Openstack Administration 101
Neutron: gestione connettività servizi, reti e IP

Diego Michelotto (INFN-CNAF)

01/12/2021

Disclaimer

- Tutte le informazioni che troverete in queste slide vengono dalla documentazione ufficiale di Openstack Neutron: https://docs.openstack.org/neutron/latest/
- I concetti trattati in queste slide sono solo parziali
  - Per informazioni complete e approfondite consultare la documentazione ufficiale
- La documentazione è un labirinto:
  - Ogni link che aprite apritelo in un nuovo tab, potreste non riuscire a tornare indietro
  - Non arrendetevi!!!
- **Don't try this in production!!!**

Overview

- Networking concepts
- Neutron
- Neutron components
- Neutron network topologies
- Neutron installation and configuration
- Neutron networks
- Neutron routers
- Neutron floating IP
- Neutron security groups
- Neutron troubleshooting
- Hands-on

Networking concepts

Networking concepts

- Ethernet
- VLAN
- Subnet and ARP
- DHCP
- IP
- TCP/UDP/ICMP
- Switch
- Router
- Firewall
- Overlay protocol: GRE, VXLAN, GENEVE
- Network namespace
- NAT

Networking concepts

- **Ref:** https://docs.openstack.org/neutron/latest/admin/intro.html
- Ethernet:
  - is a **networking protocol**, specified by the IEEE 802.3 standard.
  - In the **OSI model** of networking protocols, Ethernet occupies **the second layer**, which is known as the data link layer.
  - Every host on an Ethernet network is uniquely identified by an address called the media access control (**MAC**) address.
- VLAN:
  - is a **networking technology** that enables a single switch to act as if it was multiple independent switches. Specifically, **two hosts that are connected to the same switch but on different VLANs do not see each other's traffic.**
- Subnet and ARP:
  - While NICs use MAC addresses to address network hosts, TCP/IP applications use IP addresses.
  - **The Address Resolution Protocol (ARP)** bridges the gap between Ethernet and IP by **translating IP addresses into MAC addresses.**
  - IP addresses are broken up into two parts: **a *network number* and a *host identifier***. To calculate the network number of an IP address, you must know the *netmask* associated with the address. **A netmask indicates how many of the bits in the 32-bit IP address make up the network number.**

Networking concepts

- DHCP:
  - Hosts connected to a network use the Dynamic Host Configuration Protocol (DHCP) to **dynamically obtain IP addresses.**
  - DHCP clients locate the DHCP server by sending a UDP packet from port 68 to address 255.255.255.255 on port 67. The DHCP server must be on the same local network as the client. The DHCP server responds by sending a UDP packet from port 67 to port 68 on the client with the IP configuration.
- IP:
  - The Internet Protocol (IP) specifies **how to route packets between hosts that are connected to different local networks.** In the OSI model of networking protocols IP occupies the **third layer.**
- TCP/UDP/ICMP:
  - For networked software applications to communicate over an IP network, they must use a protocol layered atop IP. These protocols occupy the fourth layer of the OSI model
  - The *Transmission Control Protocol* (TCP) is the most commonly used layer 4 protocol in networked applications. **TCP is a *connection-oriented* protocol**: it uses a client-server model where a client connects to a server.
  - The *User Datagram Protocol* (UDP) is another layer 4 protocol that is the basis of several well-known networking protocols. UDP is a *connectionless* protocol: **two applications that communicate over UDP do not need to establish a connection** before exchanging data. UDP is also an ***unreliable* protocol.**
  - The *Internet Control Message Protocol* (ICMP) is a **protocol used for sending control messages** over an IP network.

Networking concepts

- **Switch:**
  - Switches are Multi-Input Multi-Output (MIMO) devices that **enable packets to travel from one node to another.**
  - Switches **connect hosts** that belong to the **same layer-2 network.**
  - They **forward** the **traffic** based on the **destination Ethernet address in the packet header.**
- **Router:**
  - Routers are special devices that **enable packets to travel from one layer-3 network to another.**
  - Routers **operate at layer-3** in the networking model.
  - **They route the traffic based on the destination IP address in the packet header.**
- **Firewall:**
  - Firewalls are used to **regulate traffic to and from a host or a network.**
  - They **can filter packets based** on several criteria such as **source IP address, destination IP address, port numbers, connection state**, and so on.

Networking concepts

- Overlay protocol:
  - Tunneling is a mechanism that makes **transfer of payloads feasible** over an incompatible delivery network. It **allows the network user to gain access to denied or insecure networks.** Data **encryption may be employed to transport the payload**, ensuring that the encapsulated user network data appears as public even though it is private and can easily pass the conflicting network.
  - **Generic routing encapsulation (GRE)** is a protocol that runs over IP and is employed when delivery and payload protocols are compatible but payload addresses are incompatible. For instance, a payload might think it is running on a datalink layer but it is actually running over a transport layer using datagram protocol over IP. **GRE creates a private point-to-point connection and works by encapsulating a payload.** GRE is a foundation protocol for other tunnel protocols but the GRE tunnels provide only weak authentication.
  - **VXLAN**: The purpose of VXLAN is to provide scalable network isolation. **VXLAN is a Layer 2 overlay scheme on a Layer 3 network.** It **allows an overlay layer-2 network to spread across multiple underlay layer-3** network domains. Each overlay is termed a VXLAN segment. **Only VMs within the same VXLAN segment can communicate.**
  - **GENEVE**: Generic Network Virtualization Encapsulation is designed to recognize and accommodate changing capabilities and needs of different devices in network virtualization. It provides a framework for tunneling rather than being prescriptive about the entire system. Geneve defines the content of the metadata flexibly that is added during encapsulation and tries to adapt to various virtualization scenarios. It **uses UDP as its transport protocol and is dynamic in size using extensible option headers.** Geneve supports unicast, multicast, and broadcast.

Networking concepts

- Network namespace:
  - **A namespace is a way of scoping a particular set of identifiers.**
  - **In a network namespace, the scoped 'identifiers' are network devices.** It is possible to create namespaces, and create new devices in those namespaces, or to move an existing device from one namespace to another.
  - **Each network namespace also has its own routing table**, and in fact this is the main reason for namespaces to exist.
  - **Each network namespace also has its own set of iptables** (for both IPv4 and IPv6). So, you can apply different security to flows with the same IP addressing in different namespaces, as well as different routing.
  - **Any given Linux process runs in a particular network namespace.** By default this is inherited from its parent process, but a process with the right capabilities can switch itself into a different namespace; in practice this is mostly done using the **ip netns exec**
- NAT:
  - *Network Address Translation* (NAT) is a process for modifying the source or destination addresses in the headers of an IP packet while the packet is in transit.
  - **SNAT**: In *Source Network Address Translation* (SNAT), the NAT **router modifies the IP address of the sender** in IP packets. SNAT is commonly used to enable hosts with *private addresses* to communicate with servers on the public Internet.
  - **DNAT**: In Destination Network Address Translation (DNAT), the NAT router **modifies the IP address of the destination** in IP packet headers.

