OpenStack Neutron – Software Defined Networking w prywatnych chmuarch

Radosław Kujawa – radoslaw.kujawa@osec.pl

OSEC

14 czerwca 2017

OpenStack + Neutron

- OpenStack – nie tylko wirtualizacja CPU i pamięci, ale też pamięci masowej i sieci.
- Neutron a.k.a „OpenStack Networking” – zarządzanie infrastrukturą sieciową L2/L3 i usługami sieciowymi dla potrzeb chmury.
- Różne potrzeby klientów – konieczność stworzenia bardzo elastycznego mechanizmu wirtualizacji sieci.
- Współpraca z zewnętrzną infrastrukturą sieciową.

Funkcjonalności Neutrona

- Warstwa 2 - sterowniki ML2 („mechanism driver” np. Open vSwitch).
- Warstwa 3 - Layer 3 agents (routing, DHCP. . .).
- Foo as a Service
  - Firewall as a Service.
  - VPN as a Service.
  - Load balancer as a Service.
  - My-next-Neutron-extension as a Service.
  - . . .

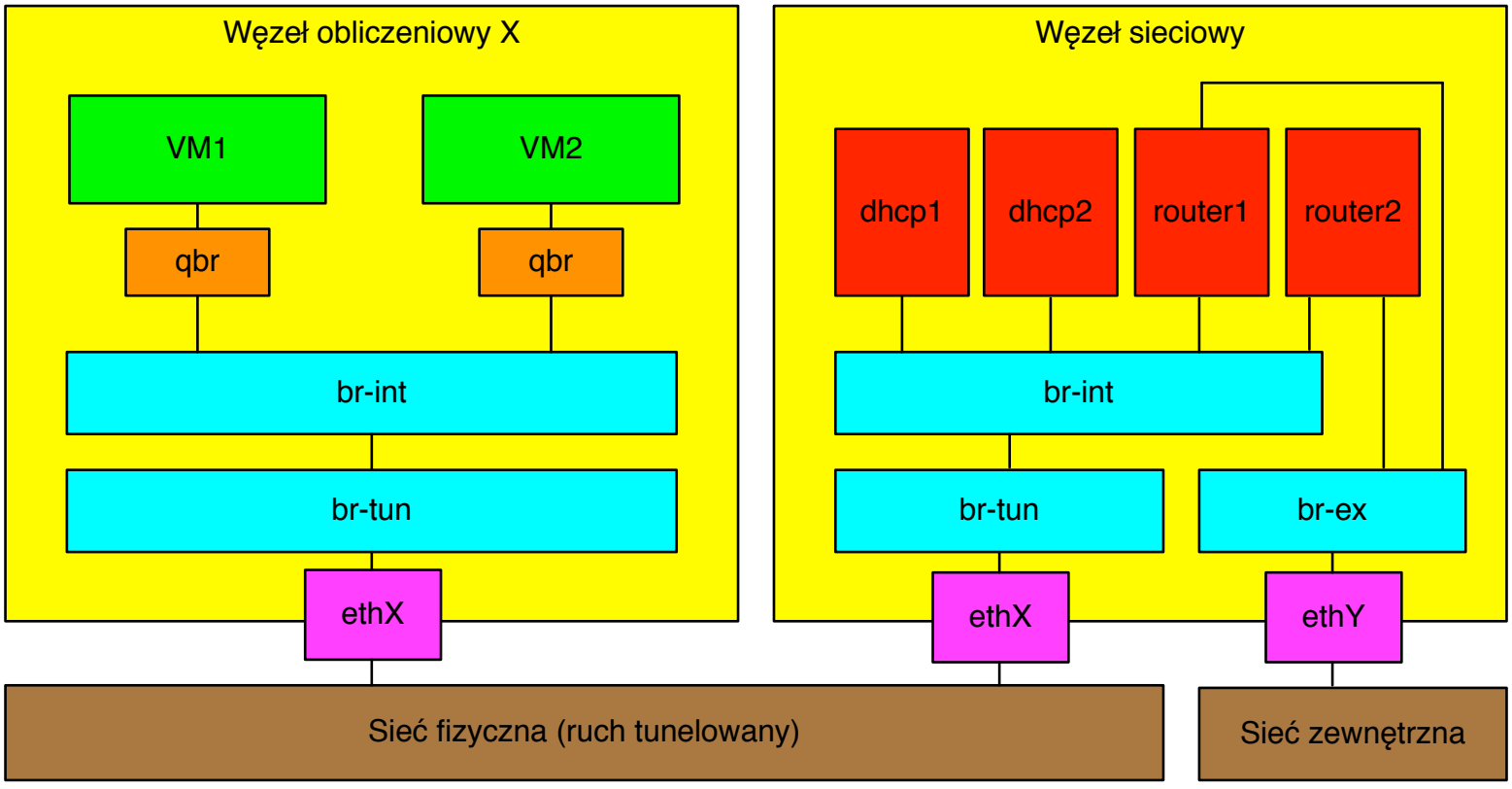
Architektura sieci w Neutronie

