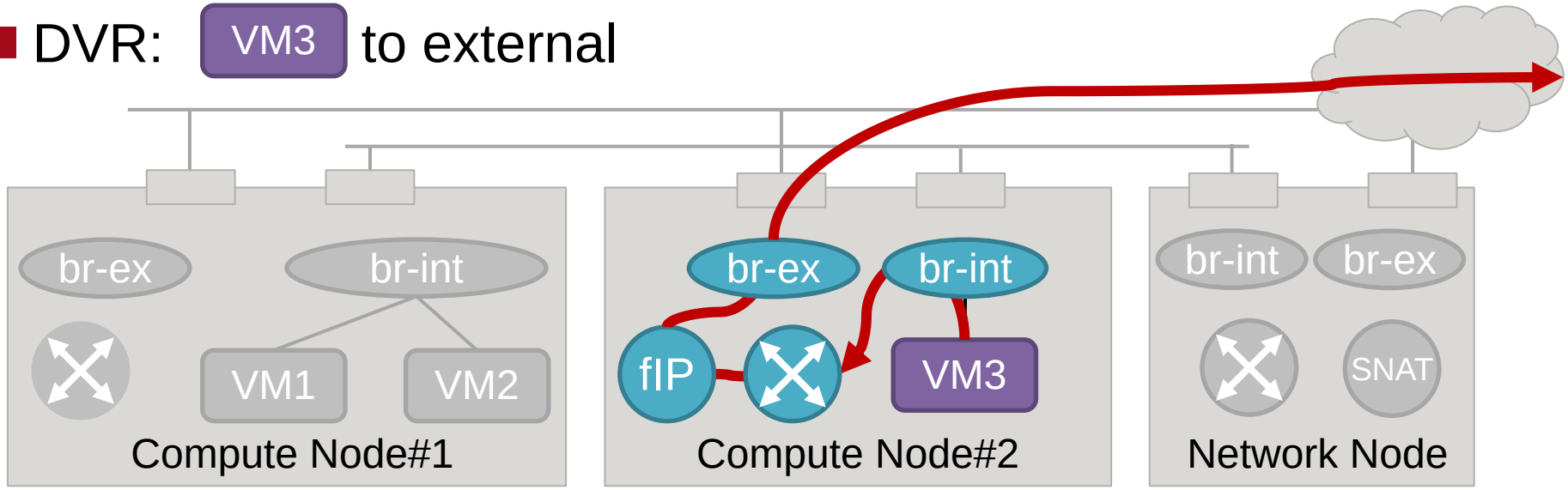
FUJITSU

Between the External Network and a VM using FloatingIP

- Legacy Router: VM3 to external



- DVR: VM3 to external

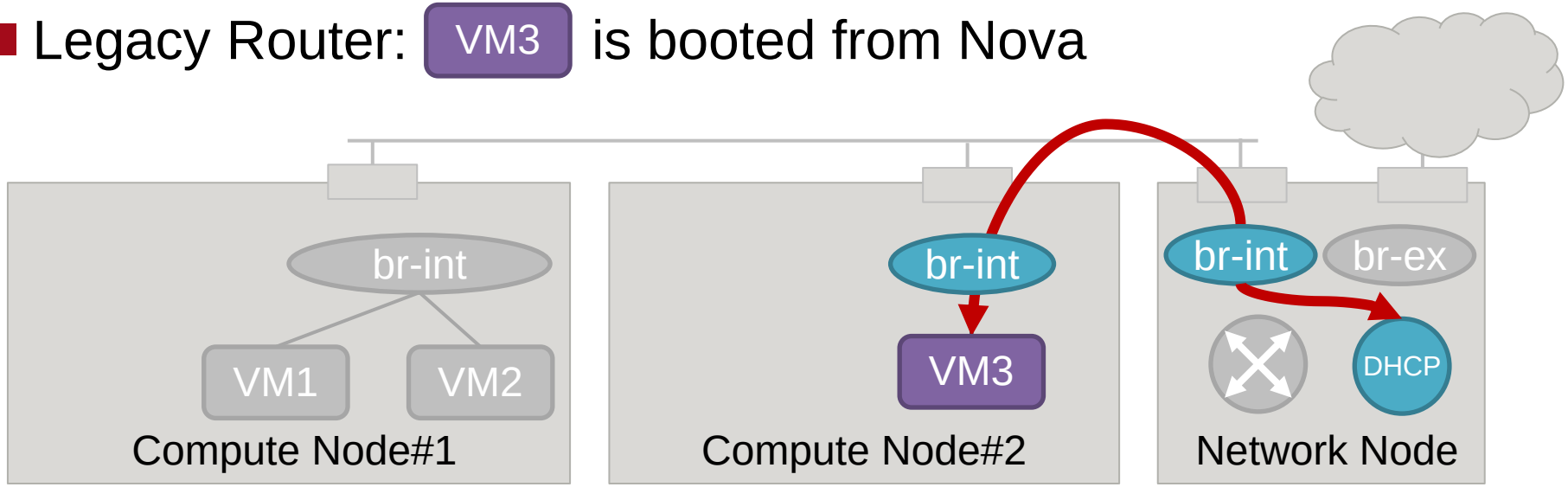