Neutron

Neutron

- Neutron is an OpenStack project to **provide "network connectivity as a service"** between interface devices (e.g., vNICs) managed by other OpenStack services (e.g., nova)
- OpenStack Networking handles the **creation and management** of a **virtual networking infrastructure**, including **networks, switches, subnets, and routers for devices** managed by the OpenStack Compute service (nova)
- **OpenStack Networking integrates** with various OpenStack components:
  - **OpenStack Identity service** (keystone) is used for authentication and authorization of API requests.
  - **OpenStack Compute service** (nova) is used to plug each virtual NIC on the VM into a particular network.
  - **OpenStack Dashboard** (horizon) is used by administrators and project users to create and manage network services through a web-based graphical interface

- Ref:
  - https://docs.openstack.org/neutron/latest/
  - https://docs.openstack.org/neutron/latest/admin/intro.html

Neutron components

- API server
  - The **neutron-server** that provides API endpoints and serves as a single point of access to the database. It usually runs on the controller nodes.
- Type Driver
  - Define **how** an OpenStack **network is technically realized.** Example: **VXLAN**
  - **Each available network type is managed by an ML2 type driver.** Type drivers maintain any needed type-specific network state. They **validate the type specific information** for provider networks and are **responsible for the allocation of a free segment in project networks.**
- Mechanism Driver
  - **Define the mechanism to access an OpenStack network** of a certain type. Example: Open vSwitch mechanism driver.
  - The mechanism driver **is responsible for taking the information established by the type driver and ensuring that it is properly applied given the specific networking mechanisms** that have been enabled.
  - Mechanism drivers can utilize L2 agents (via RPC) and/or **interact directly with external devices or controllers.**

Neutron components

- Type Driver / Mechanism Driver

type driver / mech driver	Flat	VLAN	VXLAN	GRE	Geneve
Open vSwitch	yes	yes	yes	yes	yes
Linux bridge	yes	yes	yes	no	no
OVN	yes	yes	yes (requires OVN 20.09+)	no	yes
SRIOV	yes	yes	no	no	no
MacVTap	yes	yes	no	no	no
L2 population	no	no	yes	yes	yes

Neutron components

- DHCP agent
  - The DHCP agent is responsible for DHCP (Dynamic Host Configuration Protocol) and RADVD (Router Advertisement Daemon) services.
- Metadata proxy
  - The Metadata agent allows instances to access cloud-init meta data and user data via the network.
- L2 agent
  - Layer2 agent that can utilize Open vSwitch, Linux Bridge or other vendor-specific technology to provide network segmentation and isolation for project networks. The L2 agent should run on every node where it is deemed responsible for wiring and securing virtual interfaces (usually both compute and network nodes).
- L3 agent
  - Layer3 agent that runs on network node and provides east-west and north-south routing plus some advanced services such as VPNaaS.

Neutron components

- Security
  - L2 agents support security configurations.
    - **Security group**: are user-configurable collections of rules that have been configured to allow traffic to the applied instance. Any traffic not explicitly allowed by a security group is denied, by default.
    - **MAC Spoofing Prevention**: this rule prevent IP and MAC spoofing by requiring instances to source traffic from the IP and MAC address combination assigned to the instance.

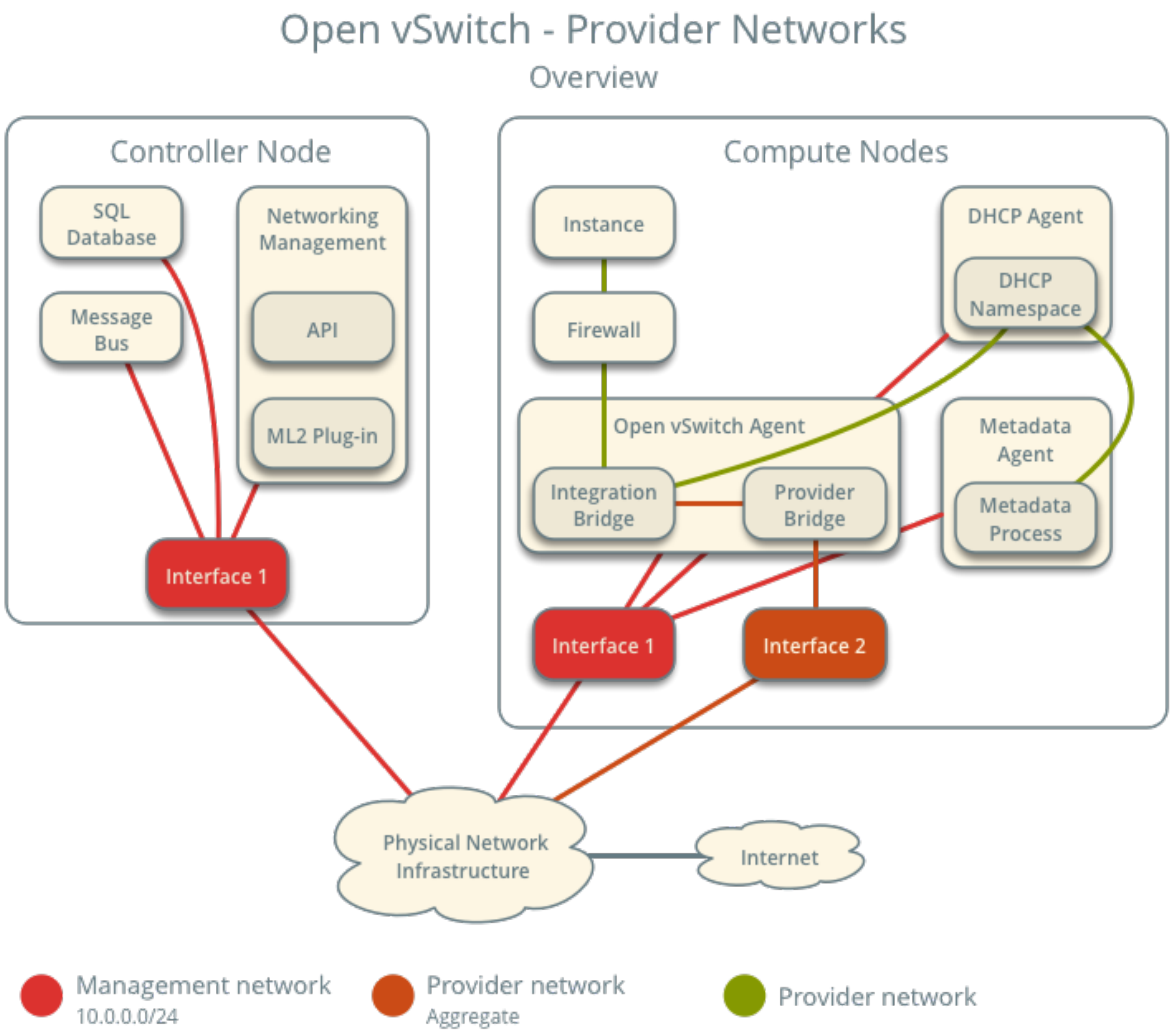
- Ref:
  - https://docs.openstack.org/neutron/latest/admin/config.html

Neutron network topologies

- Provider network
  - An instance uses a provider (external) network that connects to the physical network infrastructure via layer-2 (bridging/switching). This network includes a DHCP server that provides IP addresses to instances.
- Self-service network
  - Private network that connects to the physical network infrastructure via NAT.
  - This network includes a DHCP server that provides IP addresses to instances.
  - An instance on this network can automatically access external networks such as the Internet. However, access to an instance on this network from external networks such as the Internet requires a floating IP address.
- Ref:
  - https://docs.openstack.org/install-guide/launch-instance-networks-provider.html
  - https://docs.openstack.org/install-guide/launch-instance-networks-selfservice.html

