NAME

ovn-nb − OVN_Northbound database schema

This database is the interface between OVN and the cloud management system (CMS), such as OpenStack, running above it. The CMS produces almost all of the contents of the database. The **ovn−northd** program monitors the database contents, transforms it, and stores it into the **OVN_Southbound** database.

We generally speak of ‘‘the’’ CMS, but one can imagine scenarios in which multiple CMSes manage different parts of an OVN deployment.

External IDs

Each of the tables in this database contains a special column, named **external_ids**. This column has the same form and purpose each place it appears.

external_ids: map of string-string pairs
Key-value pairs for use by the CMS. The CMS might use certain pairs, for example, to identify entities in its own configuration that correspond to those in this database.

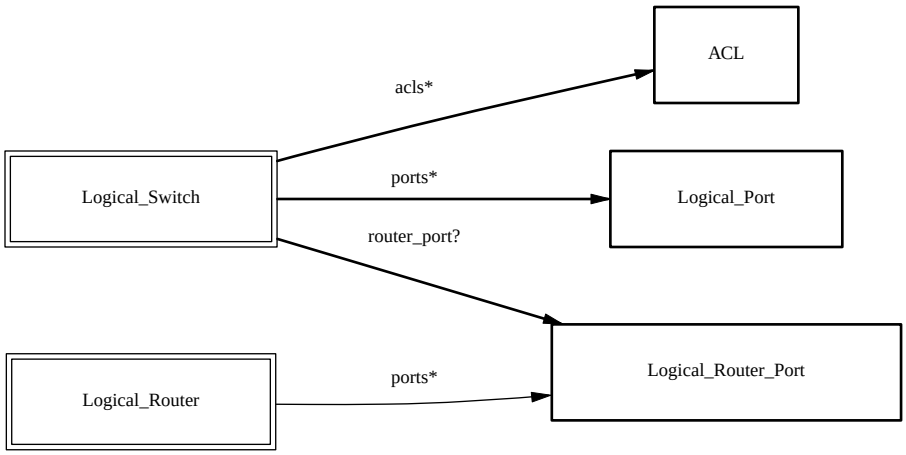
TABLE SUMMARY

The following list summarizes the purpose of each of the tables in the **OVN_Northbound** database. Each table is described in more detail on a later page.

Table	Purpose
Logical_Switch	L2 logical switch
Logical_Port	L2 logical switch port
ACL	Access Control List (ACL) rule
Logical_Router	L3 logical router
Logical_Router_Port	L3 logical router port

TABLE RELATIONSHIPS

The following diagram shows the relationship among tables in the database. Each node represents a table. Tables that are part of the ‘‘root set’’ are shown with double borders. Each edge leads from the table that contains it and points to the table that its value represents. Edges are labeled with their column names, followed by a constraint on the number of allowed values: **?** for zero or one, ***** for zero or more, **+** for one or more. Thick lines represent strong references; thin lines represent weak references.



Logical_Switch TABLE

Each row represents one L2 logical switch.

Summary:

name	string
ports	set of **Logical_Port**s
router_port	optional **Logical_Router_Port**
acls	set of **ACL**s
Common Columns:	
external_ids	map of string-string pairs

Details:

name: string

A name for the logical switch. This name has no special meaning or purpose other than to provide convenience for human interaction with the ovn-nb database. There is no requirement for the name to be unique. The logical switch's UUID should be used as the unique identifier.

ports: set of **Logical_Port**s

The logical ports connected to the logical switch.

It is an error for multiple logical switches to include the same logical port.

router_port: optional **Logical_Router_Port**

The router port to which this logical switch is connected, or empty if this logical switch is not connected to any router. A switch may be connected to at most one logical router, but this is not a significant restriction because logical routers may be connected into arbitrary topologies.

It is an error for multiple logical switches to refer to the same router port.

acls: set of **ACL**s

Access control rules that apply to packets within the logical switch.

Common Columns:

external_ids: map of string-string pairs

See **External IDs** at the beginning of this document.

Logical_Port TABLE

A port within an L2 logical switch.