Network Traffic Case#6

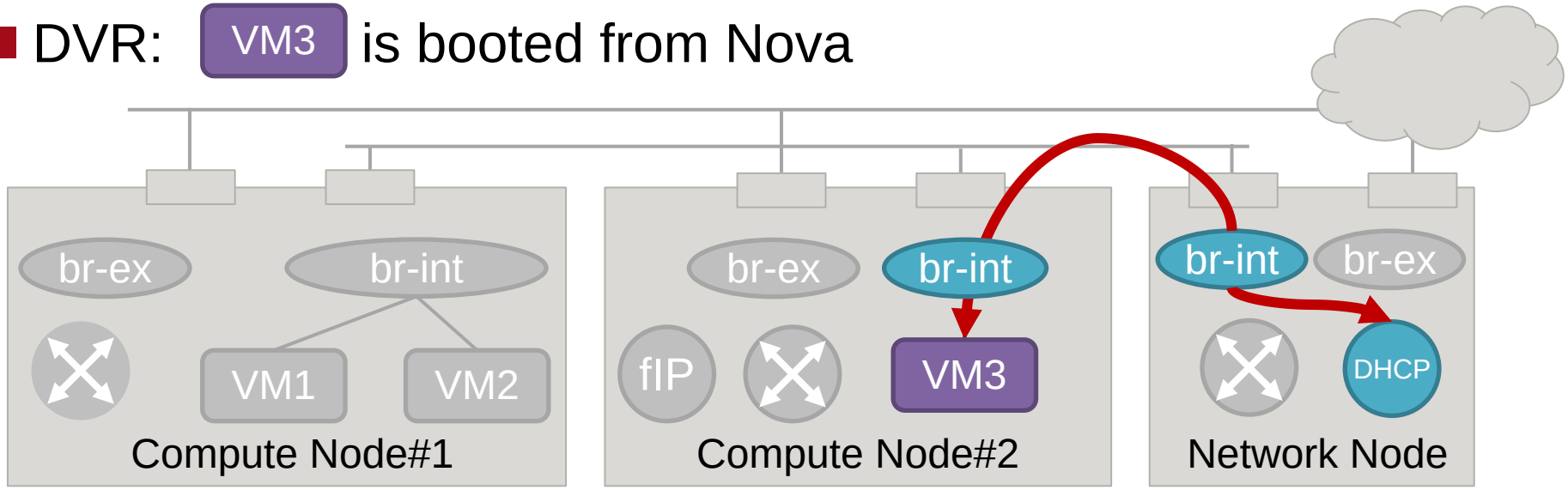
FUJITSU

VM booting: a VM accesses to DHCP server

- Legacy Router: VM3 is booted from Nova



- DVR: VM3 is booted from Nova

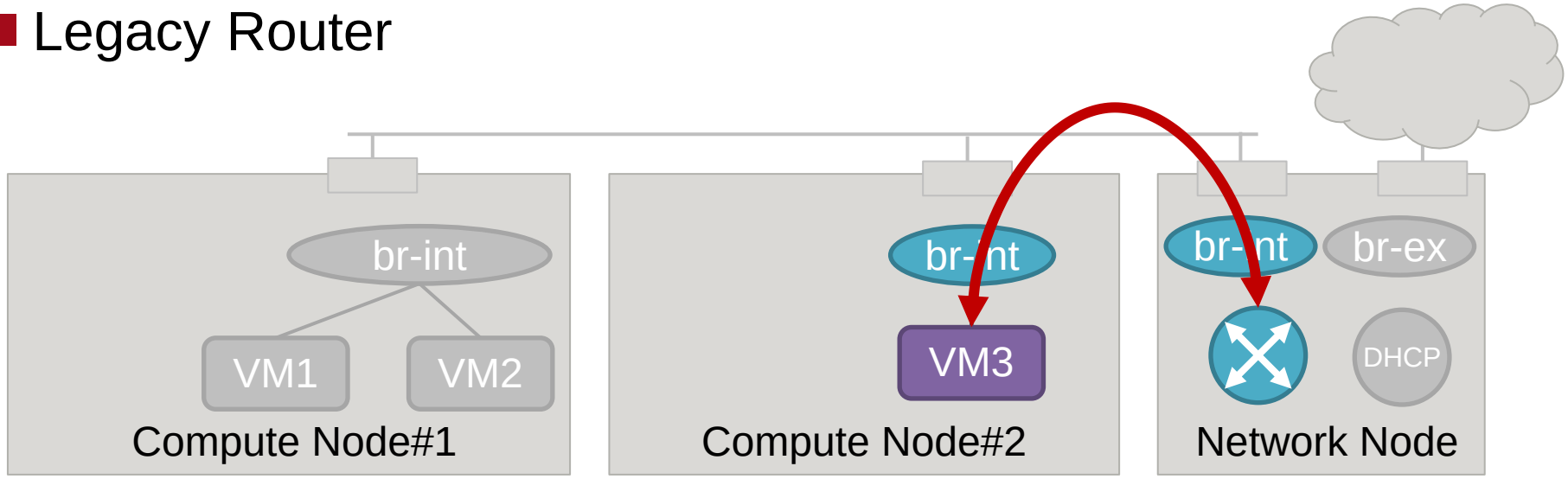