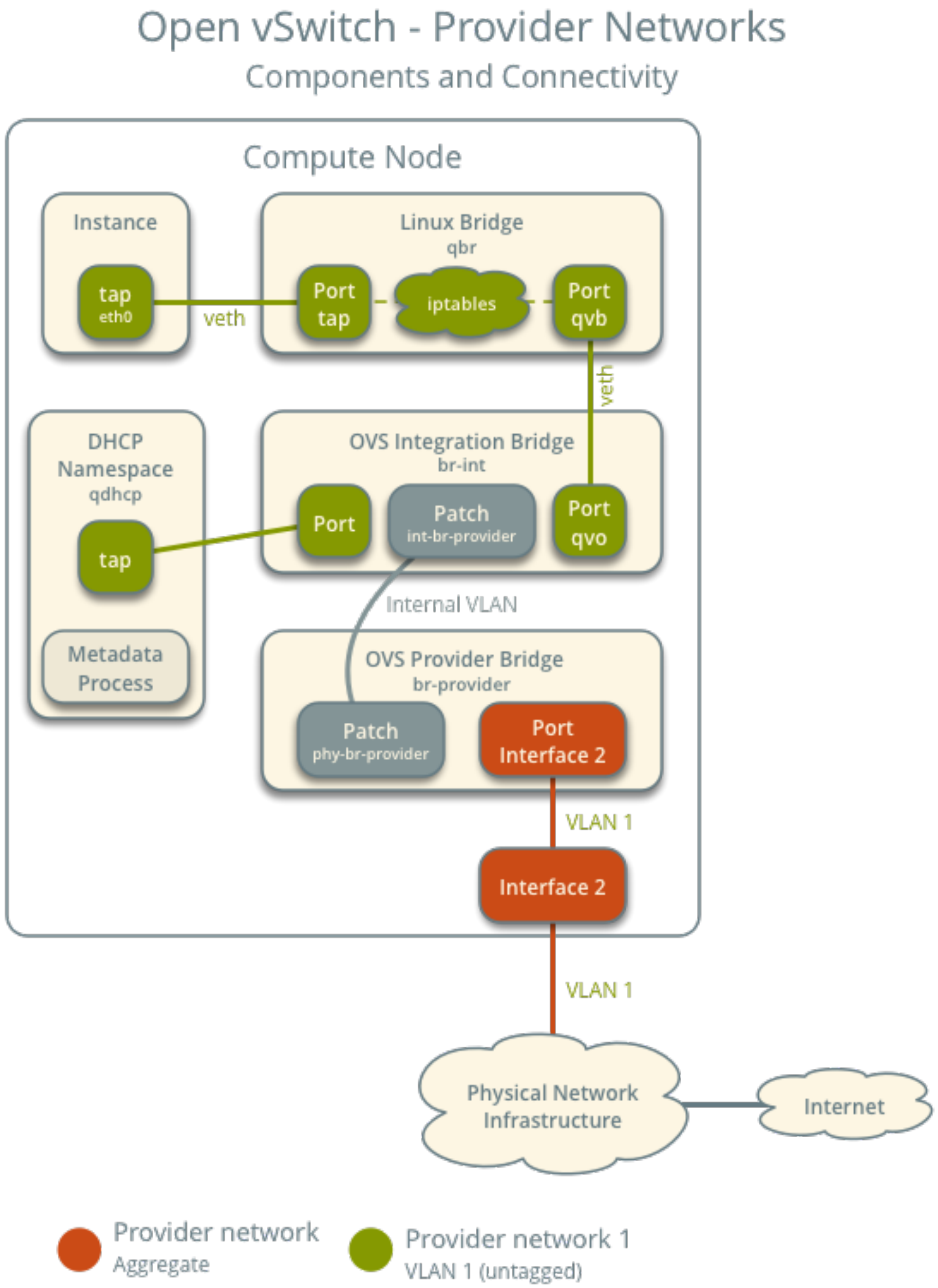
Neutron network topologies – Provider network

Ref: https://docs.openstack.org/neutron/latest/admin/deploy-ovs-provider.html



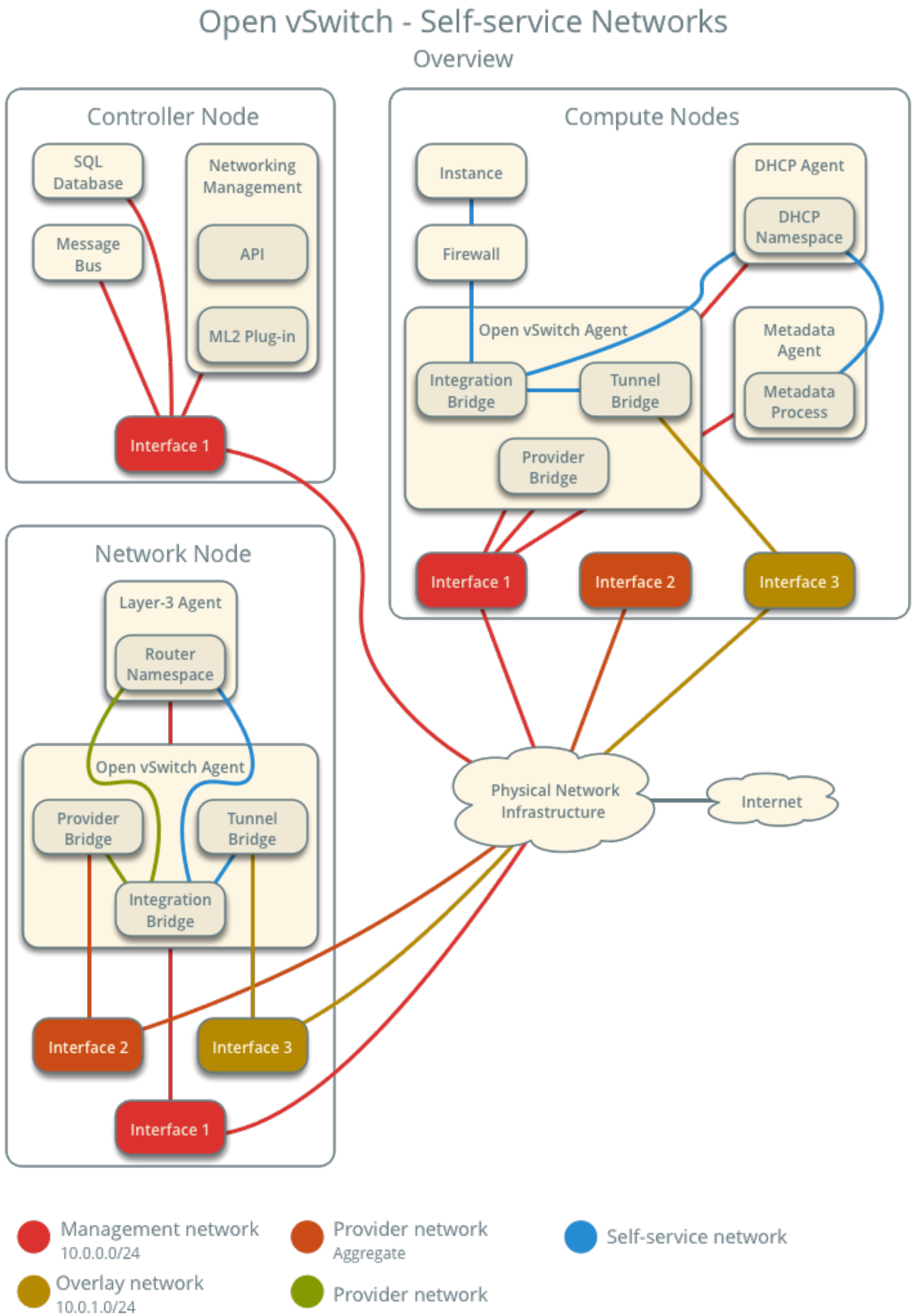
Neutron network topologies – Provider network

