Amirkabir University of Technology

(Tehran Polytechnic)

Cloud Computing

OpenStack Neutron Architecture

Seyyed Ahmad Javadi

sajavadi@aut.ac.ir

Spring 2023

https://www.slideshare.net/HaimAteya/an-intrudction-to-openstack-2017

https://docs.openstack.org/security-guide/introduction/introduction-to-openstack.html

RabbitMQ overview

➢ RabbitMQ is the most widely deployed open source message

broker.

- ▪ https://www.rabbitmq.com/

➢ Watch YouTube Video

- ▪ https://www.youtube.com/watch?v=7rkeORD4jSw&list=RDCMUC KWaEZ-_VweaEx1j62do_vQ&index=2

Neutron

➢Network as a Service (NaaS)

Network as a Service (NaaS)

https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-as-service-naas.html
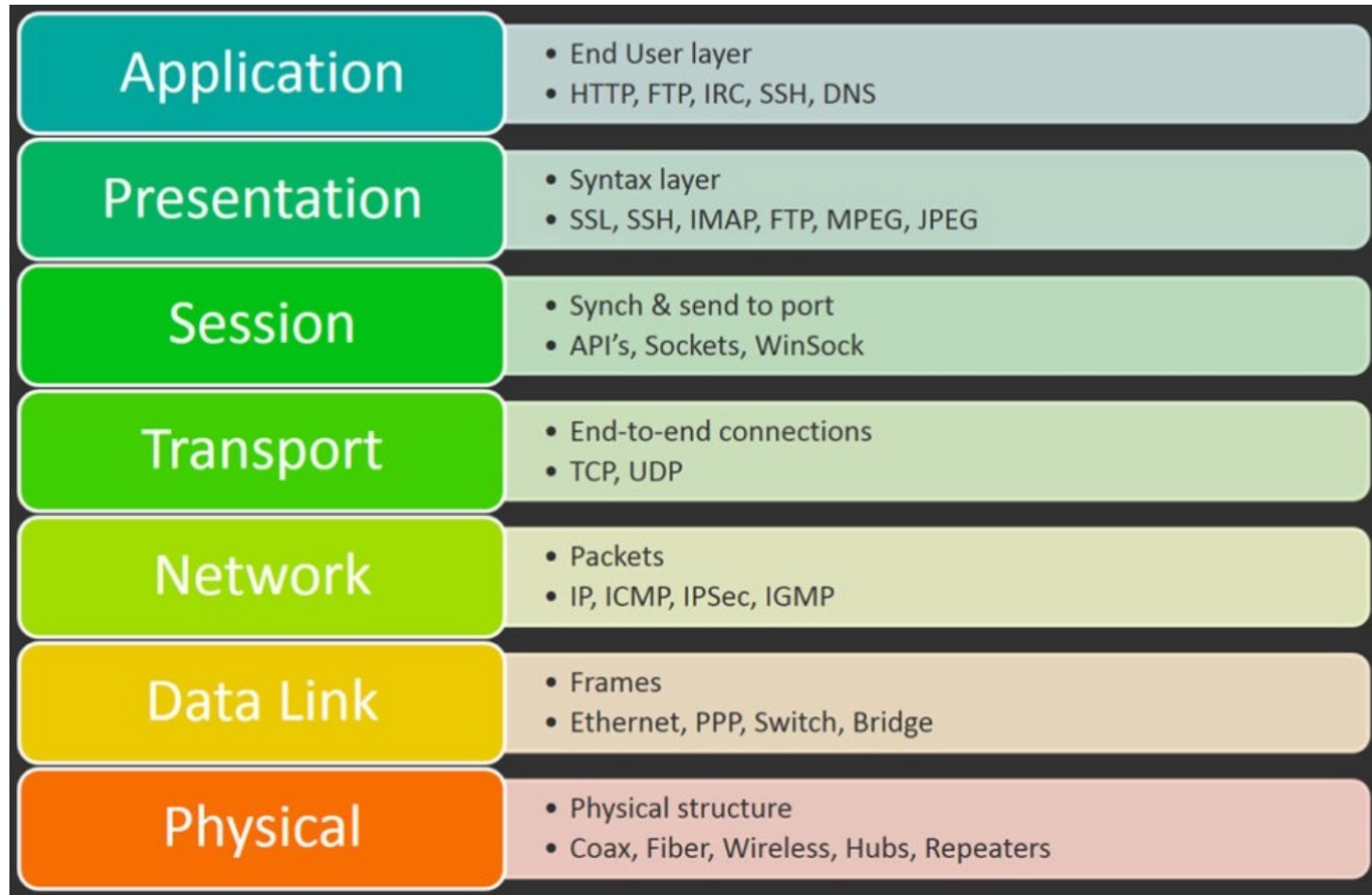
Neutron (cont.)

➢ Provides REST APIs to manage network connections for the resource managed by other OpenStack services.

➢ Complete control over the network resources in OpenStack:

