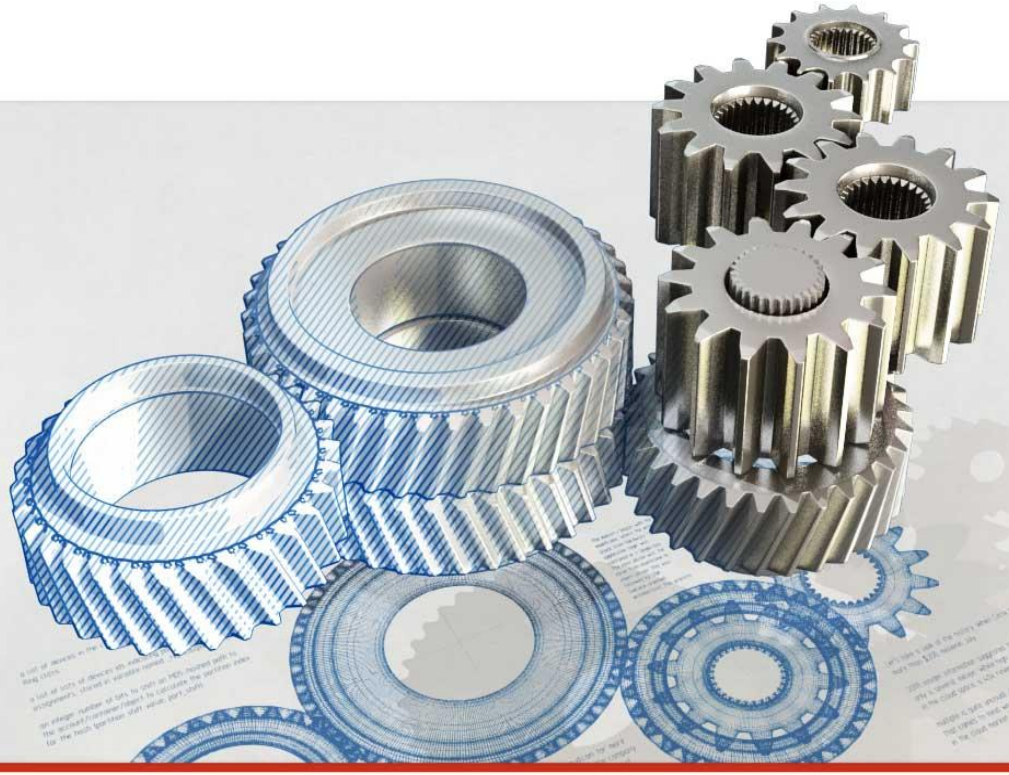
MIRANTIS

OpenStack Networking



Ilya Shakhat

Mirantis, 2013

Agenda

- What is OpenStack
- Nova network
- (Quantum) OpenStack Networking
- Open vSwitch
- Load balancing as a service

MIRANTIS

What is OpenStack?

- **Open source system for building scalable private and public clouds**
- Launched in 2010 by NASA and Rackspace, now 150+ companies, >9000 people, 87 countries
- A collection of “cloud services”
- Each service includes:
  - A tenant-facing API that exposes logical abstractions for consuming the service.
  - One or more backend implementations of that API

MIRANTIS

Agenda

- What is OpenStack
- Nova network
- (Quantum) OpenStack Networking
- Open vSwitch
- Load balancing as a service

MIRANTIS

Nova Network

Very easy to configure

Different managers (network providers):

- FlatManager
- FlatDHCPManager
- VlanManager

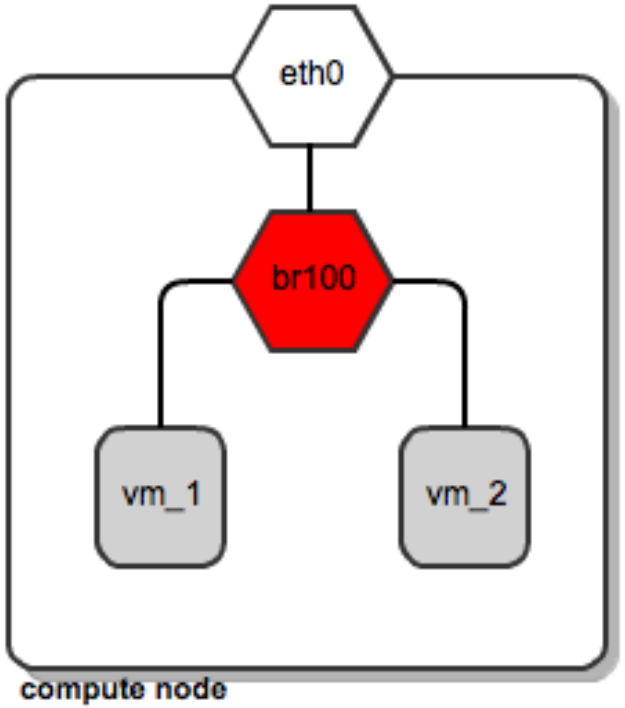
MIRANTIS

Flat Network

- Network bridge
- 'dnsmasq' DHCP server
- Bridge as default gw

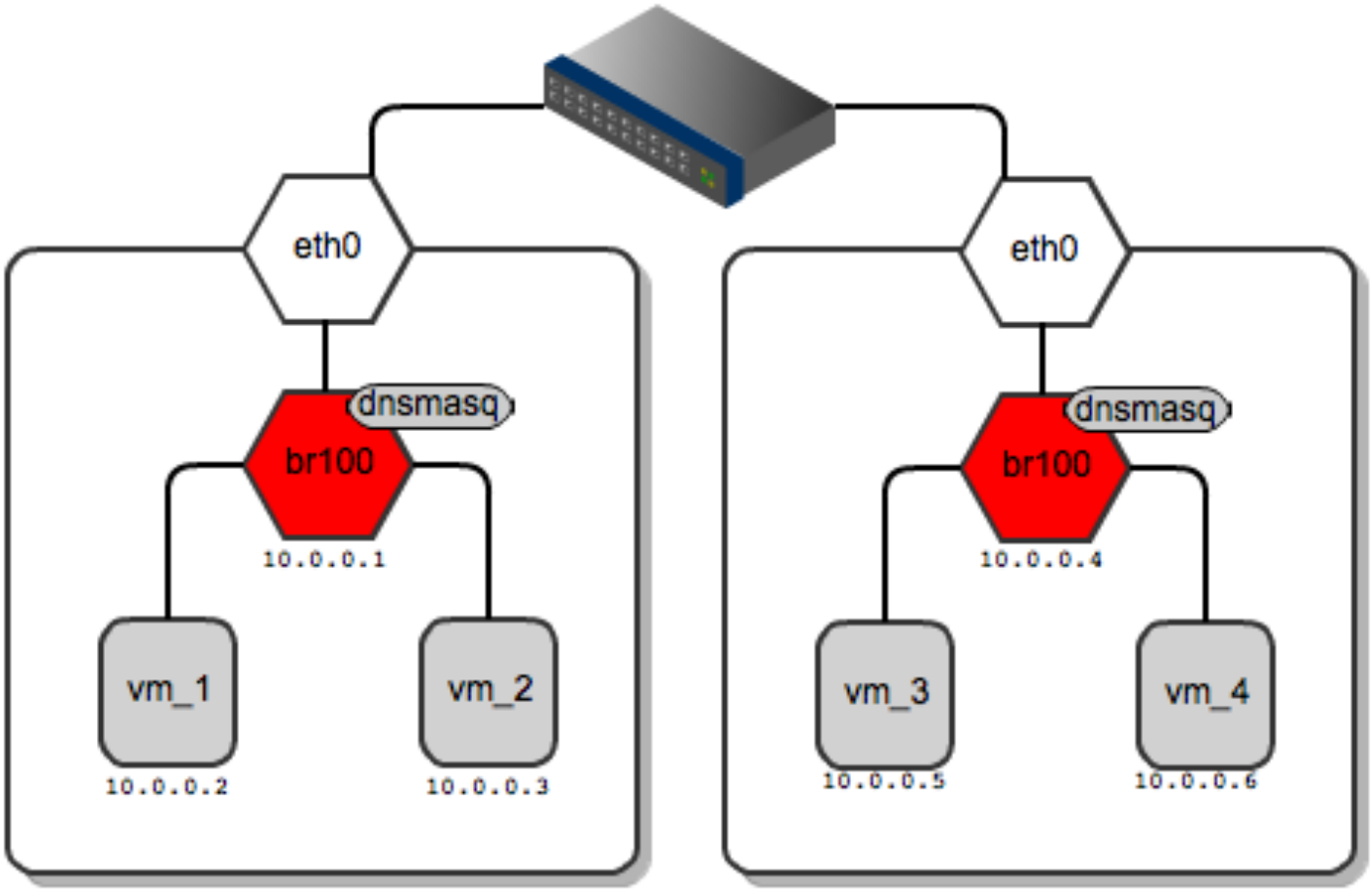
Limitations:

- Single L2 domain and ARP space, no tenant isolation
- Single IP pool



MIRANTIS

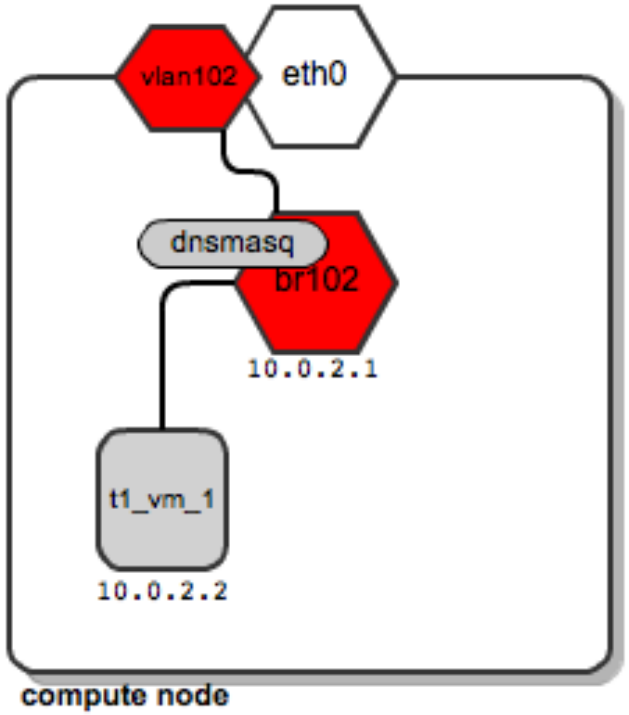
Flat Network Deployment



MIRANTIS

Vlan Network

- Network bridge
- Vlan interface over physical interface

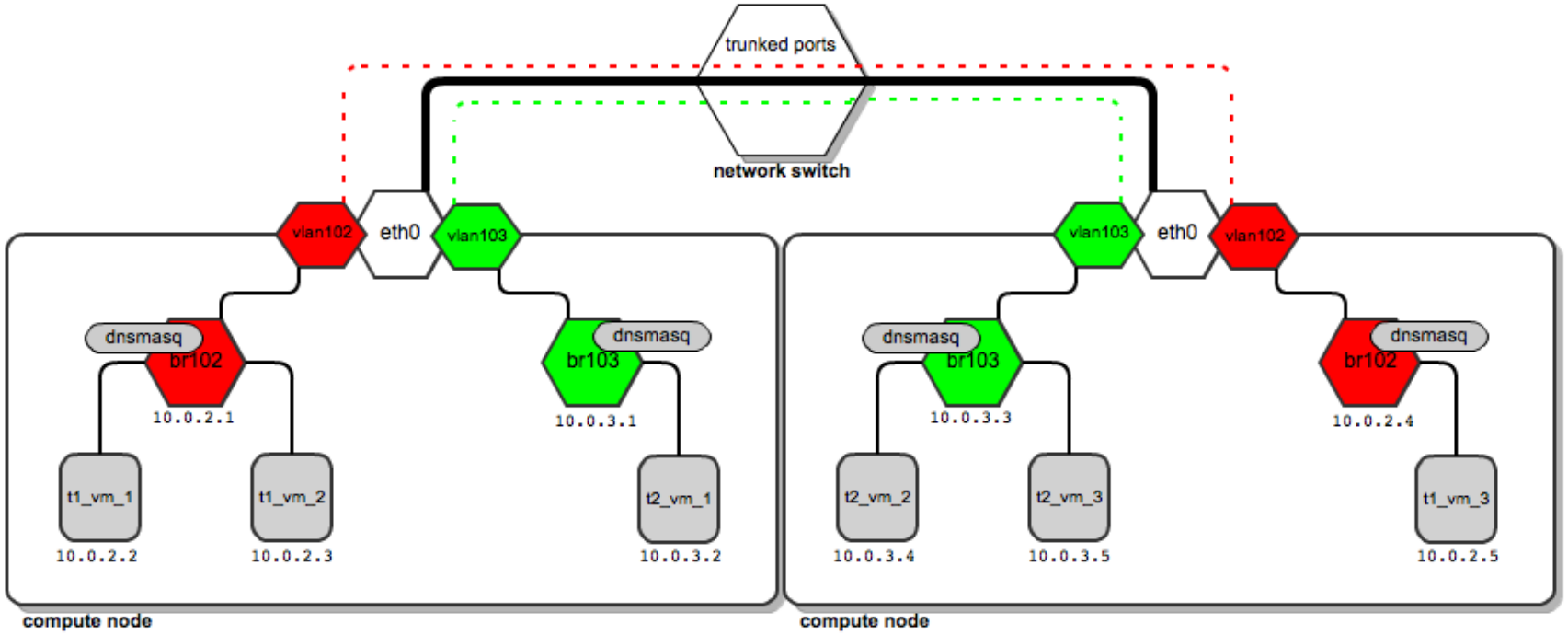


Limitations:

- Scaling limit in 4k vlan tags
- Vlans are configured manually on switch by admin
- May have issues with overlapping MACs

MIRANTIS

Vlan Network Deployment



MIRANTIS

Why new module?

- Networking is too tied to Nova
- Two Key Problems:

  1: Limited technology

  2: Tenants want to replicate rich enterprise network topologies

VLANs are Great!
- Stone Age Man

MIRANTIS

Limited technologies

Issues:

- VLANs is the only way of doing multi-tenancy
- Only Linux bridge supported (no ACLs, QoS, monitoring)
- Network controller is single point of failure

Solution:

- Software-defined Networking (SDN) / OpenFlow
- Overlay tunneling: VXLAN, NVGRE, STT
- Fabric solutions: FabricPath, Qfabric, etc.
- Pluggable mechanism via common API to enable different vendor technologies

MIRANTIS

Tenants want control

Issues:

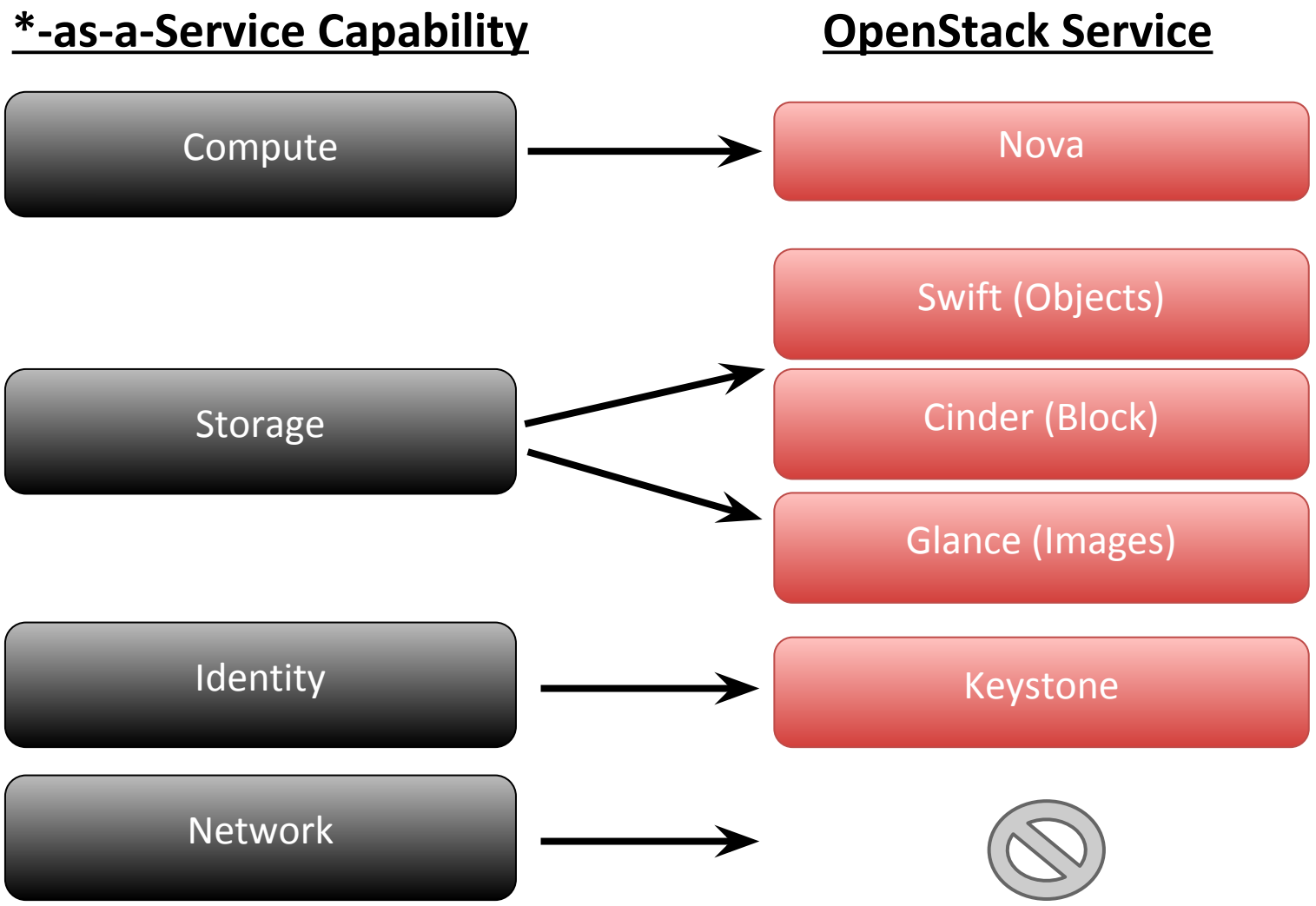
- No way to control topology nor create “multi-tier” networks
- No control over IP addressing
- No way to insert own services (e.g. firewall, IPS)

Solution:

- API for managing multiple private networks, IP addressing
- API extensions to control: security policies, quality-of-service, monitoring
- Service plugins such as firewall, intrusion detection, VPN