Ref: https://docs.openstack.org/neutron/latest/admin/deploy-ovs-provider.html



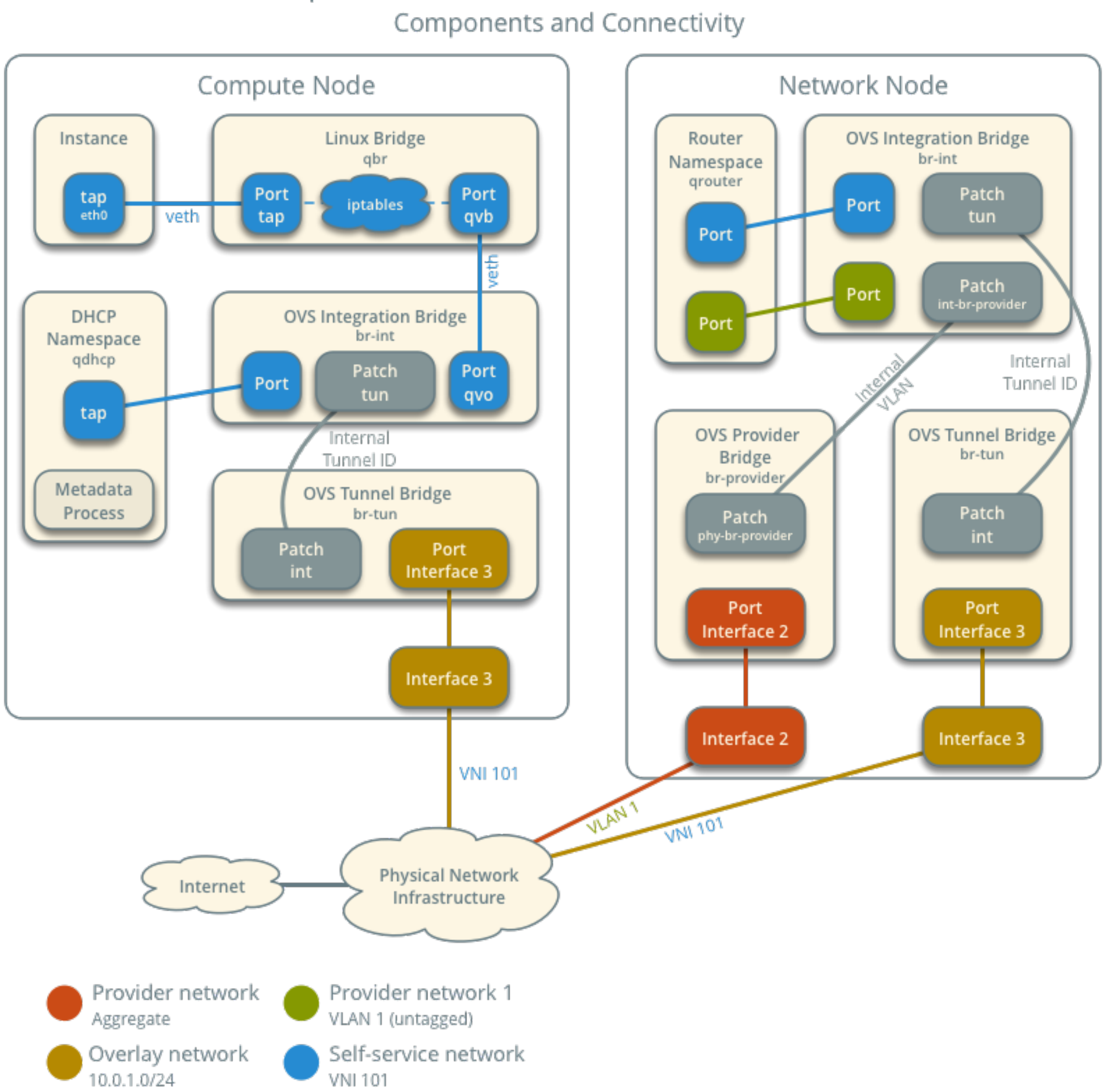
Neutron network topologies – Self-service network

Ref: https://docs.openstack.org/neutron/latest/admin/deploy-ovs-selfservice.html



Neutron network topologies – Self-service network

Ref:
https://docs.openstack.org/neutron/latest/admin/deploy-ovs-selfservice.html



Installation and Configuration

Neutron installation and configuration - Controller

- Setup database

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON neutron.* TO 'neutron'@'localhost' \ IDENTIFIED BY
'NEUTRON_DBPASS';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON neutron.* TO 'neutron'@'%' \ IDENTIFIED BY
'NEUTRON_DBPASS';
```

- Setup user, service and endpoint

```
openstack user create --domain default --password-prompt neutron
openstack role add --project service --user neutron admin
openstack service create --name neutron --description "OpenStack Networking" network
openstack endpoint create --region RegionOne network public http://controller:9696
openstack endpoint create --region RegionOne network internal http://controller:9696
openstack endpoint create --region RegionOne network admin http://controller:9696
```

- Install packages

```
yum install openstack-neutron openstack-neutron-ml2 openstack-neutron-openvswitch ebtables
```

- Ref:
  - https://docs.openstack.org/neutron/latest/install/controller-install-rdo.html
  - https://docs.openstack.org/neutron/latest/admin/deploy-ovs-selfservice.html

Neutron installation and configuration - Controller

- Configure neutron
  - /etc/neutron/neutron.conf

```
[DEFAULT]
# ...
core_plugin = ml2
service_plugins = router
allow_overlapping_ips = true
#...
transport_url = rabbit://openstack:RABBIT_PASS@controller
# ...
auth_strategy = keystone
#...
[database]
# ...
connection = mysql+pymysql://neutron:NEUTRON_DBPASS@controller/neutron
# ...
notify_nova_on_port_status_changes = true
notify_nova_on_port_data_changes = true
#...
[keystone_authtoken]
# ...
www_authenticate_uri = http://controller:5000
auth_url = http://controller:5000
memcached_servers = controller:11211
auth_type = password
project_domain_name = default
user_domain_name = default
project_name = service
username = neutron
password = NEUTRON_PASS
```

```
[nova]
# ...
auth_url = http://controller:5000
auth_type = password
project_domain_name = default
user_domain_name = default
region_name = RegionOne
project_name = service
username = nova
password = NOVA_PASS
#...
[oslo_concurrency]
# ...
lock_path = /var/lib/neutron/tmp
```

Neutron installation and configuration - Controller

- Setup ML2 Plugin
  - /etc/neutron/plugins/ml2/ml2_conf.ini

```
[ml2]
# ...
type_drivers = flat,vlan,vxlan
tenant_network_types = vxlan
mechanism_drivers = openvswitch,l2population
extension_drivers = port_security
# ...
[ml2_type_vxlan]
vxlan_group=224.0.0.1
vni_ranges=10:100
# ...
[ml2_type_flat]
# ...
flat_networks = provider
# ...
[securitygroup]
enable_security_group=True
```

Neutron installation and configuration - Controller

- Setup OVS bridge externa network

```
ovs-vsctl add-br br-ex
ovs-vsctl add-port br-ex eth0
```

- Setup ML2 Plugin
  - /etc/neutron/plugins/ml2/openvswitch_agent.ini

```
[ovs]
bridge_mappings = extnet:br-ex
integration_bridge=br-int
tunnel_bridge=br-tun
local_ip=10.10.0.21

[agent]
l2_population=False
drop_flows_on_start=False
tunnel_types=vxlan
vxlan_udp_port=4789

[securitygroup]
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver
```

Neutron installation and configuration - Controller

- Configure L3 agent
  - /etc/neutron/l3_agent.ini

```
[DEFAULT]
interface_driver = neutron.agent.linux.interface.OVSInterfaceDriver
```

- Setup DHCP agent
  - /etc/neutron/dhcp_agent.ini

```
[DEFAULT]
# ...
interface_driver = neutron.agent.linux.interface.OVSInterfaceDriver
dhcp_driver = neutron.agent.linux.dhcp.Dnsmasq
enable_isolated_metadata = true
```

Neutron installation and configuration - Controller

- Setup metadata proxy
  - /etc/neutron/metadata_agent.ini

```
[DEFAULT]
# ...
nova_metadata_host = controller
metadata_proxy_shared_secret = METADATA_SECRET
```

  - /etc/nova/nova.conf

```
[neutron]
# ...
auth_url = http://controller:5000
auth_type = password
project_domain_name = default
user_domain_name = default
region_name = RegionOne
project_name = service
username = neutron
password = NEUTRON_PASS
service_metadata_proxy = true
metadata_proxy_shared_secret = METADATA_SECRET
```

Neutron installation and configuration - Controller

- Finalize setup