- Założenie: każdy projekt w OpenStack może posiadać zupełnie odrębne, niezależne sieci (oddzielna warstwa 2).
- Projekty w OpenStack mogą o sobie na wzajem nic nie wiedzieć.
- Sieci prywatne i publiczne.
- Możliwość routowania między sieciami.
- Mechanizmy separacji sieci („type driver”):
  - VLAN.
  - VXLAN.
  - GRE.
  - Geneve.
  - ...

Architektura z centralnym punktem dostępu do sieci zewnętrznej

- Domyślna architektura idealna pod potrzeby „hostingowe”.
- Prostota wdrożenia.
- Izolacja projektów – tunelowanie sieci prywatnych.
- Jeden punkt styku z siecią fizyczną na węźle sieciowym.
- Maszyny wirtualne posiadają interfejsy w sieciach prywatnych („projektowych”).
- Instancje maszyn wirtualnych *nie mogą* posiadać interfejsów przyłączonych bezpośrednio do sieci fizycznej (brak odp. bridge'y na węzłach obliczeniowych).

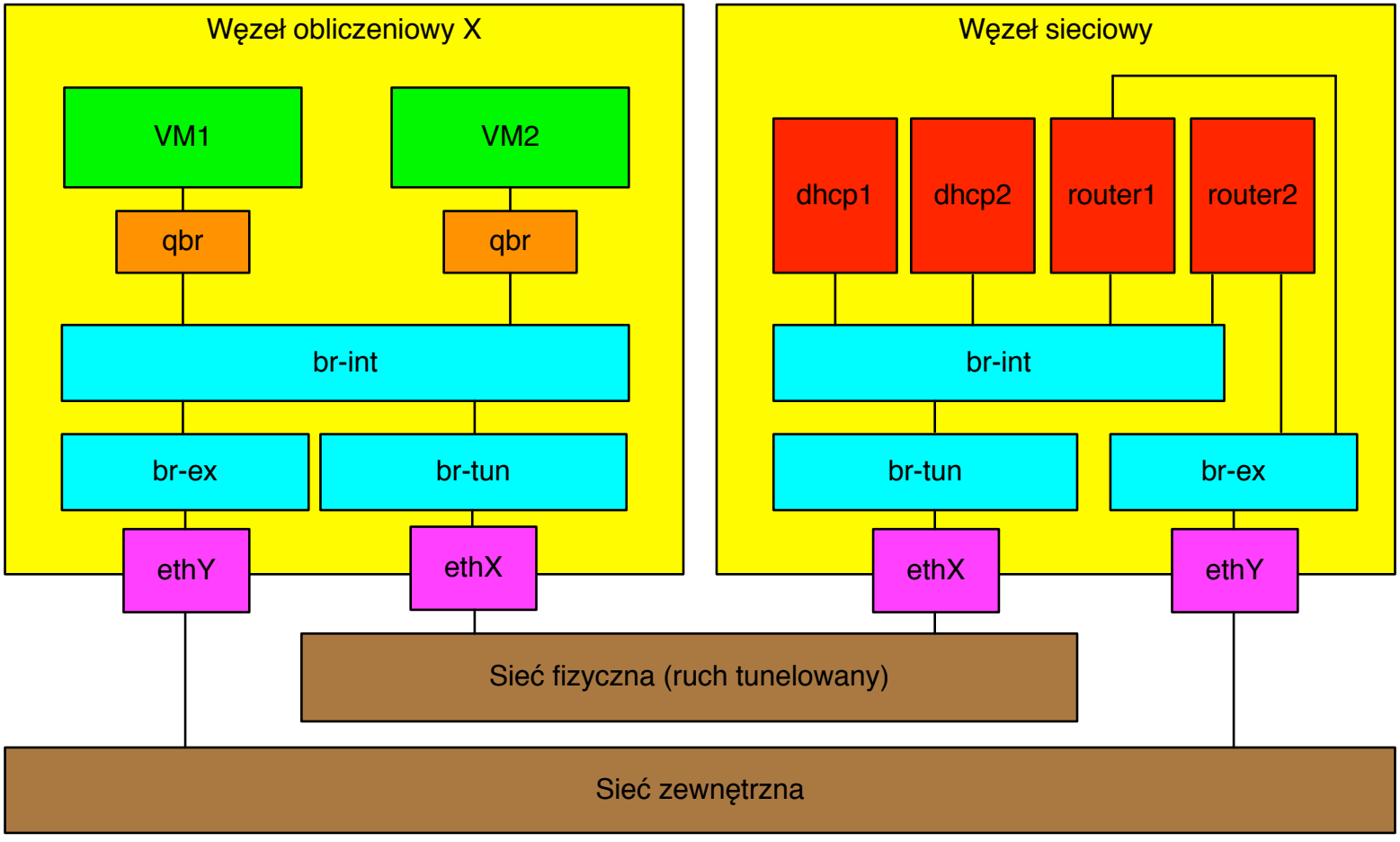
Architektura z centralnym punktem dostępu do sieci zewnętrznej