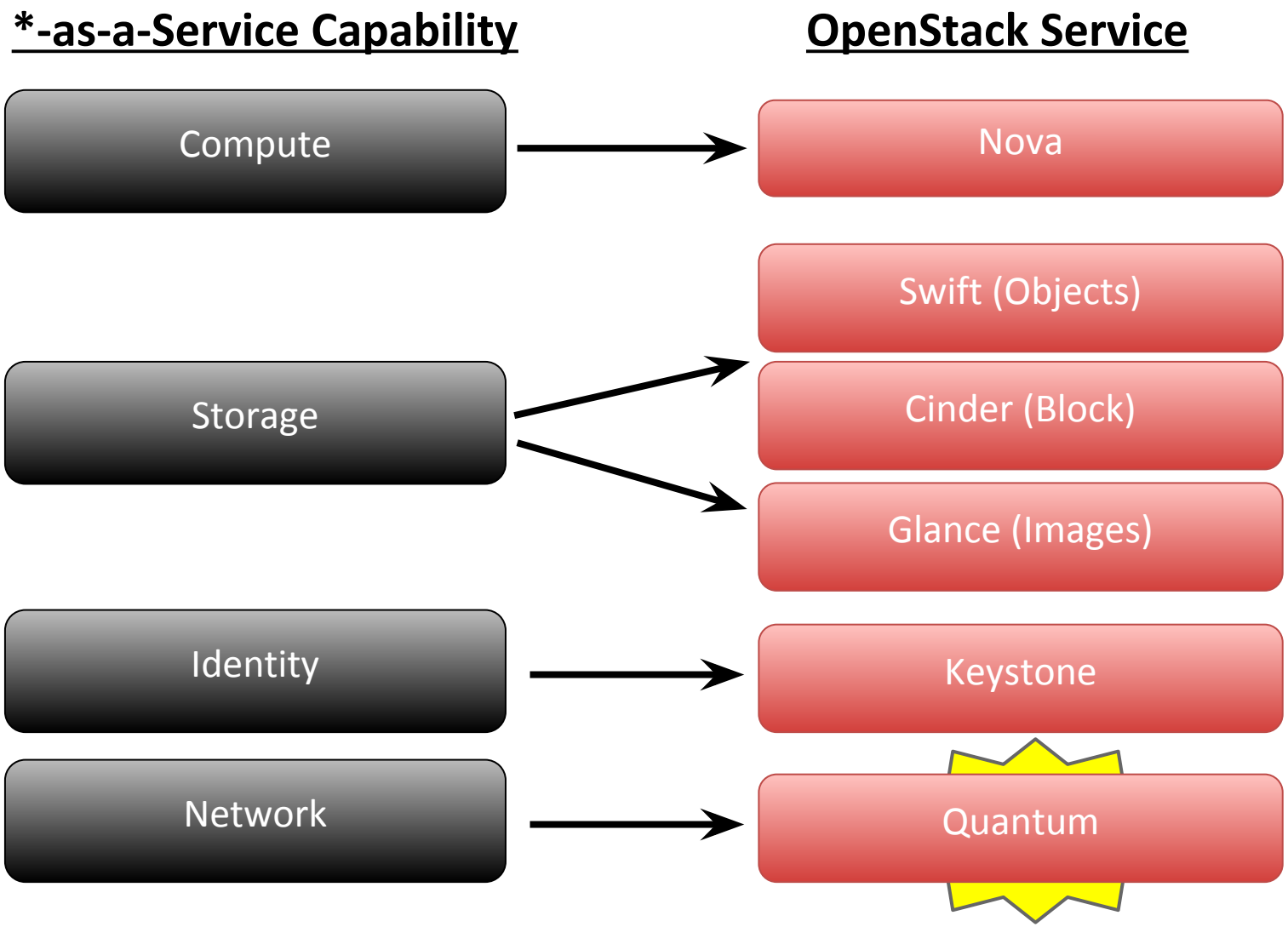
MIRANTIS

OpenStack Modules .. before



MIRANTIS

OpenStack Modules .. now



MIRANTIS

Agenda

- What is OpenStack
- Nova network
- (Quantum) OpenStack Networking
- Open vSwitch
- Load balancing as a service

MIRANTIS

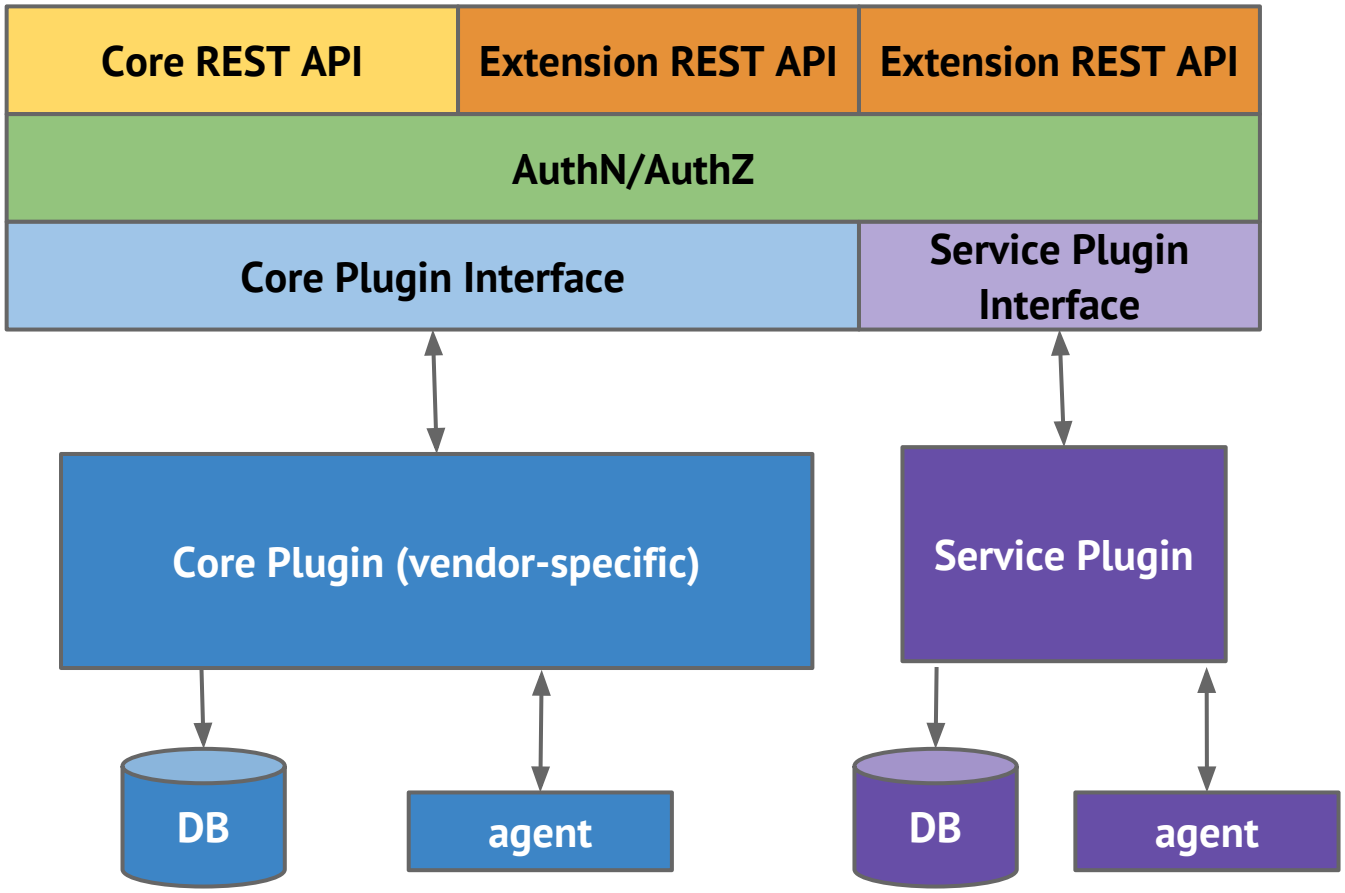
Welcome Quantum*!

- API to build rich networking topologies
- Extensible via plugins (may support virtual networks, hardware or mixed)
- More capabilities (QoS, security groups)
- Platform for services (LBaaS, FWaaS, etc)