  ▪ networks, ports, subnets.
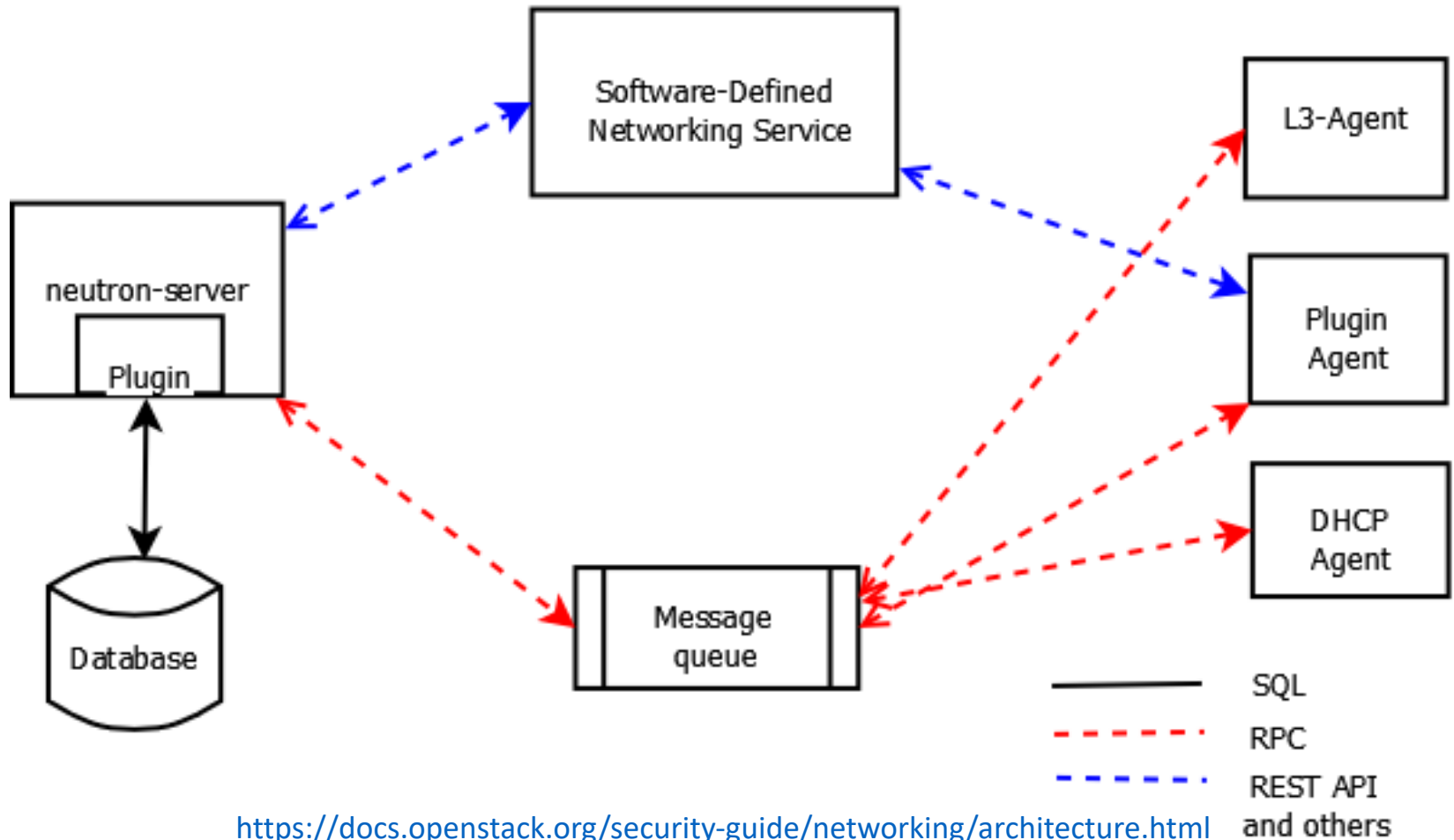
➢ Build complex network topologies.

OSI Layers

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Architectural and Networking Flow Diagram

https://docs.openstack.org/security-guide/networking/architecture.html
https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/16.0/html/networking_guide/sec-networking-concepts - l3-agent
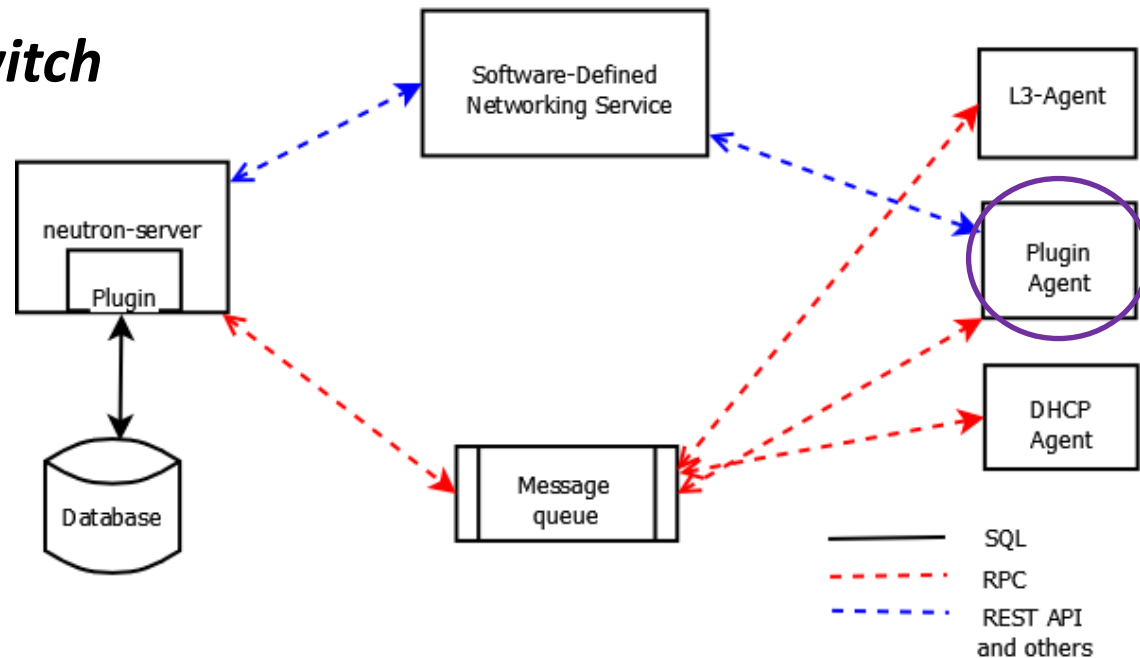
neutron server