```
ln -s /etc/neutron/plugins/ml2/ml2_conf.ini /etc/neutron/plugin.ini

su -s /bin/sh -c "neutron-db-manage --config-file /etc/neutron/neutron.conf \
  --config-file /etc/neutron/plugins/ml2/ml2_conf.ini upgrade head" neutron

systemctl restart openstack-nova-api.service

systemctl enable neutron-server.service \
  neutron-openvswitch-agent.service neutron-dhcp-agent.service \
  neutron-metadata-agent.service neutron-l3-agent.service
systemctl start neutron-server.service \
  neutron-openvswitch-agent.service neutron-dhcp-agent.service \
  neutron-metadata-agent.service neutron-l3-agent.service
```

Neutron installation and configuration - Compute

- Install packages

```
yum install openstack-neutron-openvswitch ebtables ipset
```

- Configure neutron
  - /etc/neutron/neutron.conf

```
[DEFAULT]
# ...
transport_url = rabbit://openstack:RABBIT_PASS@controller
auth_strategy = keystone

[keystone_authtoken]
# ...
www_authenticate_uri = http://controller:5000
auth_url = http://controller:5000
memcached_servers = controller:11211
auth_type = password
project_domain_name = default
user_domain_name = default
project_name = service
username = neutron
password = NEUTRON_PASS
# ...
[oslo_concurrency]
# ...
lock_path = /var/lib/neutron/tmp
```

Neutron installation and configuration - Compute

- Configure neutron
  - /etc/neutron/plugins/ml2/openvswitch_agent.ini

```
[agent]
l2_population=False
drop_flows_on_start=False
tunnel_types=vxlan
vxlan_udp_port=4789

[ovs]
integration_bridge=br-int
tunnel_bridge=br-tun
local_ip=10.10.0.16

[securitygroup]
firewall_driver=neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver
```

Neutron installation and configuration - Compute

- Setup nova
  - /etc/nova/nova.conf

```
[neutron]
# ...
auth_url = http://controller:5000
auth_type = password
project_domain_name = default
user_domain_name = default
region_name = RegionOne
project_name = service
username = neutron
password = NEUTRON_PASS
service_metadata_proxy = true
metadata_proxy_shared_secret = METADATA_SECRET
```

- Finalize

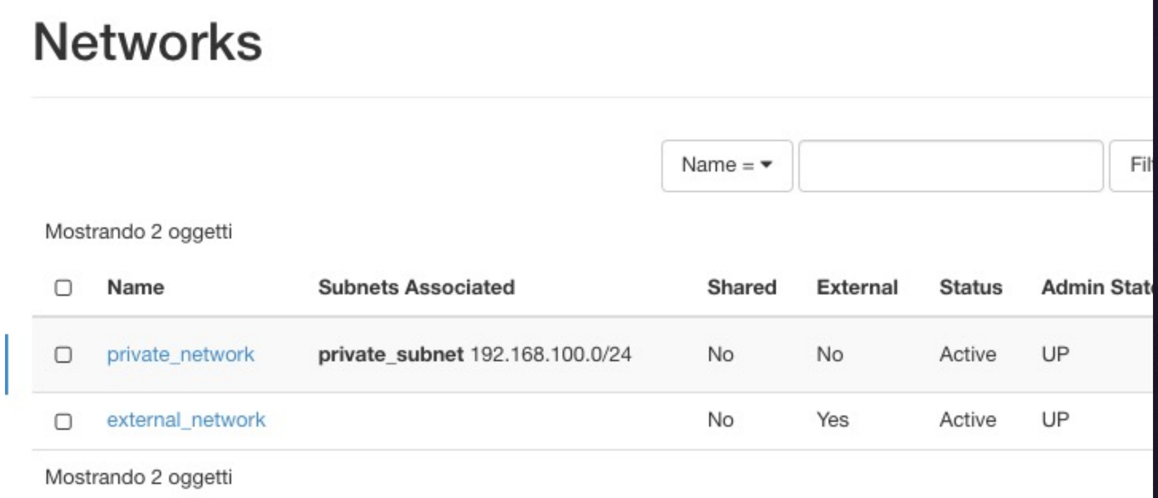
```
systemctl restart openstack-nova-compute.service

systemctl enable neutron-openvswitch-agent.service
systemctl start neutron-openvswitch-agent.service
```

Use Neutron

Neutron networks

- Network:
  - Networks correspond to the virtual "network cables" that are created for use by the cloud consumers. The mechanism for implementing these networks can be protocols such ad GRE tunnels, VLANs or VXLANs.



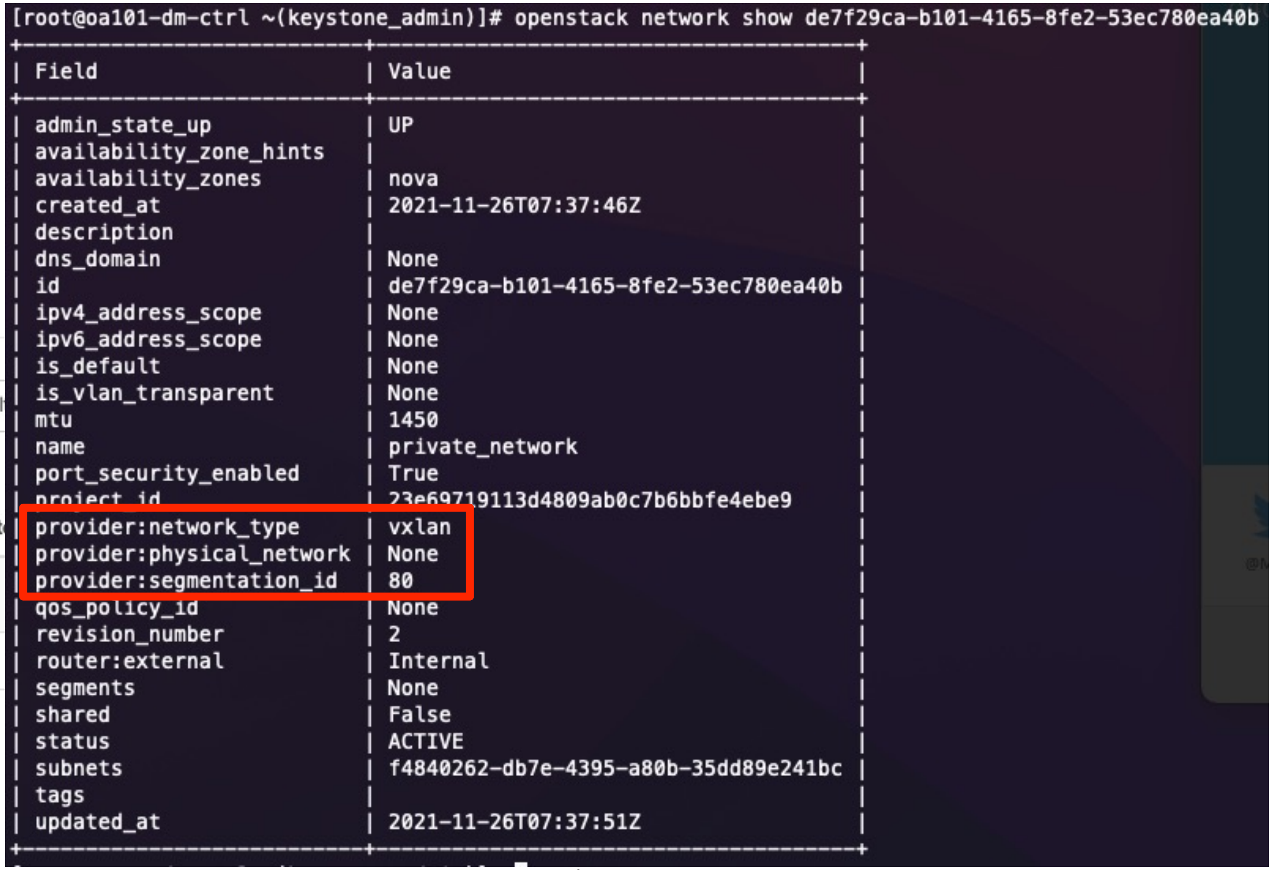
Networks

Name = ▾ | Fil

Mostrando 2 oggetti

	Name	Subnets Associated	Shared	External	Status	Admin Stat
☐	private_network	**private_subnet** 192.168.100.0/24	No	No	Active	UP
☐	external_network		No	Yes	Active	UP

Mostrando 2 oggetti