Architektura z dostępem do sieci zewnętrznej na każdym węźle obliczeniowym

- Alternatywny sposób konfiguracji Neutrona.
- Może być bardziej skomplikowany we wdrożeniu.
- Sieci „provider”.
- Type driver `flat` – dostęp maszyny wirtualnej do sieci fizycznej.
- Type driver `vlan`/`vxlan` – dostęp do odseparowanego segmentu sieci fizycznej.
- Separacja prywatnych sieci projektowych w dalszym ciągu możliwa.

Architektura z dostępem do sieci zewnętrznej na każdym węźle obliczeniowym



Integracja Neutrona z zewnętrznymi rozwiązaniami

- API REST oferowane przez Neutron.
- Pluginy do zarządzania warstwą 2 i 3.
  - Cisco Nexus.
  - Juniper.
  - VMware NSX.
  - ...
- Integracja z kontrolerami SDN i NFV.
  - OpenContrail.
  - OpenDaylight.
  - ...
- Możliwość wykorzystania Neutrona z Red Hat Virtualization.

Neutron a zastosowania telco/NFV

- Wymagany bezpośredni dostęp do sieci fizycznej.
- Jak najniższe opóźnienia w transmisji pakietów.
  - PCI passthrough.
  - SR-IOV (karty Intel/Mellanox/QLogic, od OpenStack Juno).
    - ML2 driver `sriovnicswitch` – sieci VLAN i flat.
  - DPDK (Open vSwitch data path, od OpenStack Mitaka).
- Service chaining (OpenStack Ocata) – obecnie wymaga Open vSwitch.

Demonstracja

- Kilka przykładów konfiguracji:
  - Demo: utworzenie sieci zewnętrznych.
  - Demo: utworzenie maszyny wirtualnej z interfejsem w sieci zewnętrznej.
  - Demo: utworzenie sieci prywatnej.
  - Demo: utworzenie maszyny wirtualnej z interfejsesm w sieci prywatnej.
  - Demo: utworzenie routera między siecią prywatną i zewnętrzną.
  - Demo: pływający adres IPv4.

Podsumowując

- Neutron jest elastyczny – możesz zaimplementować taką architekturę sieci jaka jest Ci potrzebna.
- Możliwość samodzielnego rozszerzania Neutrona przez pluginy.
- Wsparcie dla nowoczesnych standardów na różnych poziomach sieci – IPv6, SR-IOV, DPDK, itd.
- Jeśli masz inne potrzeby...
- Chcesz skonsultować swoją architekturę...
- Pragniesz zbudować środowisko *proof of concept*...
- Potrzebujesz nowego pluginu...
- Odezwij się do nas!

Koniec...

Dziękuje!
Czy są pytania?