➤ Runs on the **network node** to

service the Networking API and

its extensions.
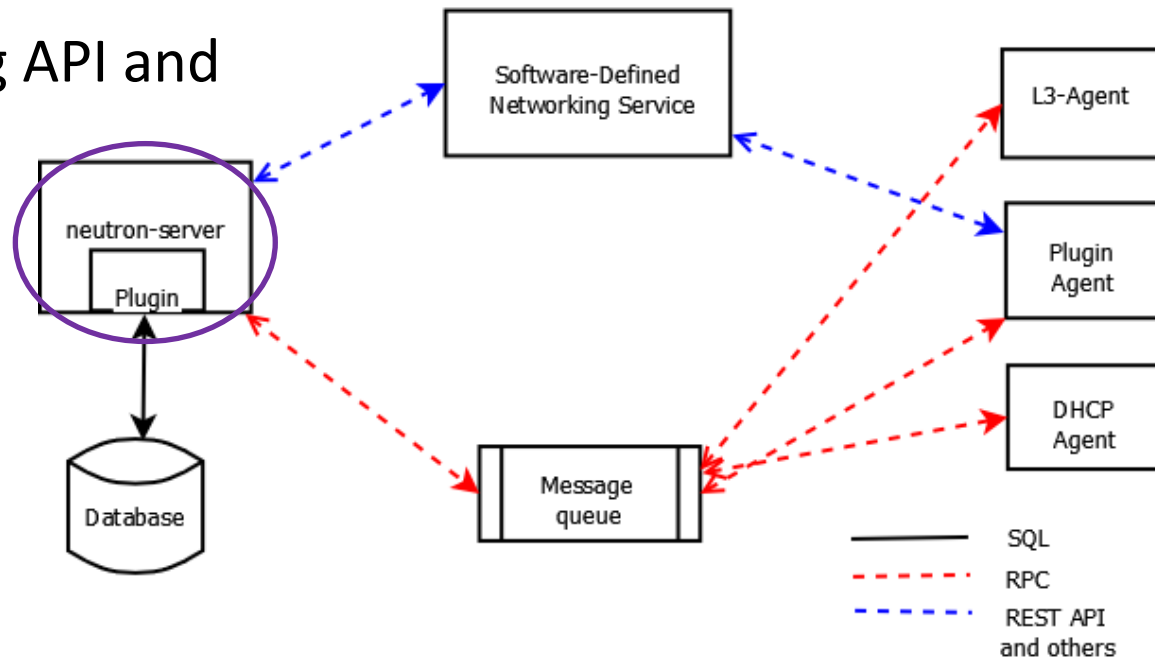
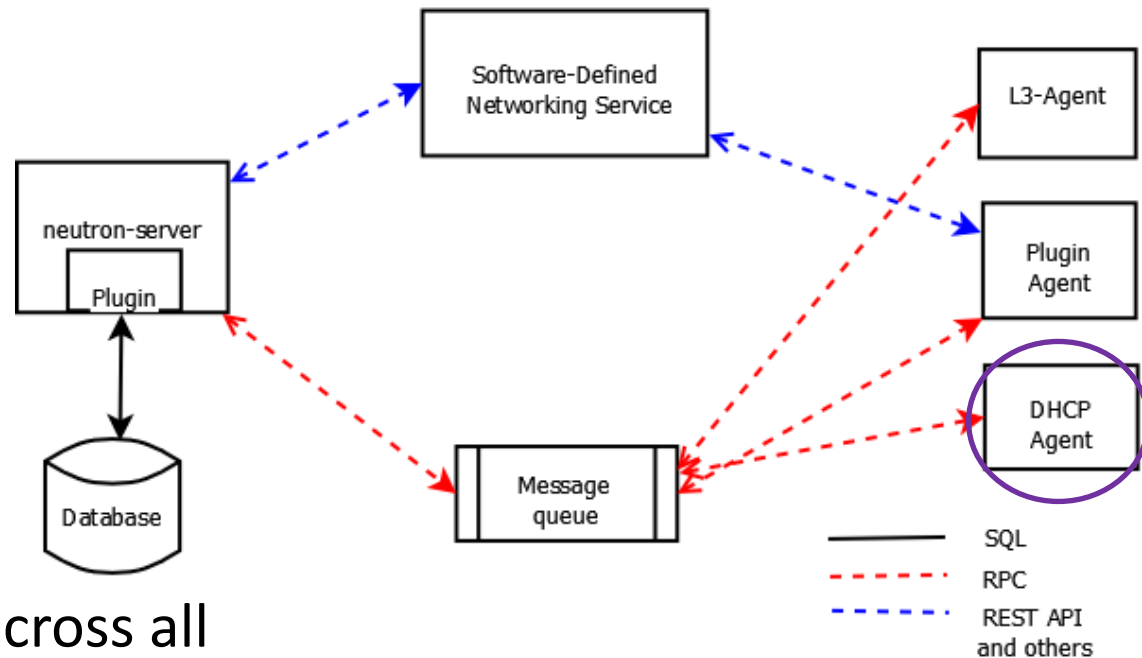➤ Enforces the network model and

IP addressing of each port.

plugin agent

➢ Runs on **each compute node** to
  manage **local virtual switch**
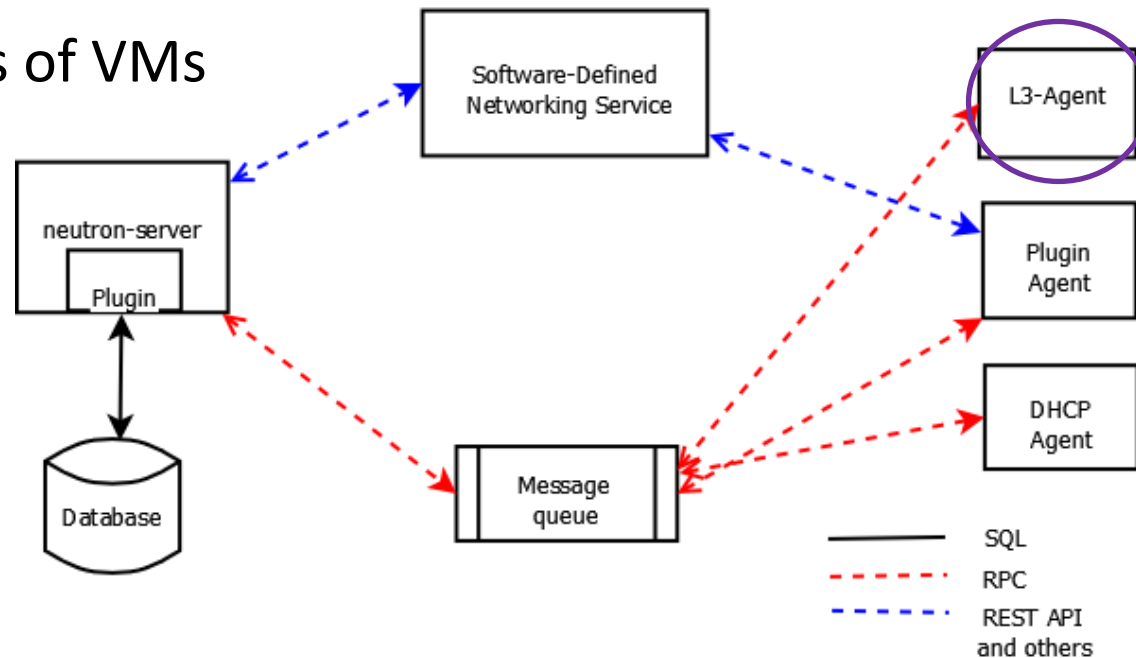 (vswitch) configuration.