```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack network show de7f29ca-b101-4165-8fe2-53ec780ea40b
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        | nova                                 |
| created_at                | 2021-11-26T07:37:46Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | de7f29ca-b101-4165-8fe2-53ec780ea40b |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | None                                 |
| is_vlan_transparent       | None                                 |
| mtu                       | 1450                                 |
| name                      | private_network                      |
| port_security_enabled     | True                                 |
| project_id                | 23e69719113d4809ab0c7b6bbfe4ebe9     |
| provider:network_type     | vxlan                                |
| provider:physical_network | None                                 |
| provider:segmentation_id  | 80                                   |
| qos_policy_id             | None                                 |
| revision_number           | 2                                    |
| router:external           | Internal                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   | f4840262-db7e-4395-a80b-35dd89e241bc |
| tags                      |                                      |
| updated_at                | 2021-11-26T07:37:51Z                 |
+---------------------------+--------------------------------------+
```

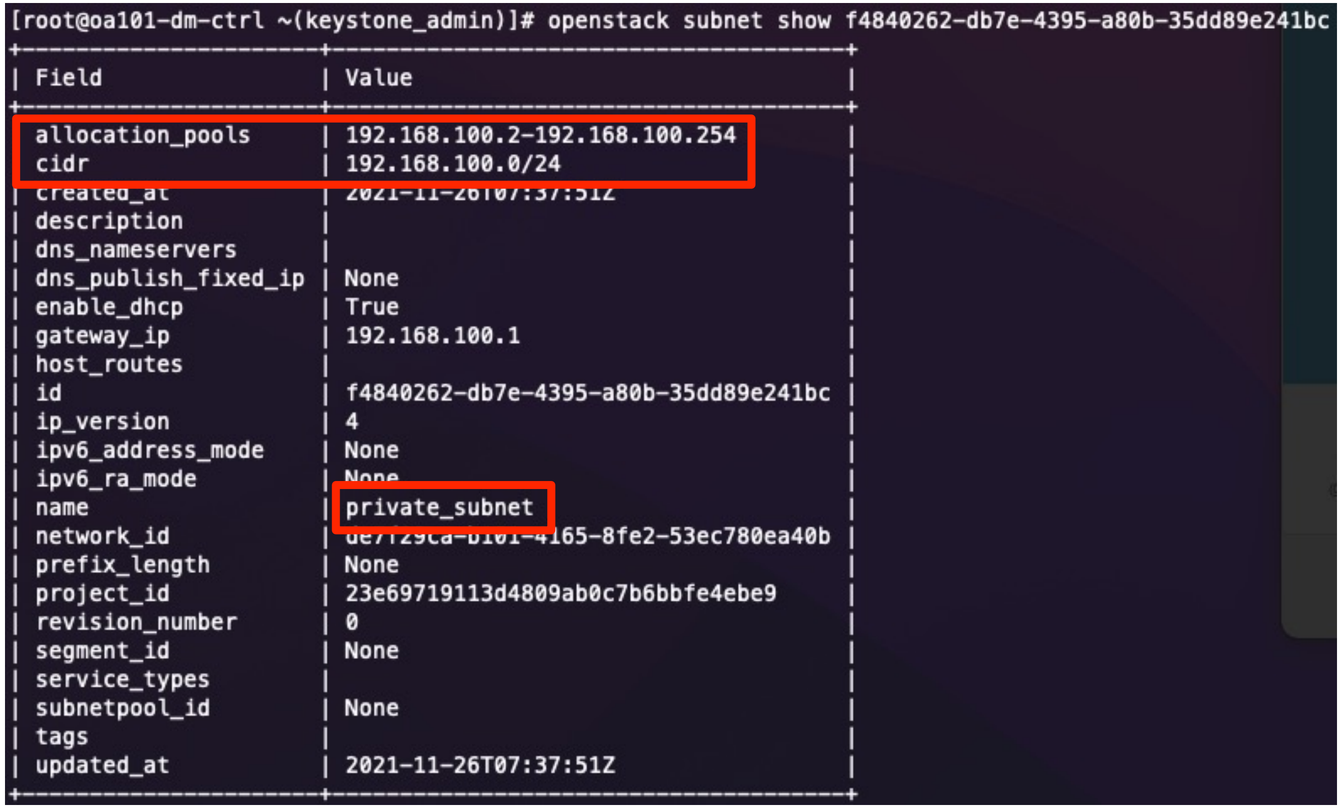
Neutron networks

- Network:

```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack network show f5a4d3d1-de6f-4d88-abc7-942147524818
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        | nova                                 |
| created_at                | 2021-11-26T07:25:35Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | f5a4d3d1-de6f-4d88-abc7-942147524818 |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | False                                |
| is_vlan_transparent       | None                                 |
| mtu                       | 1500                                 |
| name                      | external_network                     |
| port_security_enabled     | True                                 |
| project_id                | da5816c8acfc4362b9c98cfeab07875f     |
| provider:network_type     | flat                                 |
| provider:physical_network | extnet                               |
| provider:segmentation_id  | None                                 |
| qos_policy_id             | None                                 |
| revision_number           | 2                                    |
| router:external           | External                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   | 7e7c6de1-ab14-4870-9fe6-0dabd835f0db |
| tags                      |                                      |
| updated_at                | 2021-11-26T07:36:55Z                 |
+---------------------------+--------------------------------------+
```

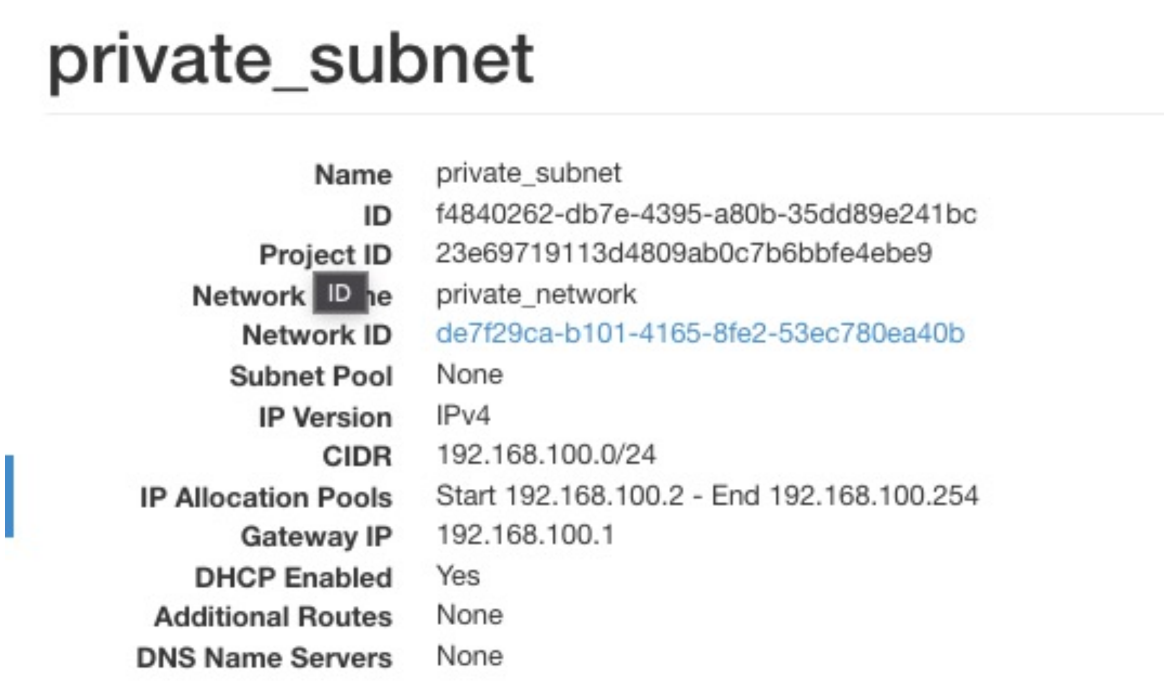
Neutron networks

- Subnet:
  - Subnets are the IP subnets that are associated with and run on these networks. It is possible to have multiple subnets associated with a single network if desired. However, it is common to have only one subnet running on a network.