Network Traffic Case#7

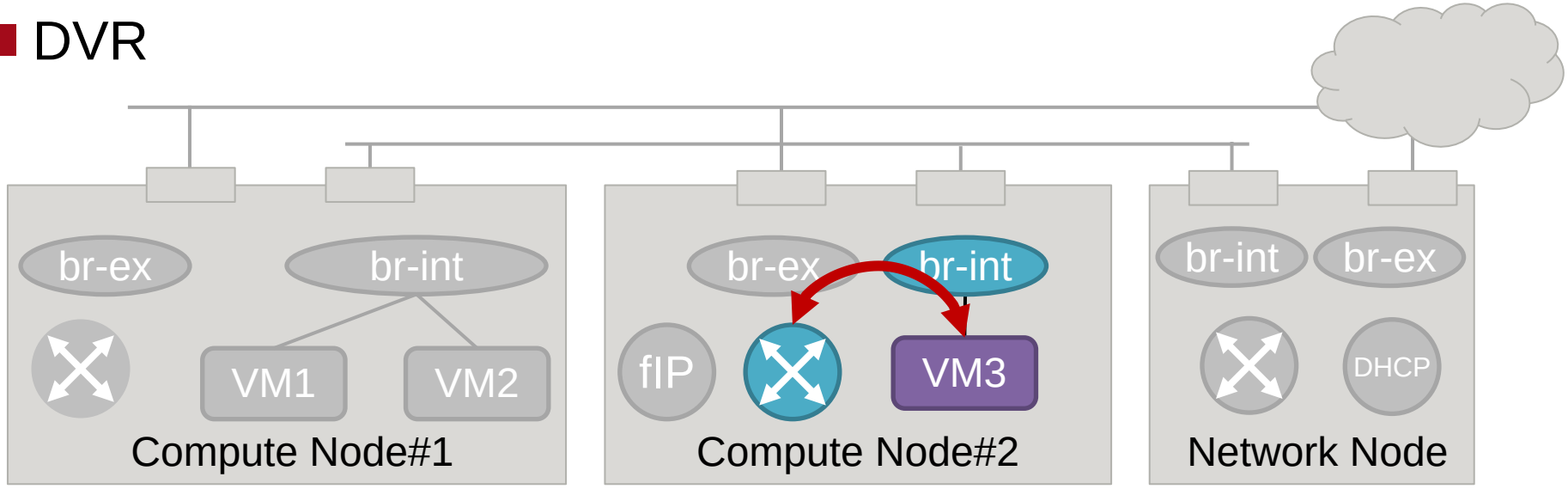
FUJITSU

VM booting: a VM gets metadata from the vRouter

- Legacy Router

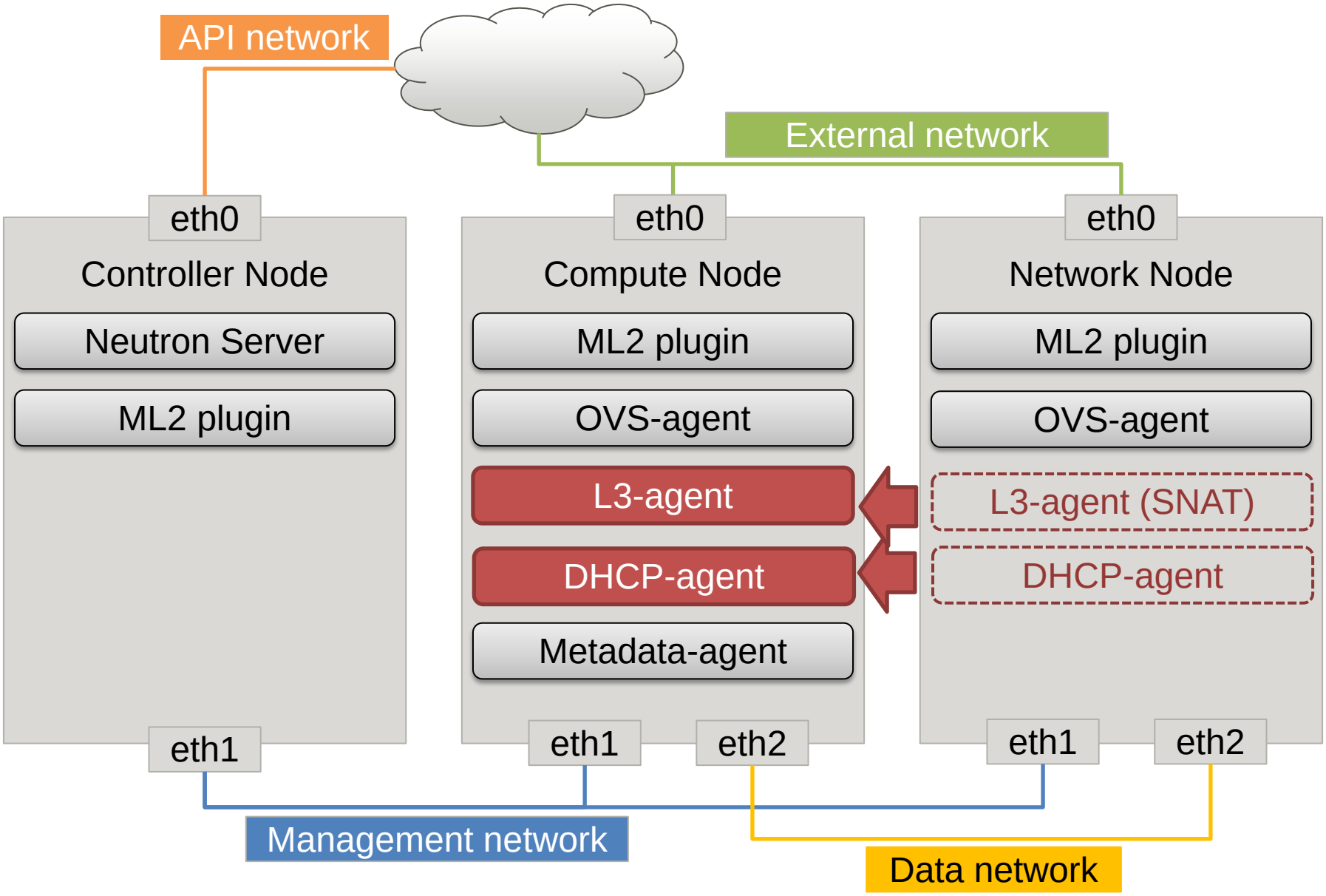


- DVR