Summary:

name	string (must be unique within table)
type	string
options	map of string-string pairs
parent_name	optional string
tag	optional integer, in range 1 to 4,095
up	optional boolean
enabled	optional boolean
macs	set of strings
port_security	set of strings
Common Columns:	
external_ids	map of string-string pairs

Details:

name: string (must be unique within table)

The logical port name.

For entities (VMs or containers) that are spawned in the hypervisor, the name used here must match those used in the **external_ids:iface-id** in the **Open_vSwitch** database's **Interface** table, because hypervisors use **external_ids:iface-id** as a lookup key to identify the network interface of that entity.

For containers that are spawned inside a VM, the name can be any unique identifier. In such a case, **parent_name** must be populated.

type: string

Specify a type for this logical port. Logical ports can be used to model other types of connectivity into an OVN logical switch. Leaving this column blank maintains the default logical port behavior, which is for a VM (or VIF) interface. The following other types are defined:

localnet

A connection to a locally accessible network from each **ovn−controller** instance. A logical switch can only have a single **localnet** port attached and at most one regular logical port. This is used to model direct connectivity to an existing network.

vtep A port to a logical switch on a VTEP gateway. In order to get this port correctly recognized by the OVN controller, the **options**:**vtep−physical−switch** and **options**:**vtep−logical−switch** must also be defined.

options: map of string-string pairs

This column provides key/value settings specific to the logical port **type**. The following options are defined:

network_name

Must be set when **type** is **localnet**. **ovn−controller** uses local configuration to determine exactly how to connect to this locally accessible network.

vtep−physical−switch

The name of the VTEP gateway. Must be set when **type** is **vtep**.

vtep−logical−switch

A logical switch name connected by the VTEP gateway. Must be set when **type** is **vtep**.

parent_name: optional string

When **name** identifies the interface of a container spawned inside a tenant VM, this column represents the VM interface through which the container interface sends its network traffic. The name used here must match those used in the **external_ids:iface-id** in the **Open_vSwitch** table, because hypervisors in this case use **external_ids:iface-id** as a lookup key to identify the network interface of the tenant VM.

tag: optional integer, in range 1 to 4,095

When **type** is empty and **name** identifies the interface of a container spawned inside a tenant VM, this column identifies the VLAN tag in the network traffic associated with that container's network interface. When there are multiple container interfaces inside a VM, all of them send their network traffic through a single VM network interface and this value helps OVN identify the correct container interface.

When **type** is set to **localnet**, this can be set to indicate that the port represents a connection to a specific VLAN on a locally accessible network. The VLAN ID is used to match incoming traffic and is also added to outgoing traffic.

up: optional boolean

This column is populated by **ovn−northd**, rather than by the CMS plugin as is most of this database. When a logical port is bound to a physical location in the OVN Southbound database **Binding** table, **ovn−northd** sets this column to **true**; otherwise, or if the port becomes unbound later, it sets it to **false**. This allows the CMS to wait for a VM's (or container's) networking to become active before it allows the VM (or container) to start.

enabled: optional boolean

This column is used to administratively set port state. If this column is empty or is set to **true**, the port is enabled. If this column is set to **false**, the port is disabled. A disabled port has all ingress and egress traffic dropped.

macs: set of strings

The logical port's own Ethernet address or addresses, each in the form *xx*:*xx*:*xx*:*xx*:*xx*:*xx*. Like a physical Ethernet NIC, a logical port ordinarily has a single fixed Ethernet address. The string **unknown** is also allowed to indicate that the logical port has an unknown set of (additional) source addresses.

port_security: set of strings

A set of L2 (Ethernet) addresses from which the logical port is allowed to send packets and to which it is allowed to receive packets. If this column is empty, all addresses are permitted. Logical ports are always allowed to receive packets addressed to multicast and broadcast addresses.

Each member of the set is an Ethernet address in the form *xx*:*xx*:*xx*:*xx*:*xx*:*xx*.

This specification will be extended to support L3 port security.

Common Columns:

external_ids: map of string-string pairs

See **External IDs** at the beginning of this document.