* urgently renamed to OpenStack Networking due to trademark violation

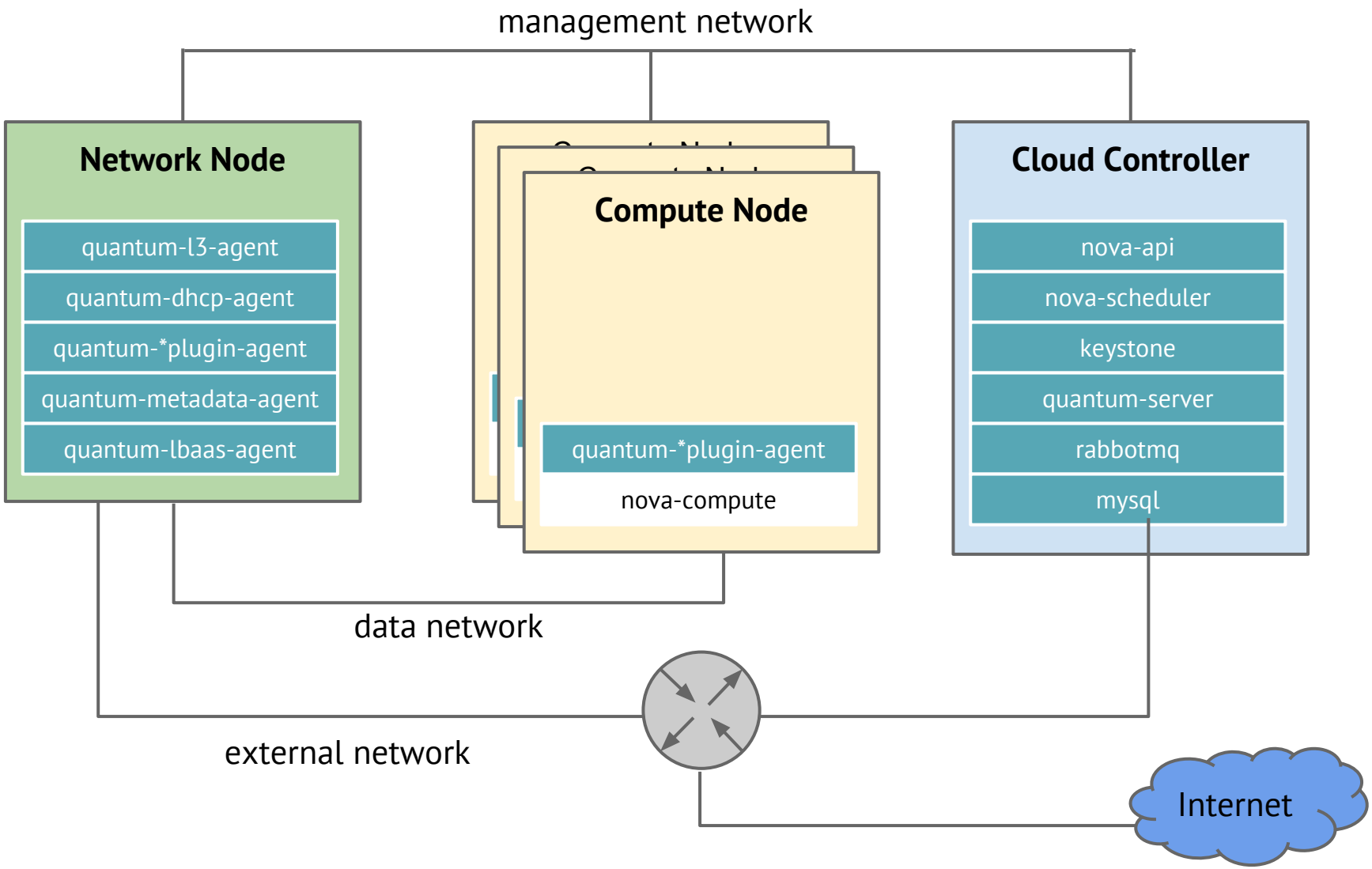
MIRANTIS

Quantum Architecture



MIRANTIS

Quantum Deployment



Quantum Objects

Core API objects

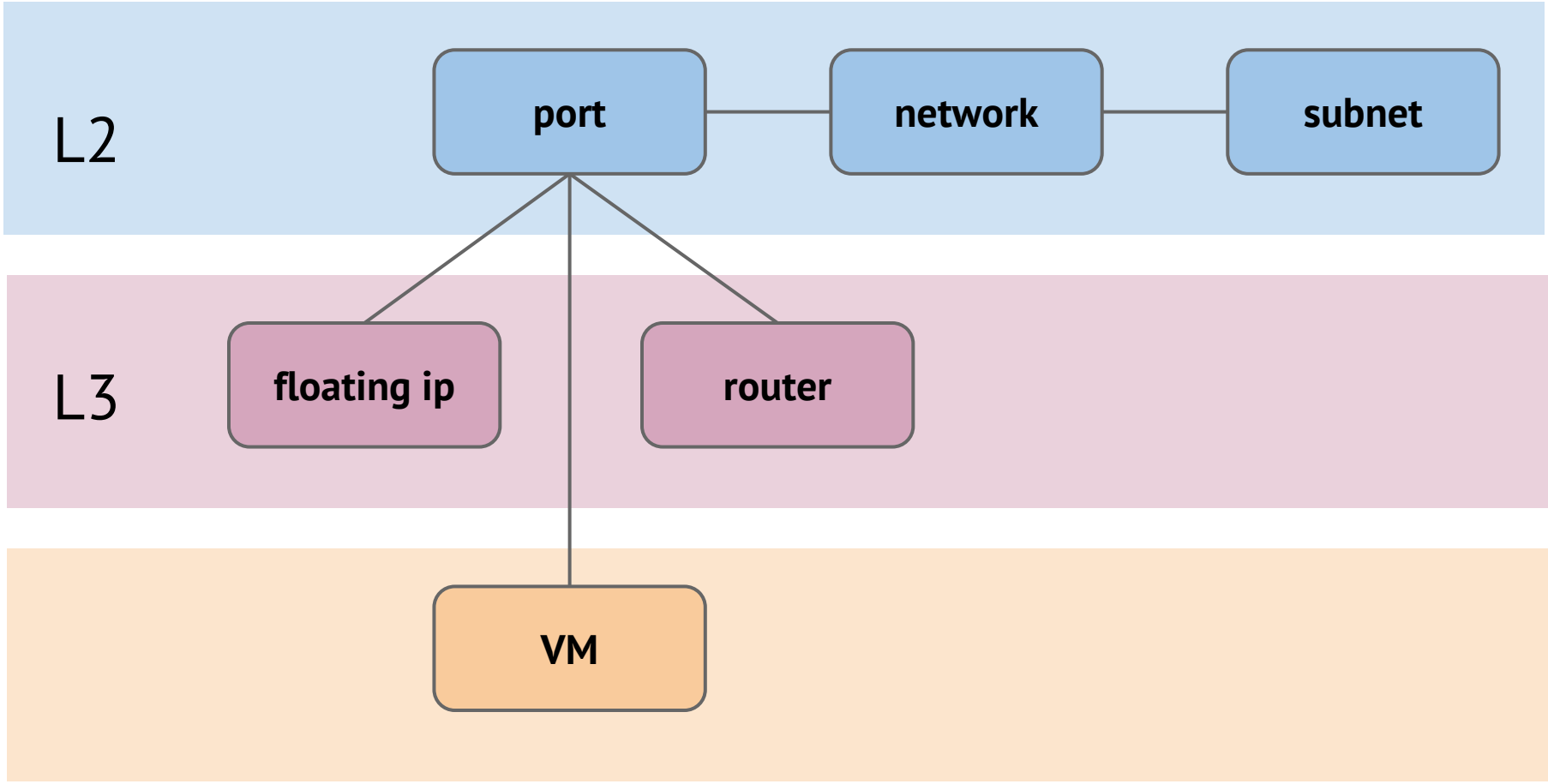
- Port - a point of attachment to network
- Network - isolated L2 network segment
- Subnet - associates a block of IP addresses with network

L3 extension objects

- Router - gateway between networks
- Floating IP - static mapping from public IP in external network to private IP in local

MIRANTIS

Quantum Object Relations



MIRANTIS

Core Plugins

- Big Switch Networks
- Brocade
- Cisco
- Hyper-V
- Linux Bridge
- Meta Plugin
- Midokura Midonet
- NEC OpenFlow
- Nicira NVP
- Open vSwitch
- PLUMgrid
- Ryu OpenFlow

MIRANTIS

Software Defined Networks

- Programmable packet forwarding and network topology configuration
- An external ‘controller’ component sets up flows and/or topologies for network traffic
- Particularly suitable for virtual networking in massively scalable environments

MIRANTIS

Agenda

- What is OpenStack
- Nova network
- (Quantum) OpenStack Networking
- Open vSwitch
- Load balancing as a service

MIRANTIS

Open vSwitch

- Open source programmable virtual switch
- Supports OpenFlow, 802.1Q VLANs, LACP, STP
- Supports KVM and Xen
- OVS is the basis for different SDN/network virtualization platforms
- Flexible controller in user-space
- Fast datapath in kernel

MIRANTIS

Open vSwitch Concepts

- Port may have more than one interface
- IEEE 802.1Q support attaching VLAN tags to interfaces
- Packets are forwarded by flow
- Fine-grained ACLs and QoS (L2-L4 matching, actions)
- Centralized control via OpenFlow
- Works on Xen, KVM, VirtualBox