DHCP agent

➢ Provides DHCP services to tenant

networks.

➢ This agent is the same across all

plug-ins and is responsible for
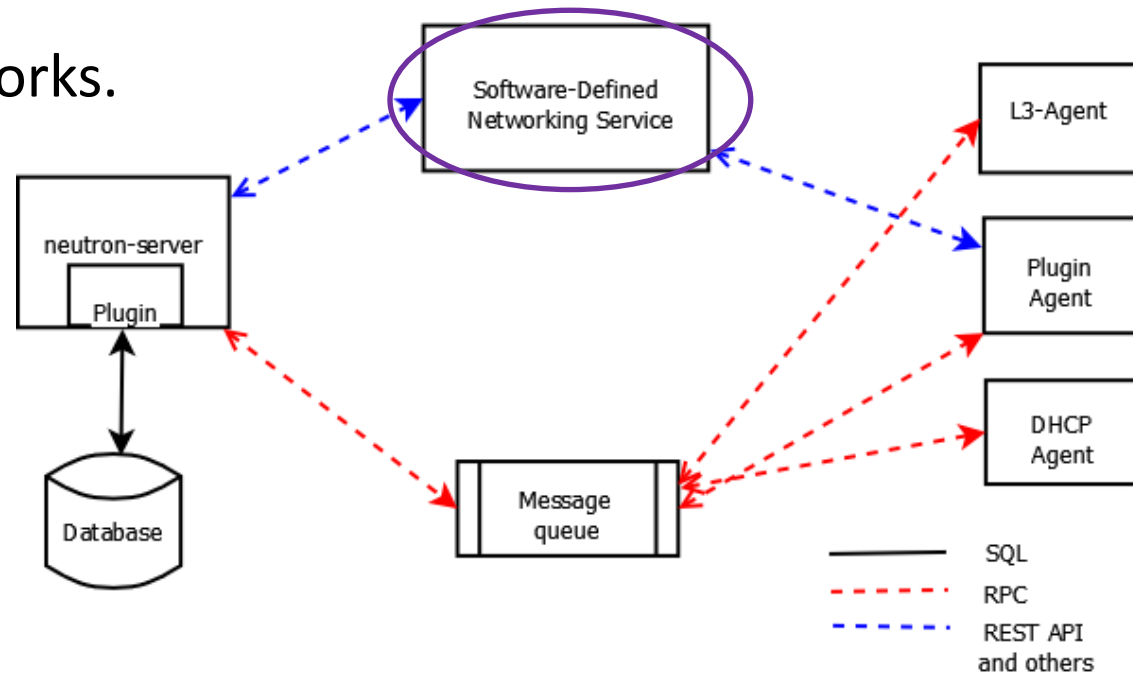
maintaining DHCP configuration.

L3 agent

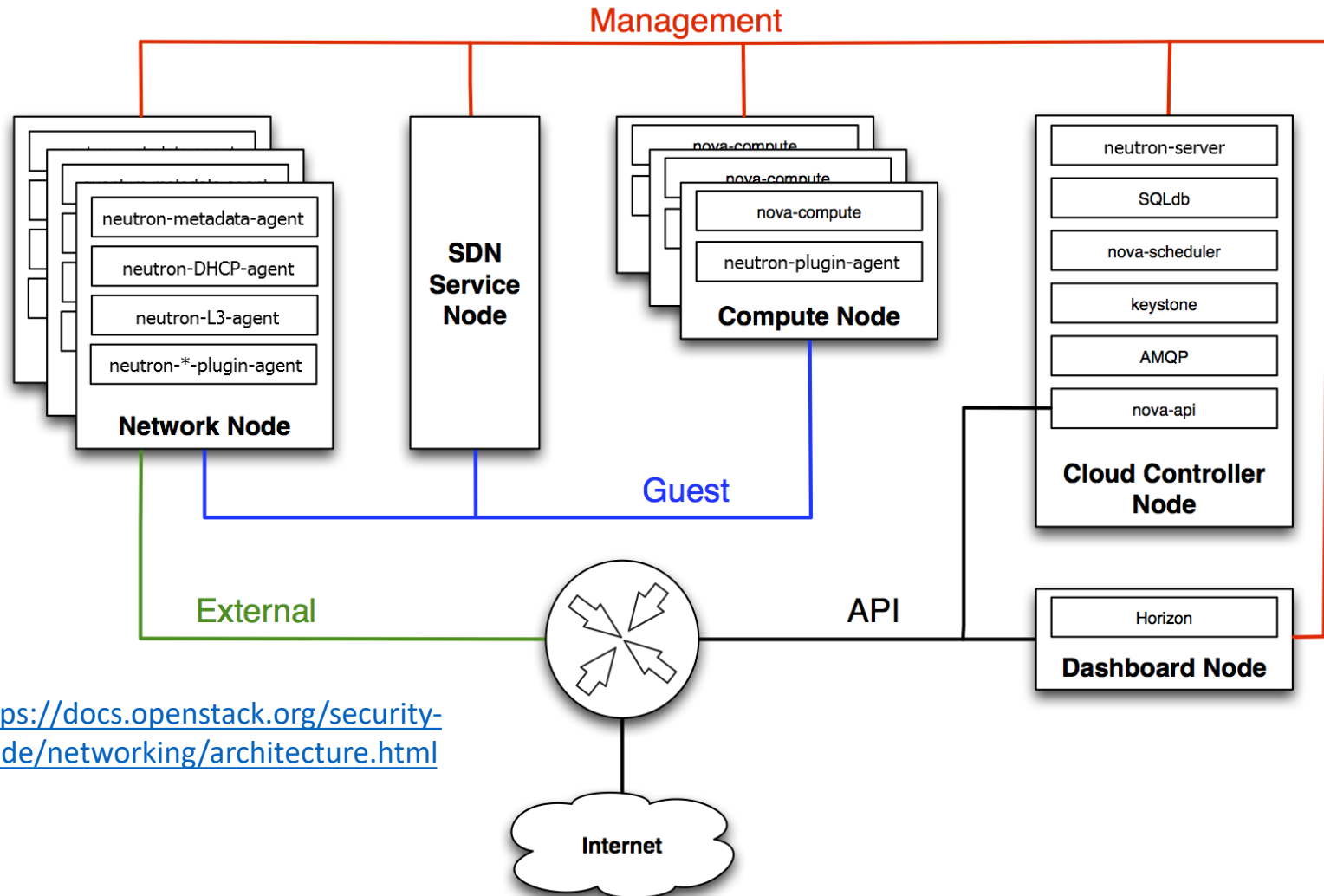➢Provides L3/NAT forwarding for external network access of VMs on tenant networks.