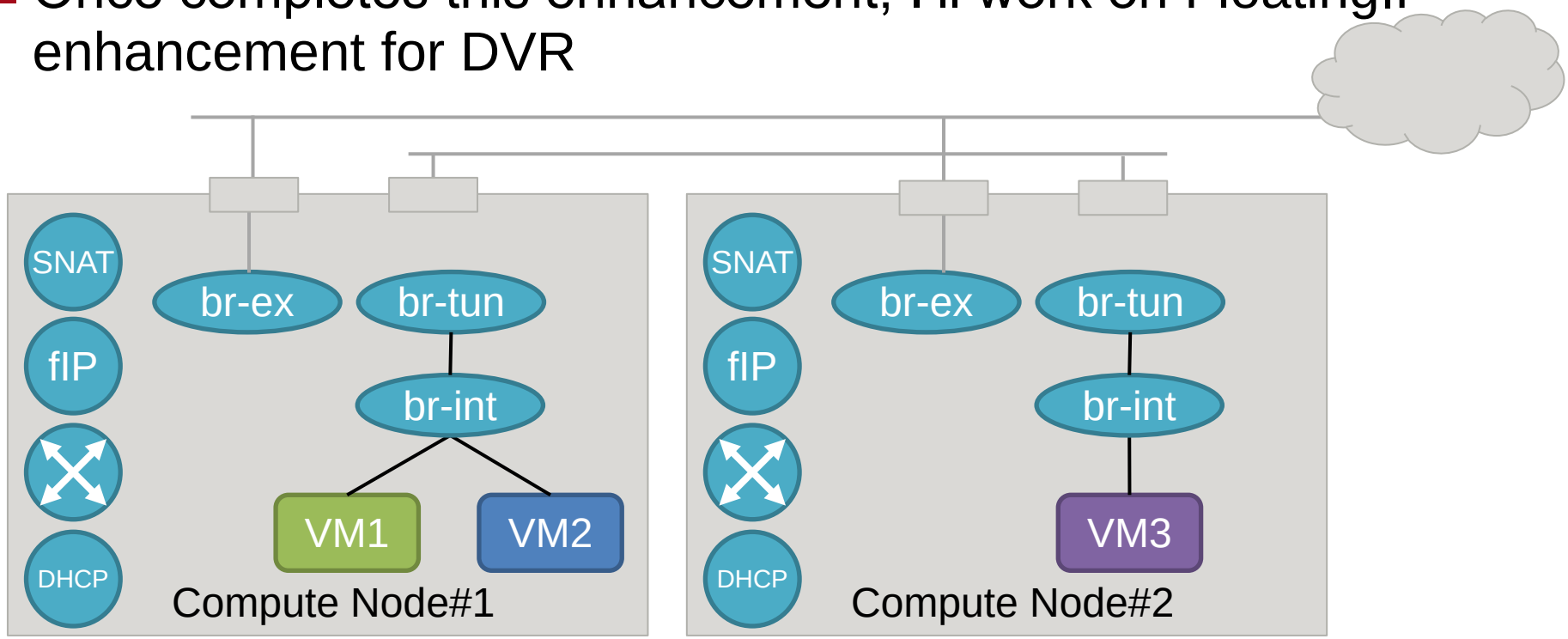
Proposal: Distributed DHCP agent and L3-agent

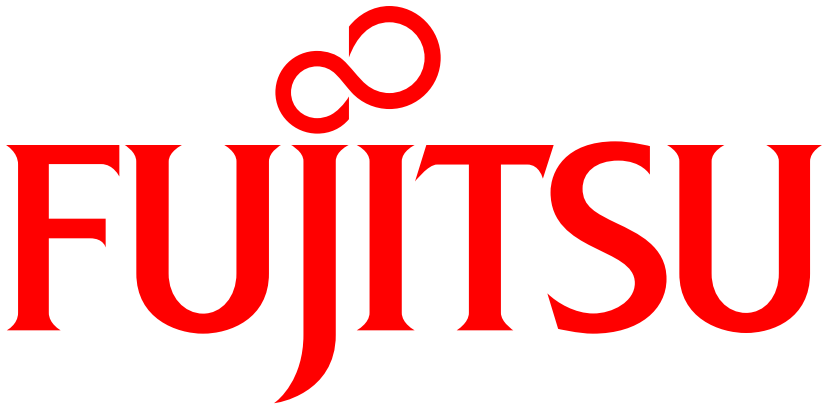
FUJITSU



Elimination of Network Node

- Distribute DHCP-agent to each Compute Node.
  => Reduce DHCP broadcast in Data Network
- Move SNAT function to Compute Node.
  => Can eliminate Single-point-of-failure
- Once completes this enhancement, I'll work on FloatingIP enhancement for DVR





shaping tomorrow with you