MIRANTIS

Open vSwitch Tools

ovs-vswitchd - daemon that implements a switch with help of kernel module

ovsdb-server - database server

ovs-vsctl - utility for working with the configuration

ovs-appctl - tool for controlling Open vSwitch daemon

ovs-dpctl - datapath management utility

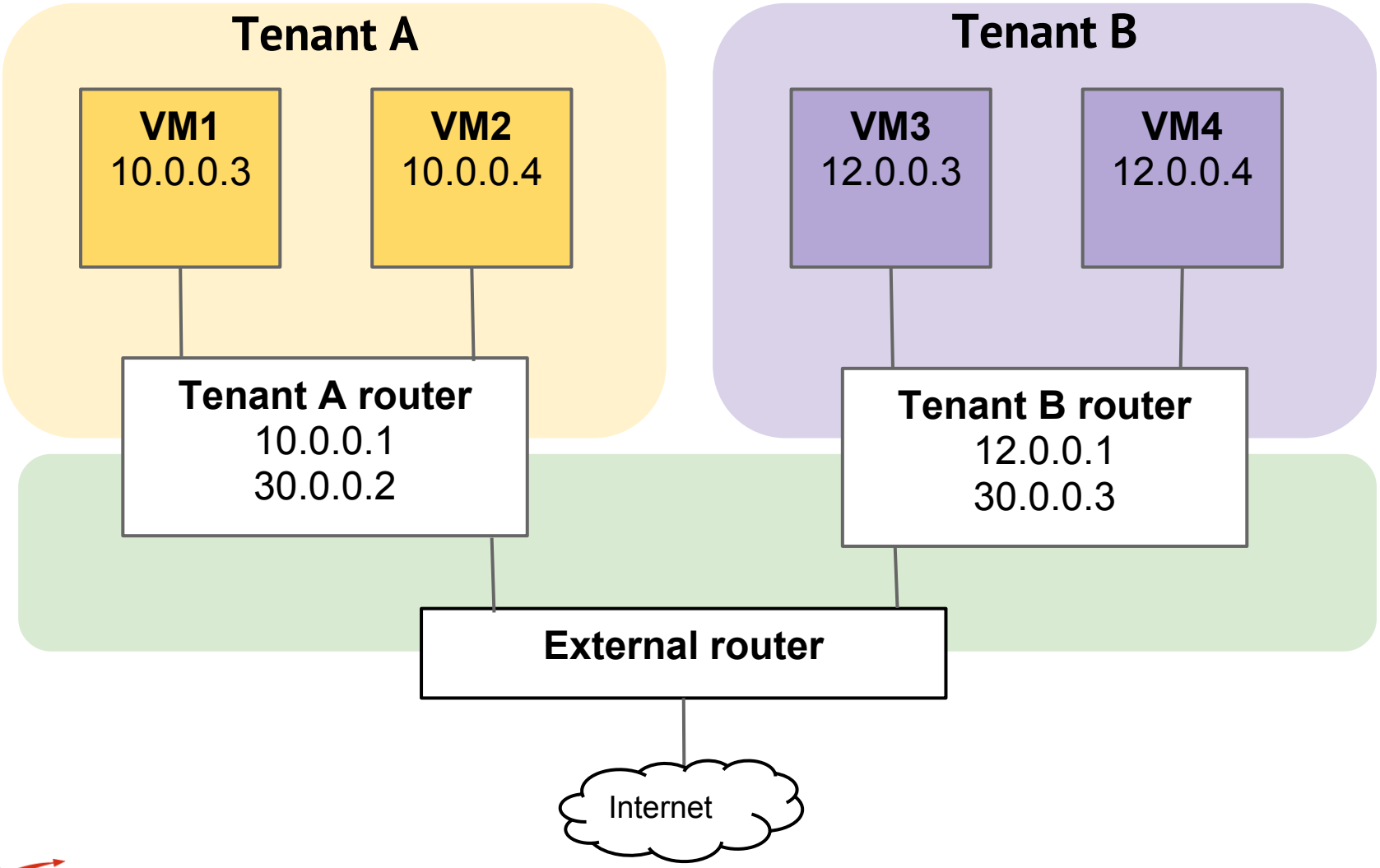
ovs-controller - simple OpenFlow controller

ovs-ofctl - OpenFlow switch management utility

ovs-pki - utility for managing public-key infrastructure

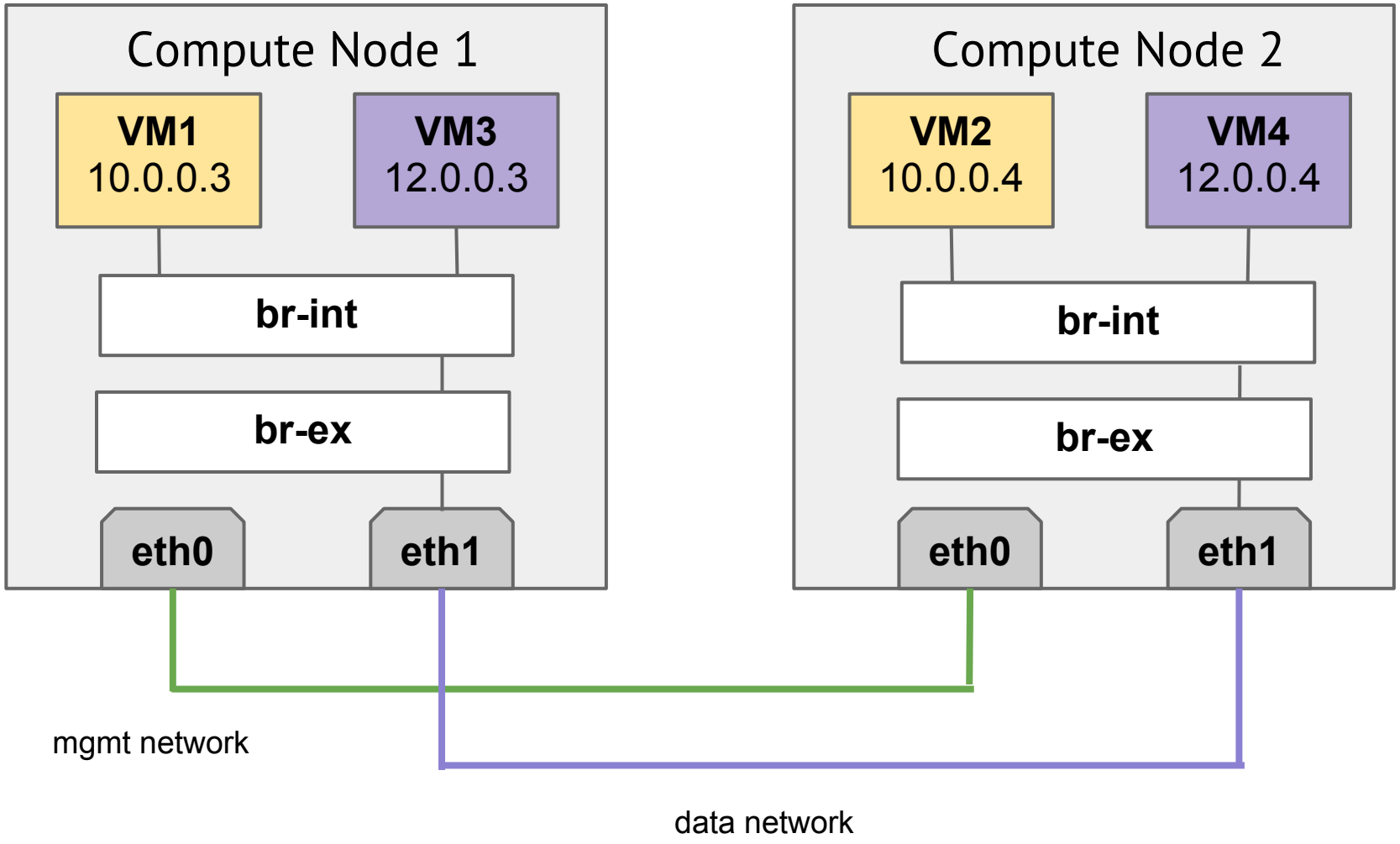
MIRANTIS

Example: logical view



MIRANTIS

Example: physical view



MIRANTIS

Let's Start (with example)!

We have:

- tenant A and network (10.0.0.0/24)
- router that wires private network with external
- DCHP enabled (quantum port is create)

Commands we need:

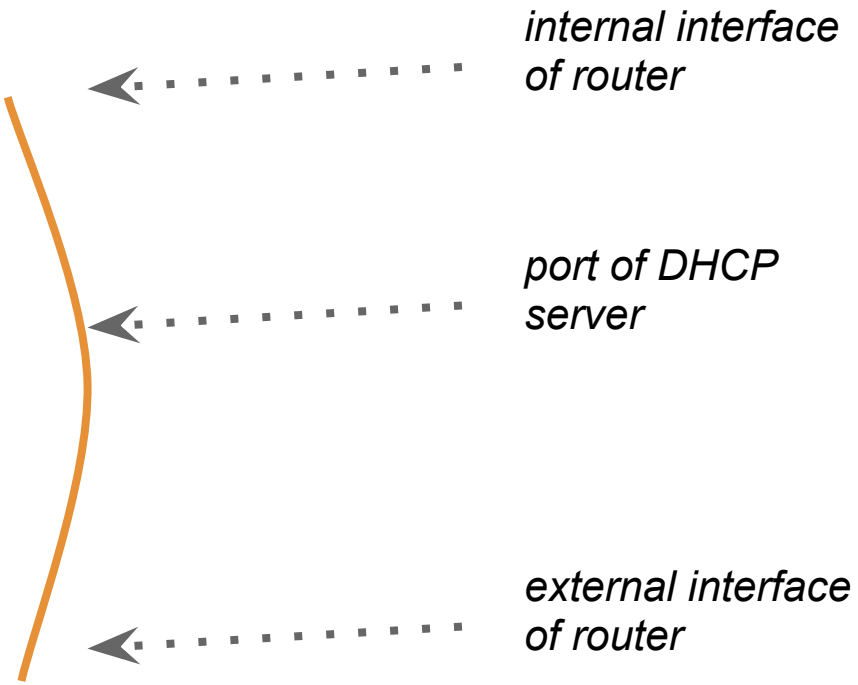
- **brctl show** - to show all bridges
- **ovs-vsctl show** - to show all interfaces
- **ip netns exec** - to show contents of namespace
- **quantum port-list, quantum net-list**

MIRANTIS

ovs-vsctl show

```
Bridge br-int
    Port "qr-9b80a882-55"
        tag: 1
        Interface "qr-9b80a882-55"
            type: internal
    Port "tap66a249f1-bf"
        tag: 1
        Interface "tap66a249f1-bf"
            type: internal
    Port br-int
        Interface br-int
            type: internal

Bridge br-ex
    Port "qg-e41c368d-a8"
        Interface "qg-e41c368d-a8"
            type: internal
    Port br-ex
        Interface br-ex
            type: internal
```