network provider services (SDN server)

➢Provides additional networking
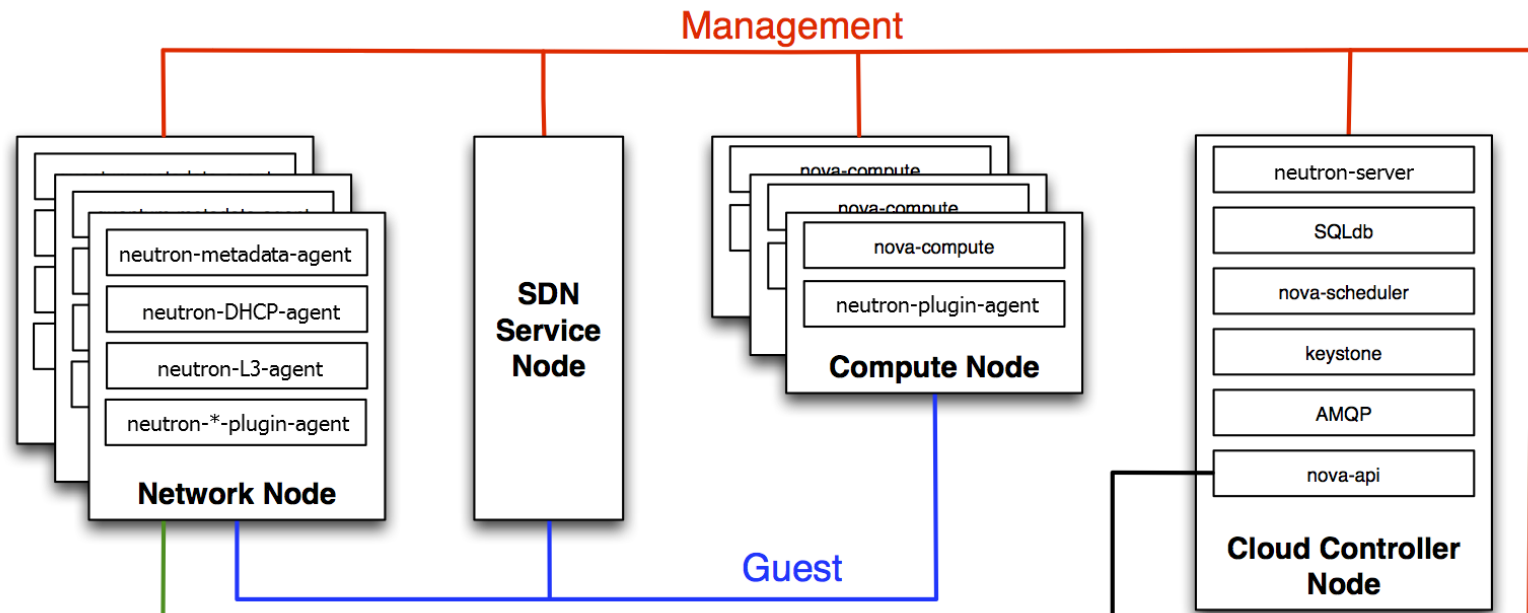
services to tenant networks.

Network connectivity of physical servers¶

https://docs.openstack.org/security-guide/networking/architecture.html

Management Network

➢ Used for internal communication between OpenStack Components.