```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack subnet show f4840262-db7e-4395-a80b-35dd89e241bc
```

Field	Value
allocation_pools	192.168.100.2-192.168.100.254
cidr	192.168.100.0/24
created_at	2021-11-26T07:37:51Z
description	
dns_nameservers	
dns_publish_fixed_ip	None
enable_dhcp	True
gateway_ip	192.168.100.1
host_routes	
id	f4840262-db7e-4395-a80b-35dd89e241bc
ip_version	4
ipv6_address_mode	None
ipv6_ra_mode	None
name	private_subnet
network_id	de7f29ca-b101-4165-8fe2-53ec780ea40b
prefix_length	None
project_id	23e69719113d4809ab0c7b6bbfe4ebe9
revision_number	0
segment_id	None
service_types	
subnetpool_id	None
tags	
updated_at	2021-11-26T07:37:51Z



Neutron networks

- Subnet:

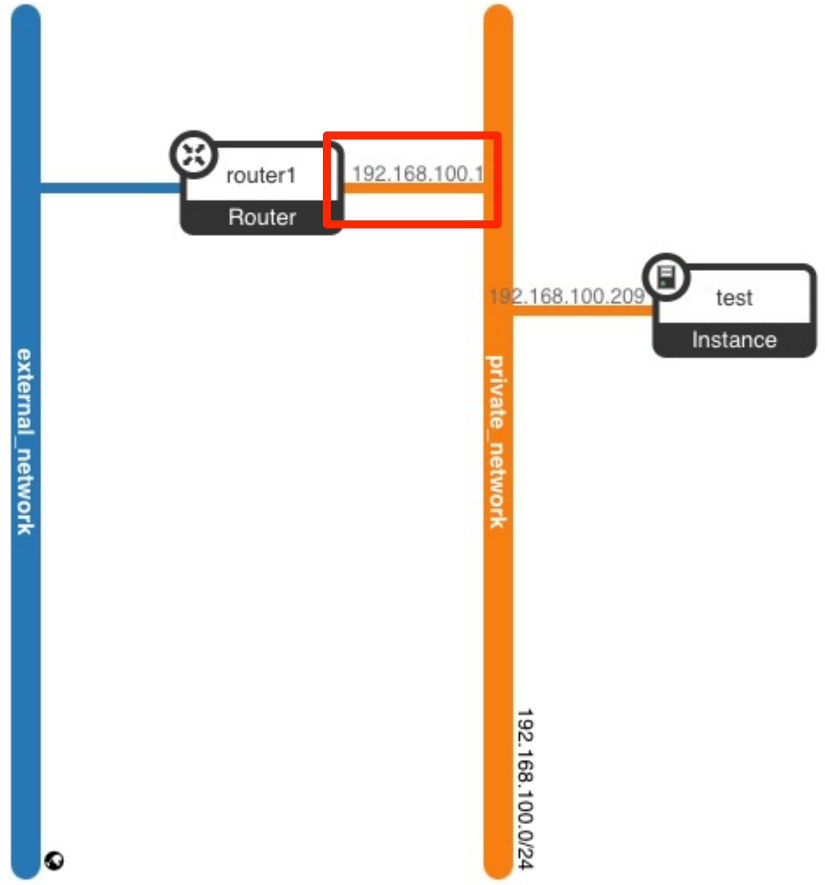
```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack subnet show 7e7c6de1-ab14-4870-9fe6-0dabd835f0db
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| allocation_pools     | 10.10.0.241-10.10.0.250              |
| cidr                 | 10.10.0.0/24                         |
| created_at           | 2021-11-26T07:36:55Z                 |
| description          |                                      |
| dns_nameservers      |                                      |
| dns_publish_fixed_ip | None                                 |
| enable_dhcp          | False                                |
| gateway_ip           | 10.10.0.1                            |
| host_routes          |                                      |
| id                   | 7e7c6de1-ab14-4870-9fe6-0dabd835f0db |
| ip_version           | 4                                    |
| ipv6_address_mode    | None                                 |
| ipv6_ra_mode         | None                                 |
| name                 | public_subnet                        |
| network_id           | f5a4d3d1-de6f-4d88-abc7-942147524818 |
| prefix_length        | None                                 |
| project_id           | da5816c8acfc4362b9c98cfeab07875f     |
| revision_number      | 0                                    |
| segment_id           | None                                 |
| service_types        |                                      |
| subnetpool_id        | None                                 |
| tags                 |                                      |
| updated_at           | 2021-11-26T07:36:55Z                 |
+----------------------+--------------------------------------+
```

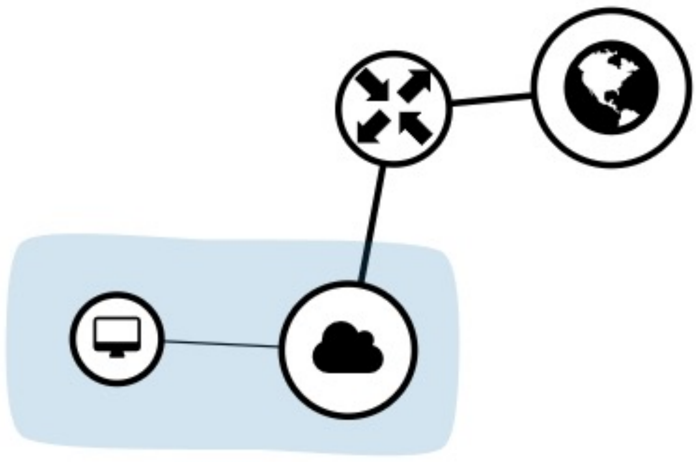
Neutron routers

- Router:
  - Routers connect subnets. Routers in OpenStack can have only one external interface but can have multiple internal interfaces. Routers are created by tenants to allow their instances to communicate with both the external world and with other instances that may be connected to other networks/subnets that they have created.
- Gateway:
  - The term gateway, when using it in the context of OpenStack, refers to the external interface on a router

```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack router show router1
+-------------------------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| Field                   | Value                                                                                                                                                                          |
+-------------------------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| admin_state_up          | UP                                                                                                                                                                             |
| availability_zone_hints |                                                                                                                                                                                |
| availability_zones      | nova                                                                                                                                                                           |
| created_at              | 2021-11-26T07:37:33Z                                                                                                                                                           |
| description             |                                                                                                                                                                                |
| distributed             | False                                                                                                                                                                          |
| external_gateway_info   | {"network_id": "f5a4d3d1-de6f-4d88-abc7-942147524818", "external_fixed_ips": [{"subnet_id": "7e7c6de1-ab14-4870-9fe6-0dabd835f0db", "ip_address": "10.10.0.241"}], "enable_snat": true} |
| flavor_id               | None                                                                                                                                                                           |
| ha                      | False                                                                                                                                                                          |
| id                      | 5f6b8893-8a63-4a3d-abb8-81e6a3406a8b                                                                                                                                           |
| interfaces_info         | [{"port_id": "99683f56-a368-41dd-a70c-b08e121eb3f8", "ip_address": "192.168.100.1", "subnet_id": "f4840262-db7e-4395-a80b-35dd89e241bc"}]                                        |
| name                    | router1                                                                                                                                                                        |
| project_id              | 23e69719113d4809ab0c7b6bbfe4ebe9                                                                                                                                               |
| revision_number         | 4                                                                                                                                                                              |
| routes                  |                                                                                                                                                                                |
| status                  | ACTIVE                                                                                                                                                                         |
| tags                    |                                                                                                                                                                                |
| updated_at              | 2021-11-26T07:38:00Z                                                                                                                                                           |
+-------------------------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
```

Neutron networks and routers





Neutron floating IP

- Floating IP (FIP):
  - Floating IP addresses exist on external networks. These addresses can be allocated to tenants and the tenants can then associate them with instances running on their private networks. The number of floating IP addresses that can be allocated to a tenant can be restricted via quota.
  - The Floating IP addresses, when allocated to a tenant, are created on the external interface of the tenant's virtual router. When associated with an instance on a private network, the network traffic is SNATed/DNATed between the instance and the external world, allowing that instance to be accessed by the external world.