MIRANTIS

brctl show

```
bridge name     bridge id           STP enabled     interfaces

br-ex           0000.6eed69b21a4b   no              qg-e41c368d-a8

br-int          0000.f68d58076046   no              qr-9b80a882-55
                                                    tap66a249f1-bf
```

MIRANTIS

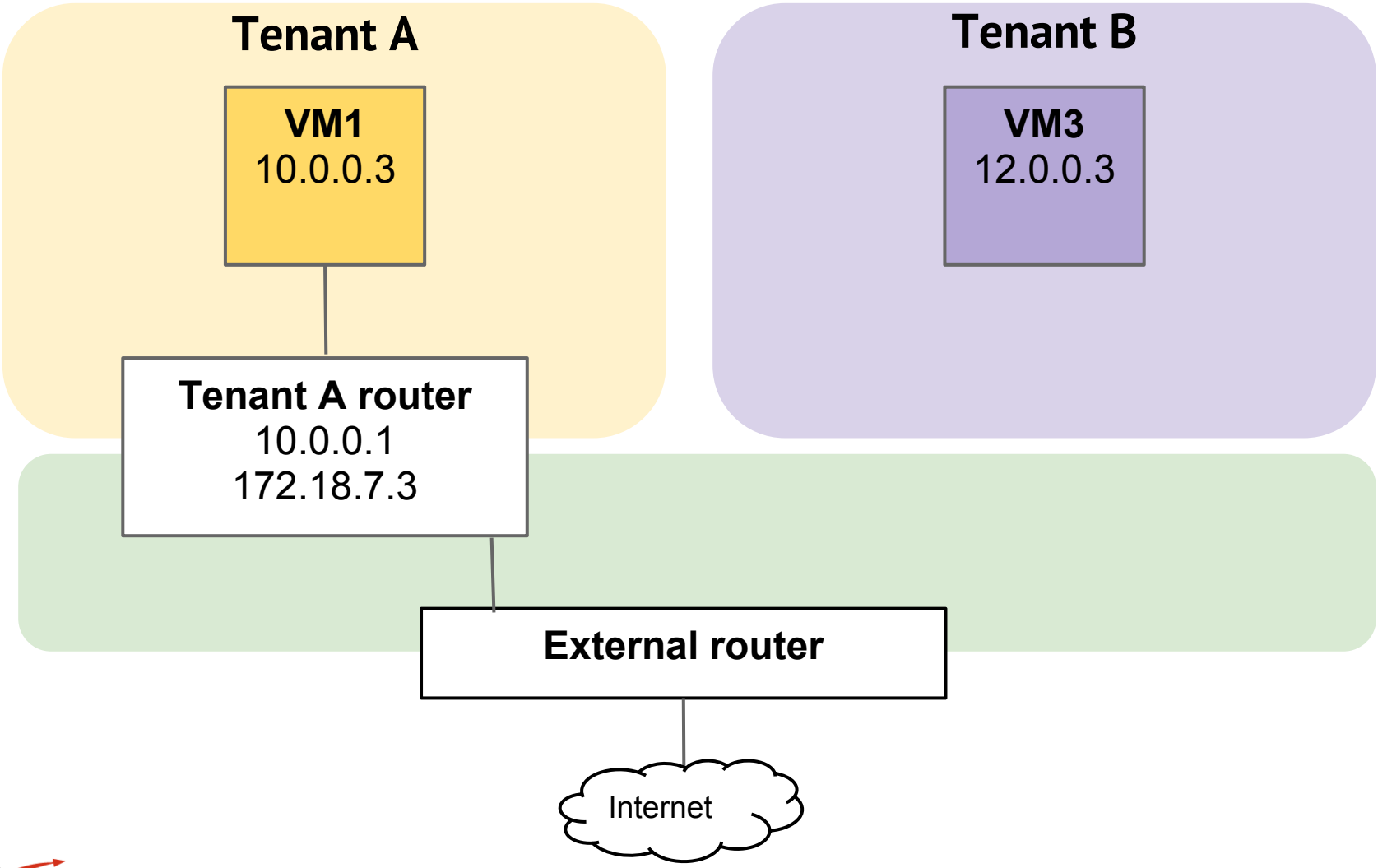
Let's Rock!

Expand the configuration:

- Launch VM in tenant A (10.0.0.3)
- Create network for tenant B (12.0.0.0/24)
  with DHCP enabled (12.0.0.2)
  but without router
- Launch VM in tenant B (12.0.0.3)

MIRANTIS

logical view



MIRANTIS

ovs-vsctl show

```
Bridge br-int
     Port "qvo8b0b577a-2c"
          tag: 1
          Interface "qvo8b0b577a-2c"
     Port "qr-9b80a882-55"
          tag: 1
          Interface "qr-9b80a882-55"
               type: internal
     Port "tap66a249f1-bf"
          tag: 1
          Interface "tap66a249f1-bf"
               type: internal
     Port "qvo4a744a65-92"
          tag: 2
          Interface "qvo4a744a65-92"
     Port "tap3aa4a560-d2"
          tag: 2
          Interface "tap3aa4a560-d2"
               type: internal
     Port br-int
          Interface br-int
               type: internal
```

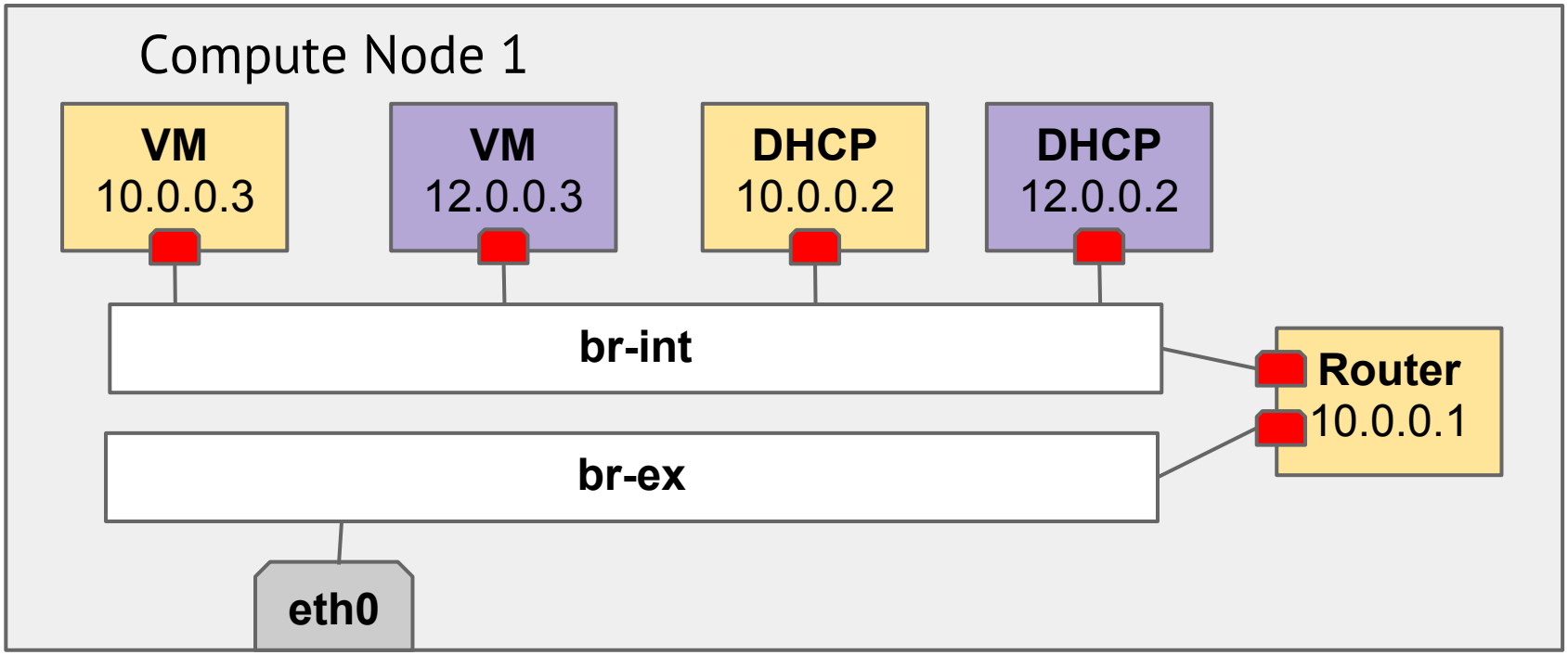
interface for VM in tenant A

interface for VM in tenant B

interface of DHCP server in tenant B

MIRANTIS

physical view



MIRANTIS

brctl show

```
bridge name     bridge id           STP enabled     interfaces

br-ex           0000.6eed69b21a4b   no              qg-e41c368d-a8

br-int          0000.f68d58076046   no              qr-9b80a882-55
                                                    qvo4a744a65-92
                                                    qvo8b0b577a-2c
                                                    tap3aa4a560-d2
                                                    tap66a249f1-bf

qbr4a744a65-92   8000.7a95a8a2b9bd   no             qvb4a744a65-92
                                                    tap4a744a65-92

qbr8b0b577a-2c   8000.de84d986f61e   no             qvb8b0b577a-2c
                                                    tap8b0b577a-2c
```