➢ The IP addresses on this network should be reachable only within the data center and is considered the Management Security Domain.
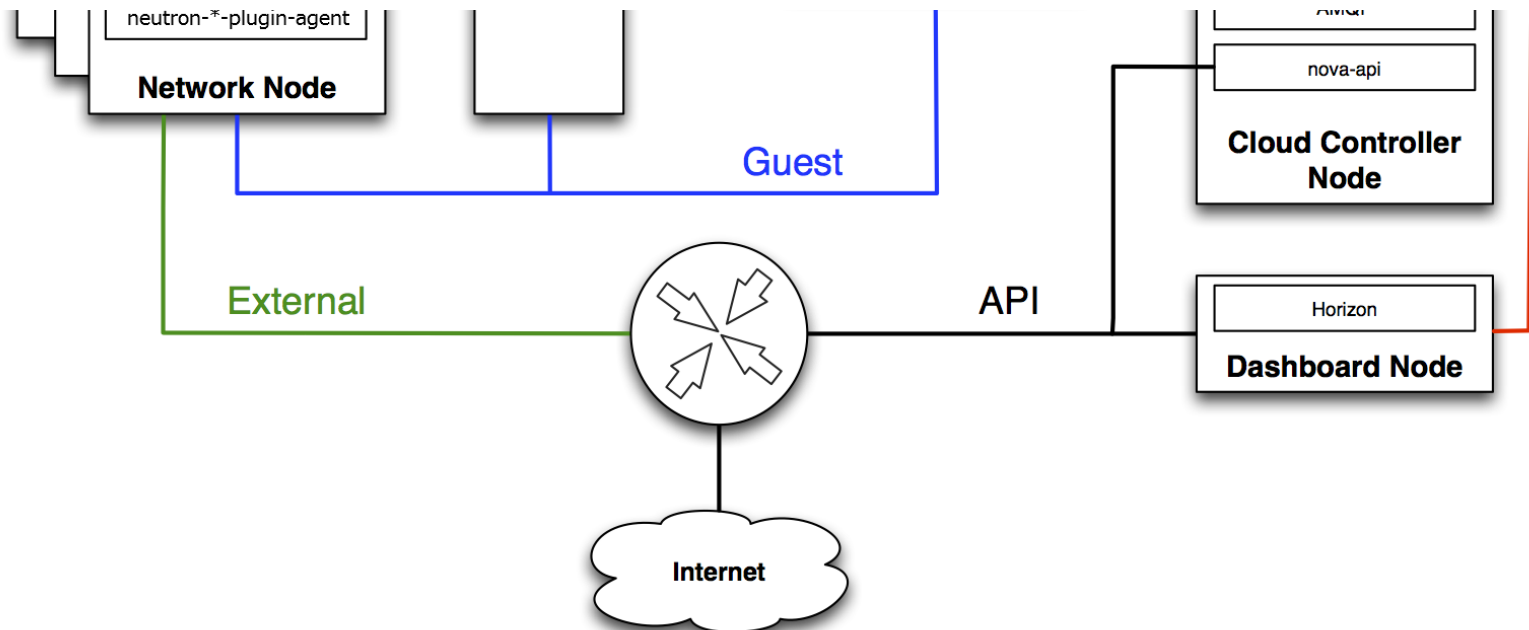
Guest network

➢ Used for VM data communication within the cloud deployment.

➢ This network is considered the Guest Security Domain.
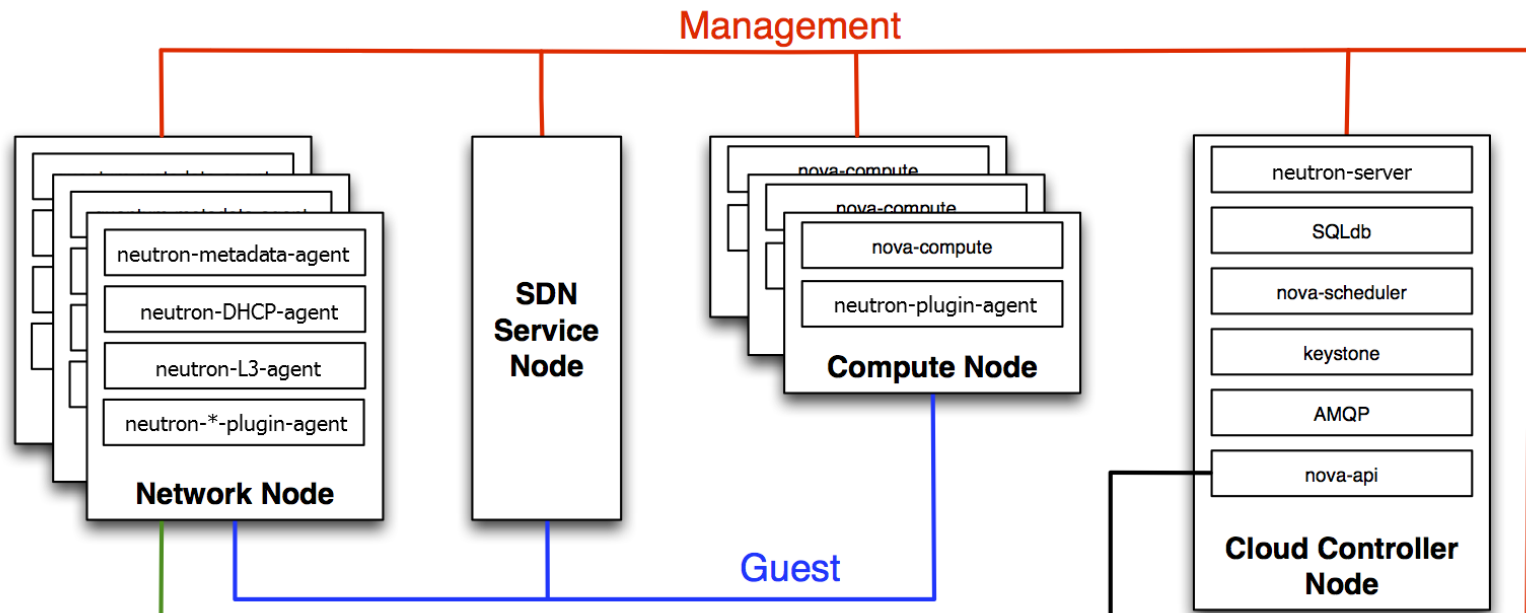
External network

➤ Used to provide VMs with Internet access in some deployment scenarios.

➤ IP addresses on this network should be reachable by anyone on the Internet.

➤ This network is considered to be in the Public Security Domain.

API network

➢ Exposes all OpenStack APIs (e.g., OpenStack Networking API), to tenants.

➢ IP addresses on this network should be reachable by anyone on the Internet.