```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack floating ip list
```

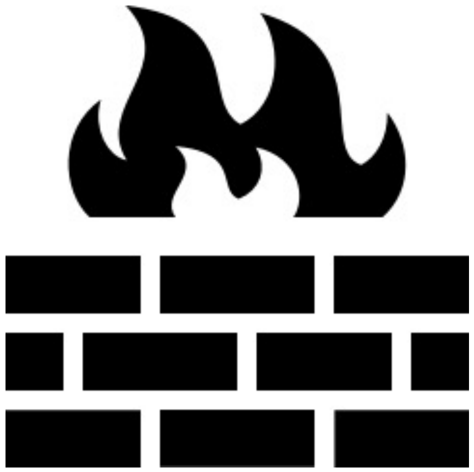
ID	Floating IP Address	Fixed IP Address	Port	Floating Network	Project
a7bb45bc-64b3-4919-98ae-a079bb7af210	10.10.0.247	192.168.100.209	825d4bec-ffcb-4dd6-9ace-0b36a6494881	f5a4d3d1-de6f-4d88-abc7-942147524818	23e69719113d4809ab0c7b6bbfe4ebe9

```
[root@oa101-dm-ctrl ~(keystone_admin)]# openstack server list --project dmichelotto
```

ID	Name	Status	Networks	Image	Flavor
0022c98a-dfdf-4b20-9c52-6db3a99c045b	test	ACTIVE	private_network=10.10.0.247, 192.168.100.209	cirros image 0.5.2	m1.tiny

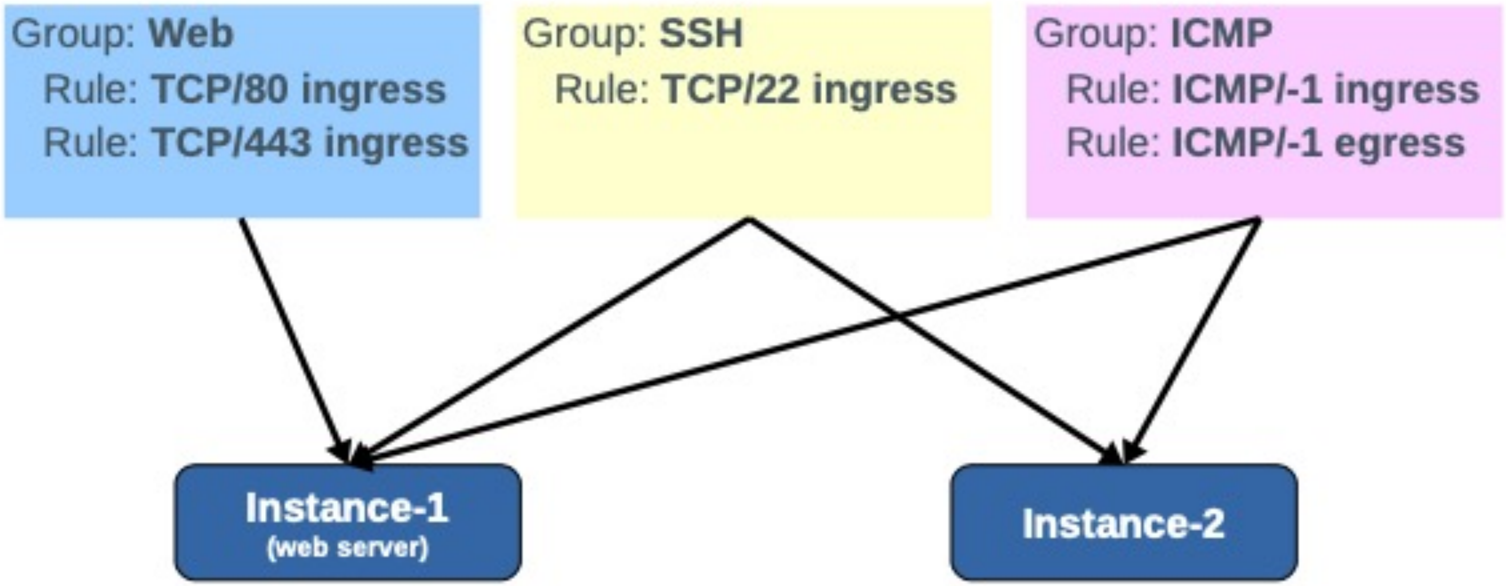
Neutron security groups

- Security groups:
  - Security groups are a method of simplifying the creation of firewall rules for instances. Security groups allow you to define firewall rules for different protocols/ports and then group them together. These groups can then be associated with instances. You only need to define the firewall rules once, when defining them in the security group, rather than having to define them every time a new instance is launched.
  - The number of security groups created by a tenant and the number of rules created by a project can be restricted via quota. This is important because firewall rule creation and management can create significant overhead on the cloud when there are large numbers of projects running large amounts of instances.
  - Any traffic not explicitly allowed by a security group is denied, by default.



Neutron security groups

- Security groups:
  - Multiple security groups can be associated with an instance. When this is done, all firewall rules in each of the security groups will be created for the instance.



Neutron security groups

- Security groups:
  - Remote security group it’s use to permit traffic come from machines beloging to the remote security group. It’s used in the Default security group in order to permitt all traffic between VMs that have Default security group

Manage Security Group Rules: default (0ba9cb68-232d-4dd8-9d6c-904808a4fffb)

+ Add Rule | Delete Rules

Displaying 4 items

	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
▢	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
▢	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
▢	Ingress	IPv4	Any	Any	-	default	-	Delete Rule
▢	Ingress	IPv6	Any	Any	-	default	-	Delete Rule

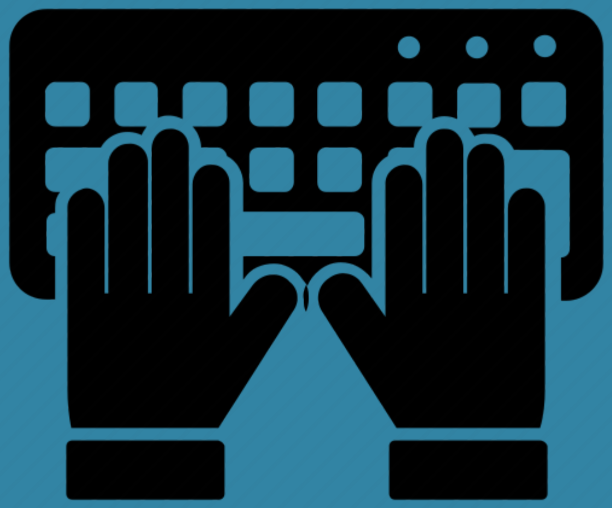
Displaying 4 items

Neutron troubleshooting

Neutron troubleshooting

- Review log file on controller and compute nodes:
  - /var/log/neutron/dhcp-agent.log
  - /var/log/neutron/l3-agent.log
  - /var/log/neutron/metadata-agent.log
  - /var/log/neutron/openvswitch-agent.log
  - /var/log/neutron/server.log
- If logs don’t report error, probably the configuration it’s OK and you have to use tools like:
  - ip netns
  - tcpdump
  - ovs-vsctl ovs-ofctl
- Other typical problem can be related to physical network configuration
  - Are physical network interface of controller and hypervisor up?
  - Network switch are correctly configured?
  - Alle VLAN are correctly propagated?

Questions



Hands-on

https://corso_oa101.baltig-pages.infn.it/hands-on/neutron/overview/