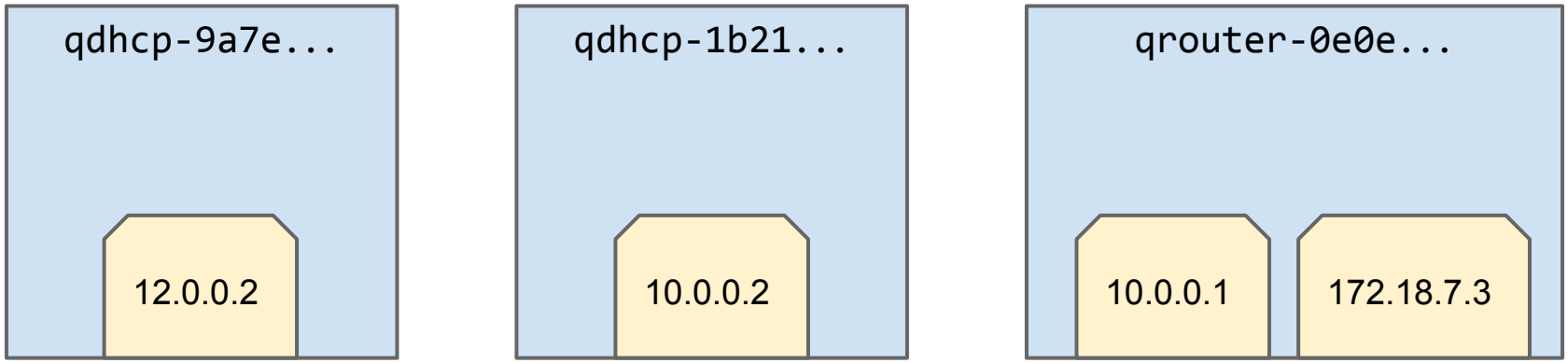
one bridge for VM
(created by VIF driver in Nova)

MIRANTIS

ip netns

List of namespaces. There's one namespace per DHCP port and per router port

```
qdhcp-9a7e9331-2508-4615-889b-b99a6f260eef
qdhcp-1b2101e0-cefa-4347-a581-e1f1f02215a1
qrouter-0e0e2e6e-a60b-4808-b914-8f45cae02b2e
```



MIRANTIS

ip netns exec <> ifconfig

Show interfaces for namespace associated with router

```
qg-e41c368d-a8 Link encap:Ethernet  HWaddr fa:16:3e:27:a1:85
        inet addr:172.18.7.3  Bcast:172.18.76.135  Mask:255.255.255.248
        inet6 addr: fe80::f816:3eff:fe27:a185/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:60 errors:0 dropped:0 overruns:0 frame:0
        TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:6608 (6.6 KB)  TX bytes:5298 (5.2 KB)

qr-9b80a882-55 Link encap:Ethernet  HWaddr fa:16:3e:9e:ed:50
        inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
        inet6 addr: fe80::f816:3eff:fe9e:ed50/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:18878 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3958 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:3269696 (3.2 MB)  TX bytes:349880 (349.8 KB)
```

MIRANTIS

Agenda

- What is OpenStack
- Nova network
- (Quantum) OpenStack Networking
- Open vSwitch
- Load balancing as a service

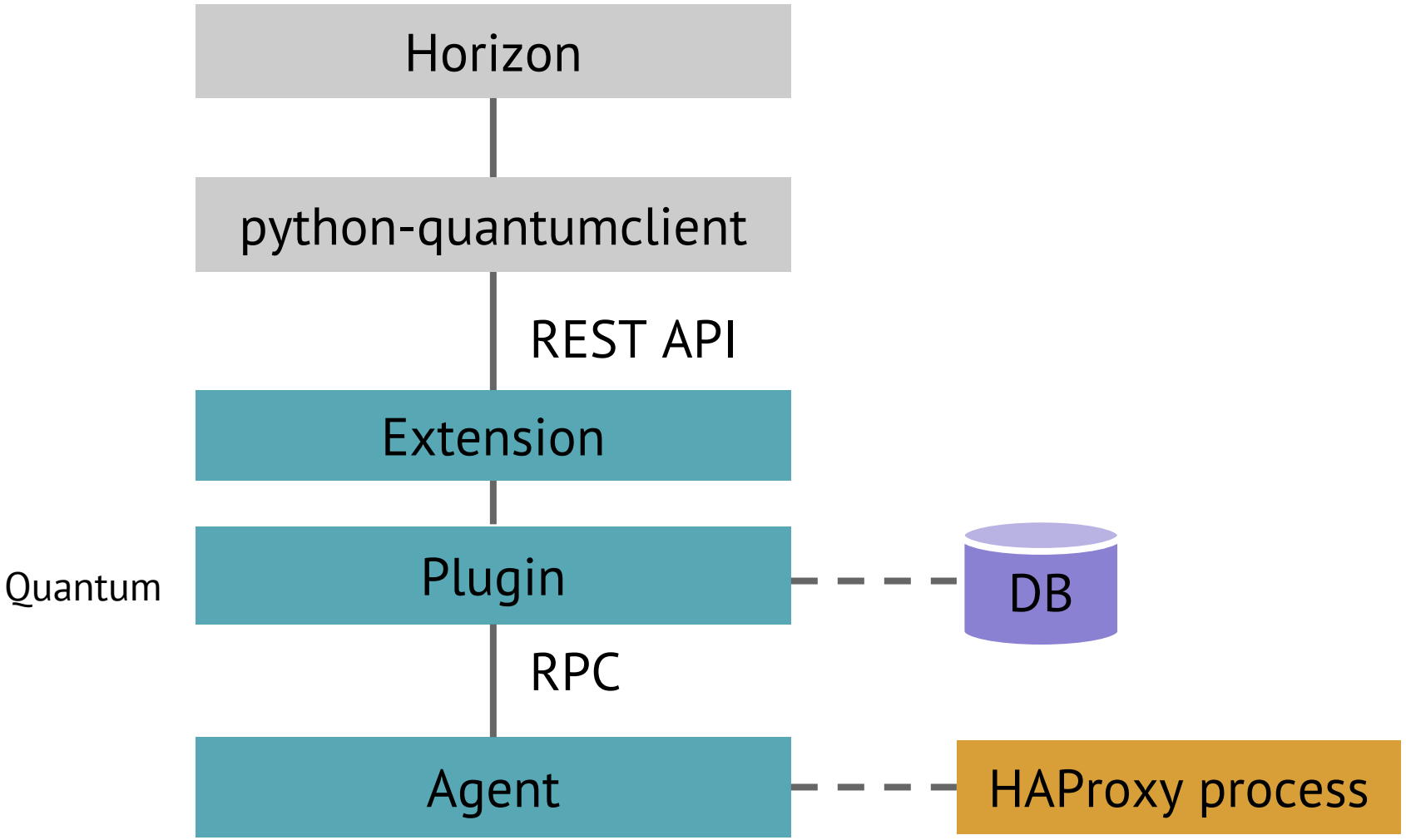
MIRANTIS

Load Balancing as a Service

- Unified API for load balancing
- Features:
  - LB between services on VMs
  - configurable LB methods (e.g. round-robin)
  - session persistence
  - health monitoring (TCP, HTTP)
- Reference implementation based on HAProxy