➢ This may be the same network as the external network

➢ This network is considered the Public Security Domain.
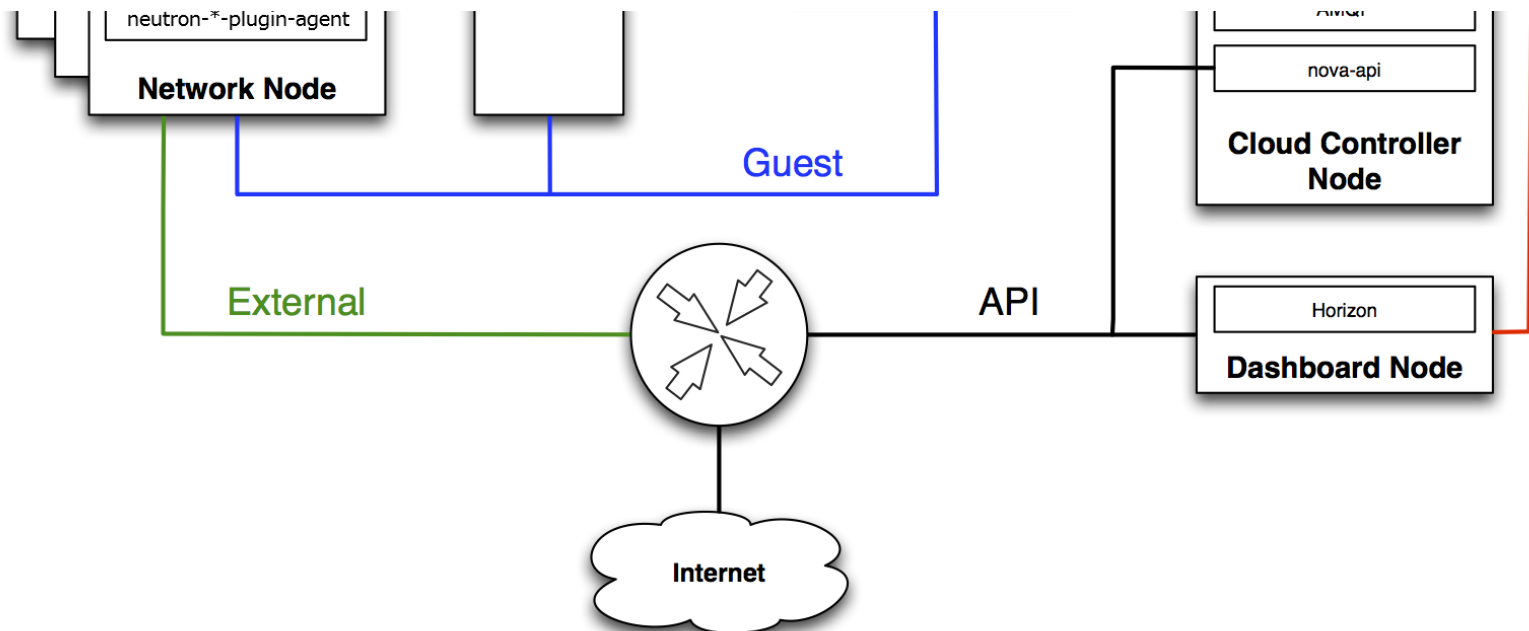
Neutron Plug-ins

➢ Modular Layer2 (ML2)

➢ Linux Bridge

➢ Open vSwitch

Modular Layer2 (ML2)

➢ A framework allowing OpenStack Networking to simultaneously utilize the variety of layer 2 networking technologies found in complex real-world data centers.

➢ It currently works with the existing OpenvSwitch, linuxbridge, and hyperv L2 agents

source: https://wiki.openstack.org/wiki/Neutron/ML2

Modular Layer2 (ML2) (cont.)

➢ Replace and deprecate the monolithic plugins associated with those L2 agents.

➢ Greatly simplify adding support for new L2 networking technologies, requiring much less initial and ongoing effort than would be required to add a new monolithic core plugin.

Modular Layer2 (ML2) (cont.)

➢ML2 uses the Linux Bridge to provide L2 connectivity for VM instances running on the compute node to the public network.

➢In most common deployments, there is a **compute** and a **network** node.

Modular Layer2 (ML2) (cont.)

➢ On both the compute and the network node, the **Linux Bridge**

Agent will manage

- virtual switches,

- connectivity among them,

- and interaction via virtual ports with other network components

  - Such as namespaces and underlying interfaces.

➢ Additionally, on the compute node, the Linux Bridge Agent will

manage security groups.

Linux Bridge

Linux Bridge - Provider Networks
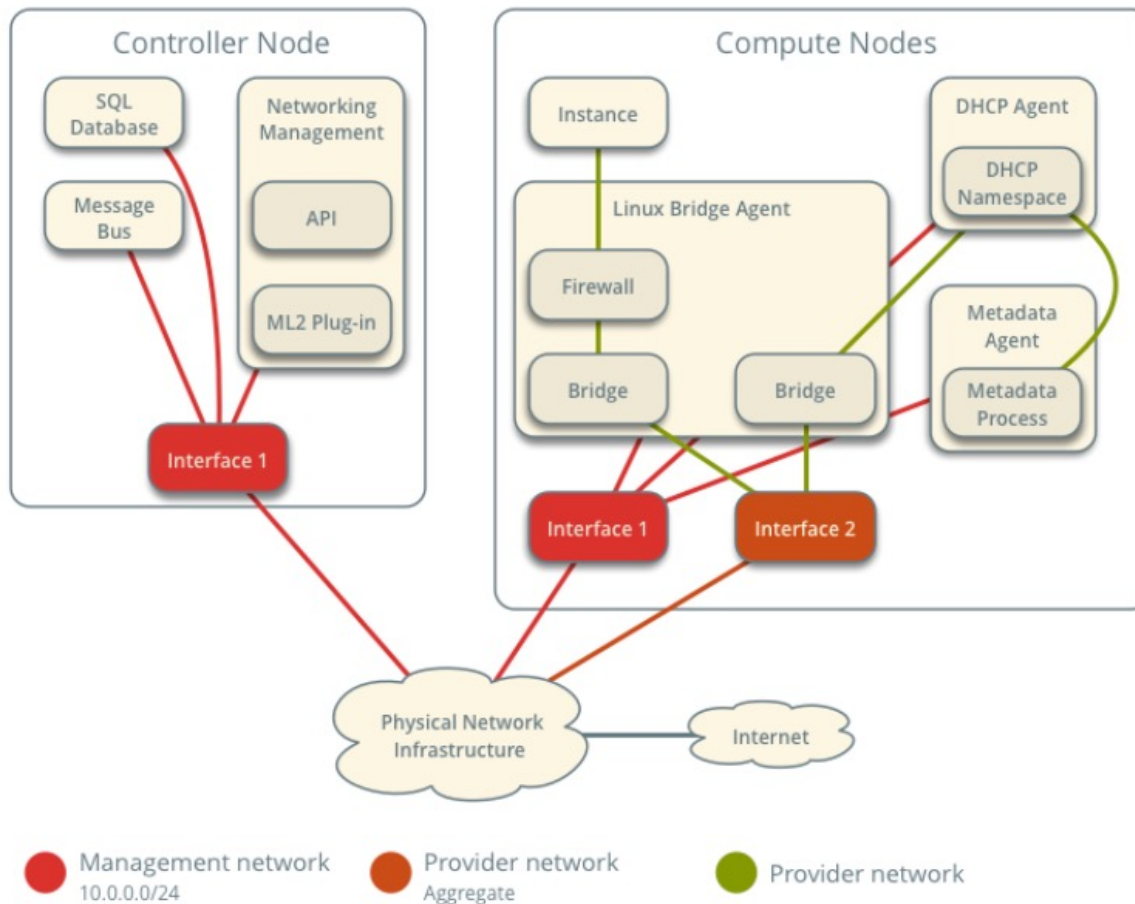
Source: https://docs.openstack.org/neutron/queens/admin/deploy-lb-provider.html#architecture