ACL TABLE

Each row in this table represents one ACL rule for a logical switch that points to it through its **acls** column. The **action** column for the highest-**priority** matching row in this table determines a packet's treatment. If no row matches, packets are allowed by default. (Default-deny treatment is possible: add a rule with **priority** 1, **1** as **match**, and **deny** as **action**.)

Summary:

priority	integer, in range 1 to 65,534
direction	string, either **to−lport** or **from−lport**
match	string
action	string, one of **allow−related**, **drop**, **allow**, or **reject**
log	boolean
Common Columns:	
external_ids	map of string-string pairs

Details:

priority: integer, in range 1 to 65,534

The ACL rule's priority. Rules with numerically higher priority take precedence over those with lower. If two ACL rules with the same priority both match, then the one actually applied to a packet is undefined.

Return traffic from an **allow−related** flow is always allowed and cannot be changed through an ACL.

direction: string, either **to−lport** or **from−lport**

Direction of the traffic to which this rule should apply:

- **from−lport**: Used to implement filters on traffic arriving from a logical port. These rules are applied to the logical switch's ingress pipeline.
- **to−lport**: Used to implement filters on traffic forwarded to a logical port. These rules are applied to the logical switch's egress pipeline.

match: string

The packets that the ACL should match, in the same expression language used for the **match** column in the OVN Southbound database's **Logical_Flow** table. The **outport** logical port is only available in the **to−lport** direction (the **inport** is available in both directions).

By default all traffic is allowed. When writing a more restrictive policy, it is important to remember to allow flows such as ARP and IPv6 neighbor discovery packets.

In logical switches connected to logical routers, the special port name **ROUTER** refers to the logical router port.

action: string, one of **allow−related**, **drop**, **allow**, or **reject**

The action to take when the ACL rule matches:

- **allow**: Forward the packet.
- **allow−related**: Forward the packet and related traffic (e.g. inbound replies to an outbound connection).
- **drop**: Silently drop the packet.
- **reject**: Drop the packet, replying with a RST for TCP or ICMP unreachable message for other IP-based protocols. **Not implemented−−currently treated as drop**

log: boolean

If set to **true**, packets that match the ACL will trigger a log message on the transport node or nodes that perform ACL processing. Logging may be combined with any **action**.

Logging is not yet implemented.

Common Columns:

external_ids: map of string-string pairs
See **External IDs** at the beginning of this document.

Logical_Router TABLE

Each row represents one L3 logical router.

Summary:

name	string
ports	set of weak reference to **Logical_Router_Port**s
default_gw	optional string
Common Columns:	
external_ids	map of string-string pairs

Details:

name: string

A name for the logical router. This name has no special meaning or purpose other than to provide convenience for human interaction with the ovn-nb database. There is no requirement for the name to be unique. The logical router's UUID should be used as the unique identifier.

ports: set of weak reference to **Logical_Router_Port**s

The router's ports. This is a set of weak references, so a **Logical_Switch** must also refer to any given **Logical_Router_Port** or it will automatically be deleted.

default_gw: optional string

IP address to use as default gateway, if any.

Common Columns:

external_ids: map of string-string pairs

See **External IDs** at the beginning of this document.

Logical_Router_Port TABLE

A port within an L3 logical router.

A router port is always attached to a logical switch and to a logical router. The former attachment, which is enforced by the database schema, can be identified by finding the **Logical_Switch** row whose **router_port** column points to the router port. The latter attachment, which the database schema does not enforce, can be identified by finding the **Logical_Router** row whose **ports** column includes the router port.

Summary:

name	string
network	string
mac	string
Common Columns:	
external_ids	map of string-string pairs

Details:

name: string

A name for the logical router port. This name has no special meaning or purpose other than to provide convenience for human interaction with the ovn-nb database. There is no requirement for the name to be unique. The logical router port's UUID should be used as the unique identifier.

network: string

The IP address of the router and the netmask. For example, **192.168.0.1/24** indicates that the router's IP address is 192.168.0.1 and that packets destined to 192.168.0.*x* should be routed to this port.

mac: string

The Ethernet address that belongs to this router port.

Common Columns:

external_ids: map of string-string pairs

See **External IDs** at the beginning of this document.