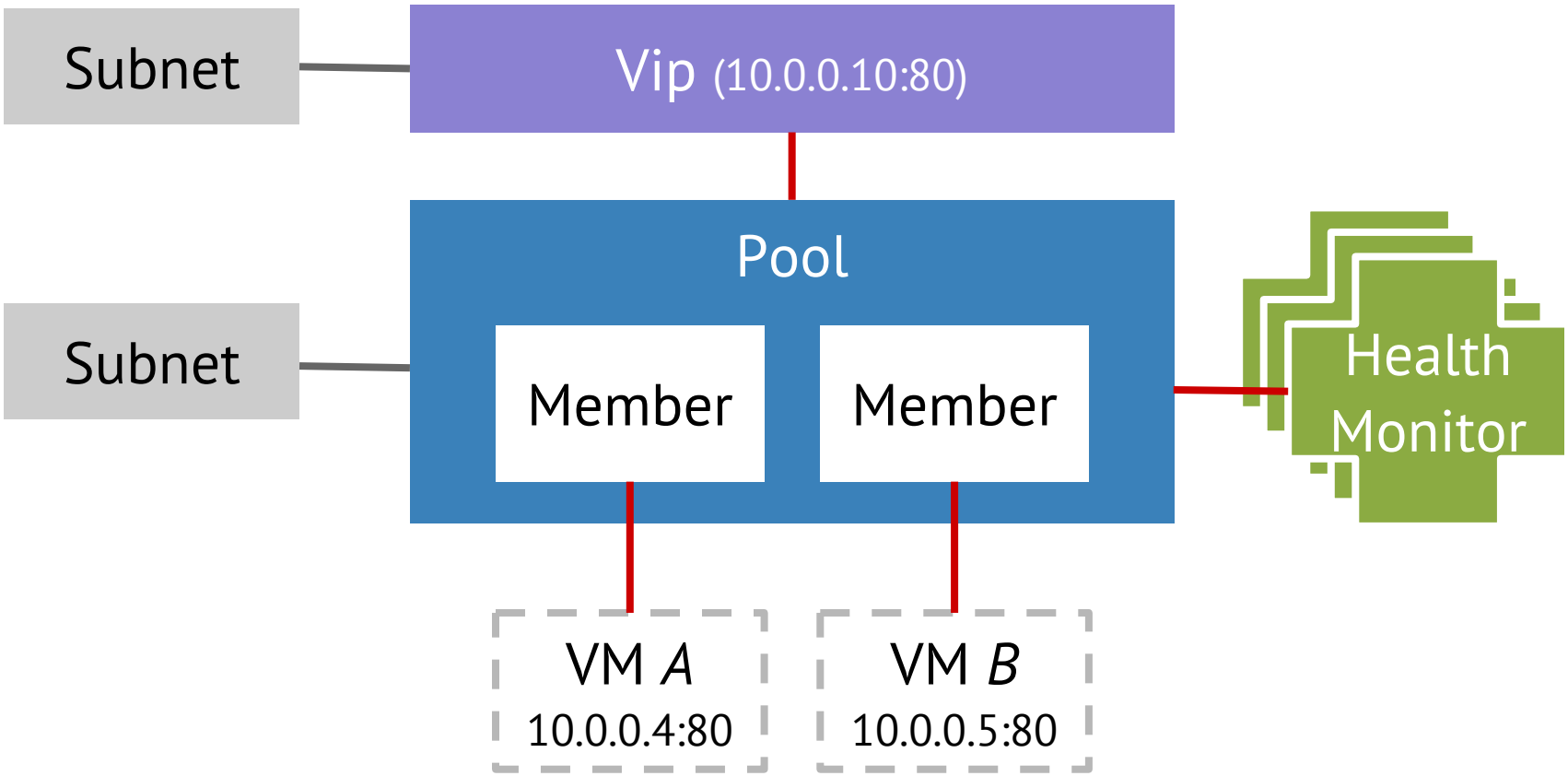
MIRANTIS

LBaaS Architecture



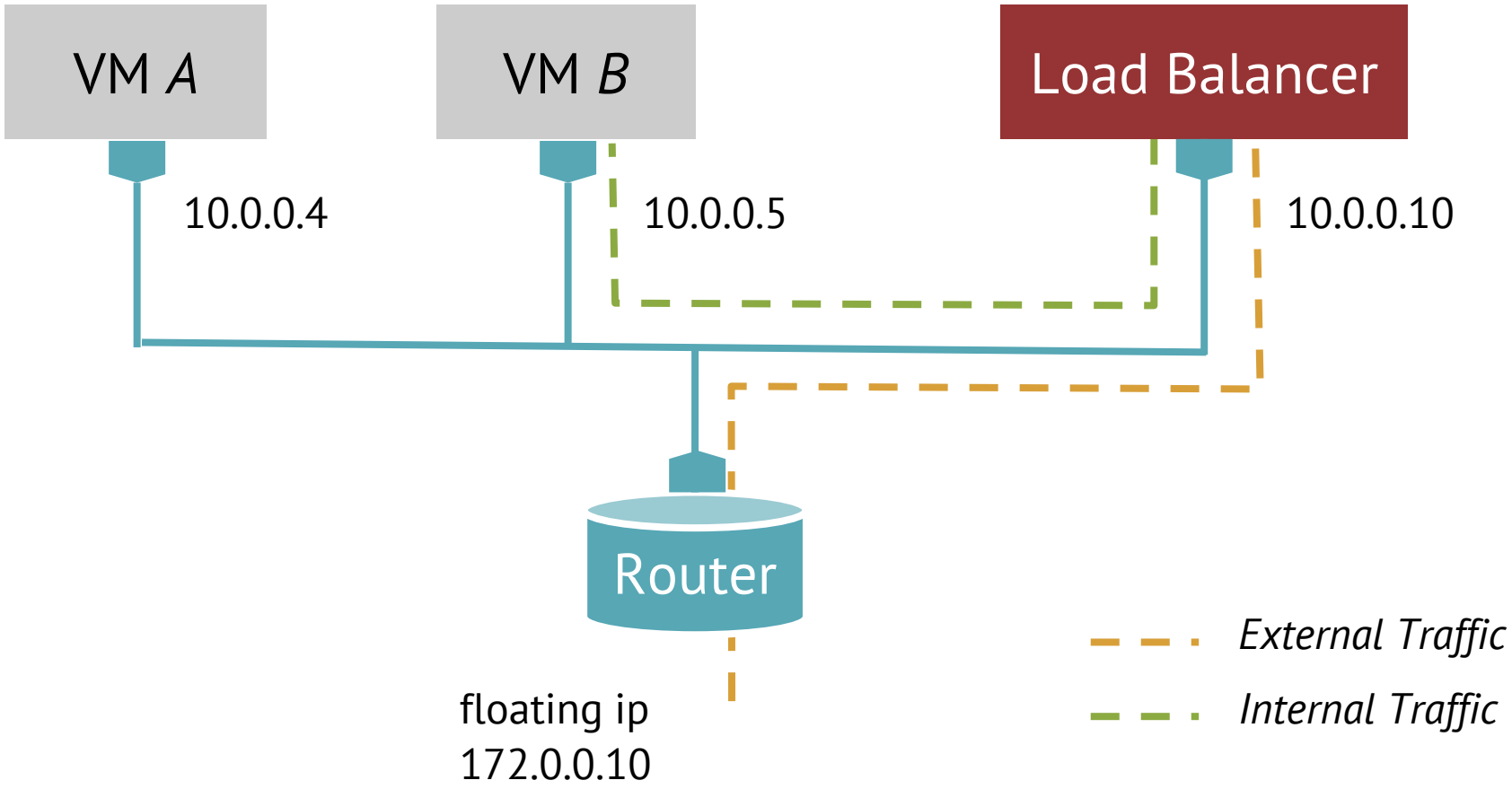
MIRANTIS

LBaaS Model



MIRANTIS

LBaaS Wiring



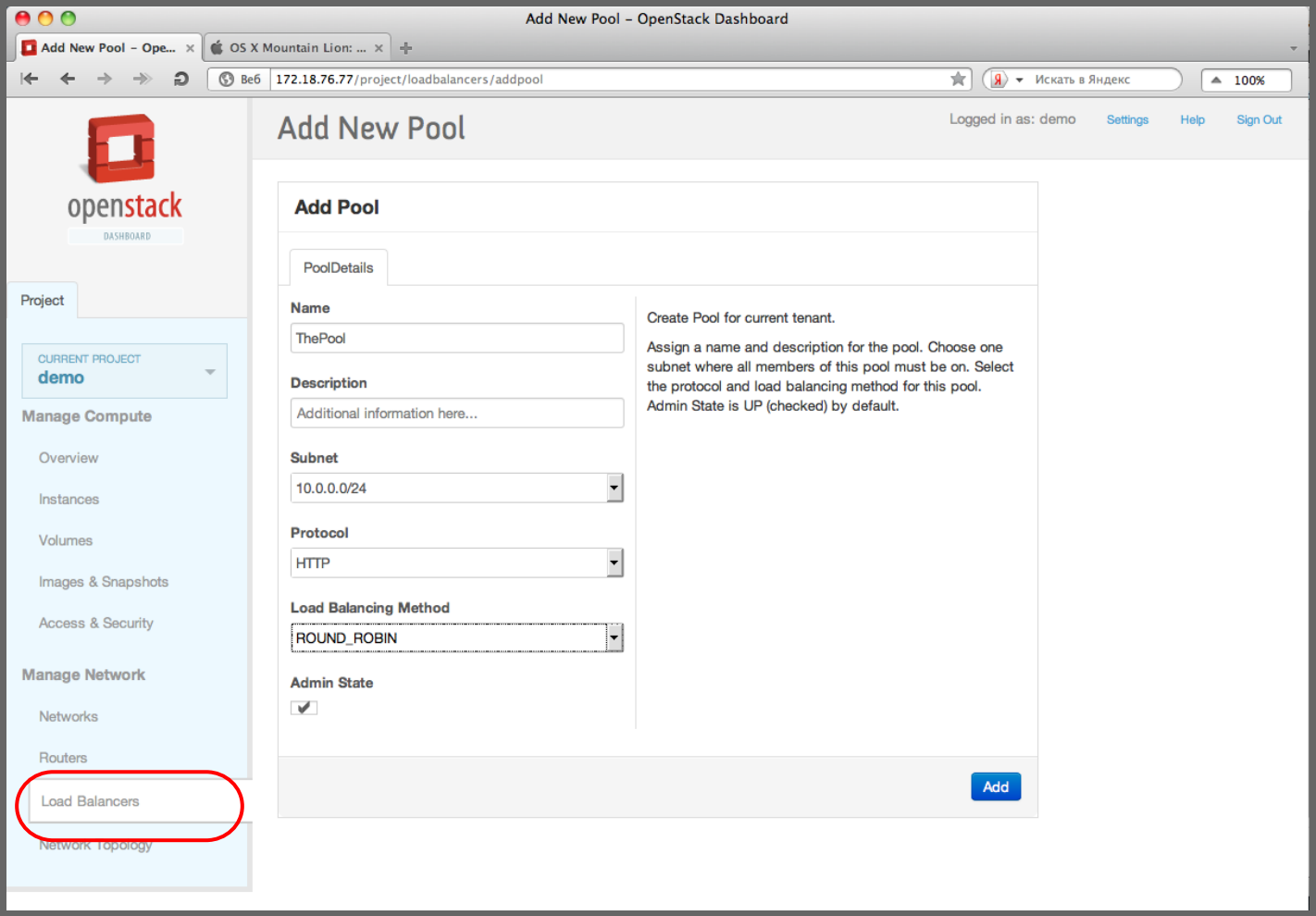
MIRANTIS

LBaaS Workflow

1. Create pool
2. Create members (1 per VM / service)
3. Create vip for the pool
4. (opt.) Create health monitor and associate with Pool

MIRANTIS

LBaaS UI



MIRANTIS

Future of OpenStack Networking

Havana Release:

- More services: firewall-as-a-service, vpn-as-a-service
- Multi-host DHCP agent (analog to Nova)
- IPv6 support for L3 services

Provide API for every service in the network!

MIRANTIS

Q&A

MIRANTIS