Open vSwitch

➤ An open-source project that allows hypervisors to virtualize the networking layer.

➤ This caters for the large number of virtual machines running on one or more physical nodes.

➤ The virtual machines connect to virtual ports on virtual bridges (inside the virtualized network layer.)

Open vSwitch (cont.)

➢This is very similar to a physical server connecting to physical ports on a Layer 2 networking switch.

➢These virtual bridges then allow the virtual machines to communicate with each other on the same physical node.

➢These bridges also connect these virtual machines to the physical network for communication outside the hypervisor node.
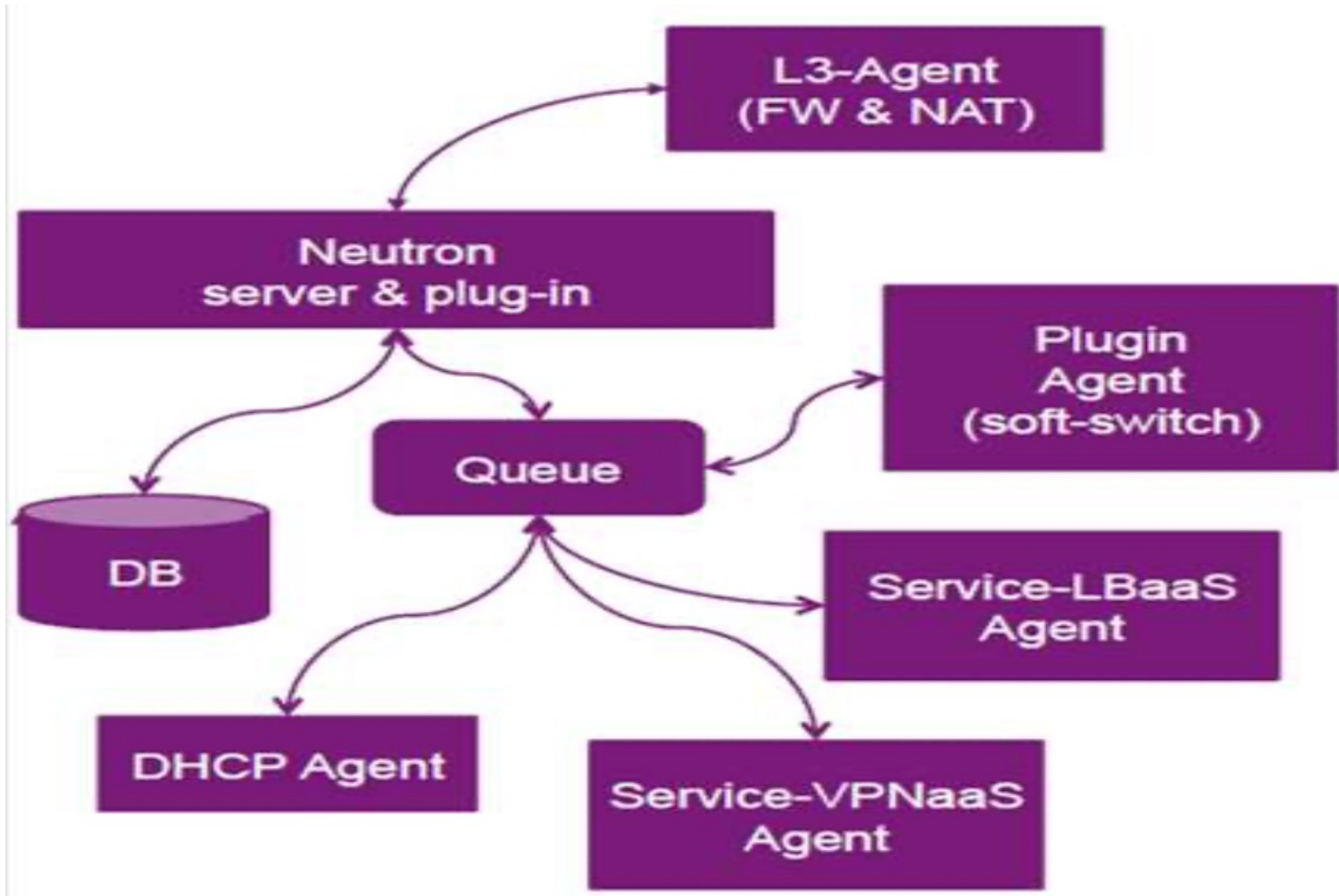
Open vSwitch (cont.)

In OpenStack, both the Neutron node and the compute node (Nova)

are running Open vSwitch to provide virtualized network services.

Neutron Services

➢Load Balancer as a Service (LBaaS)

➢Virtual Private Network as a Service (VPNaaS)

➢Firewall as a Service (FWaaS)

Neutron Components

Neutron Components (cont.)

➢Neutron Server

- Implement REST APIs

- Enforce network model

- Network, subnet, and port

- IP addressing to each port (IPAM)

➢Plugin agent

- Run on each compute node

- Connect instances to network port

Neutron Components (cont.)

➢Queue
- ▪ Enhanced communication between each components of neutron

➢Database
- ▪ Persistent network model

➢DHCP agent
- ▪ In multi-host mode, run on each compute node
- ▪ Maintain dhcp configuration

➢L3 agent
- ▪ To implement floating IPs and other L3 features, such as NAT