Hardware Acceleration in an SDN/NFV World: MRV POC with Charter Communications

AusNOG 2016 Lightning Talk

John Jones (jjones@mrv.com)

Sept 2, 2016

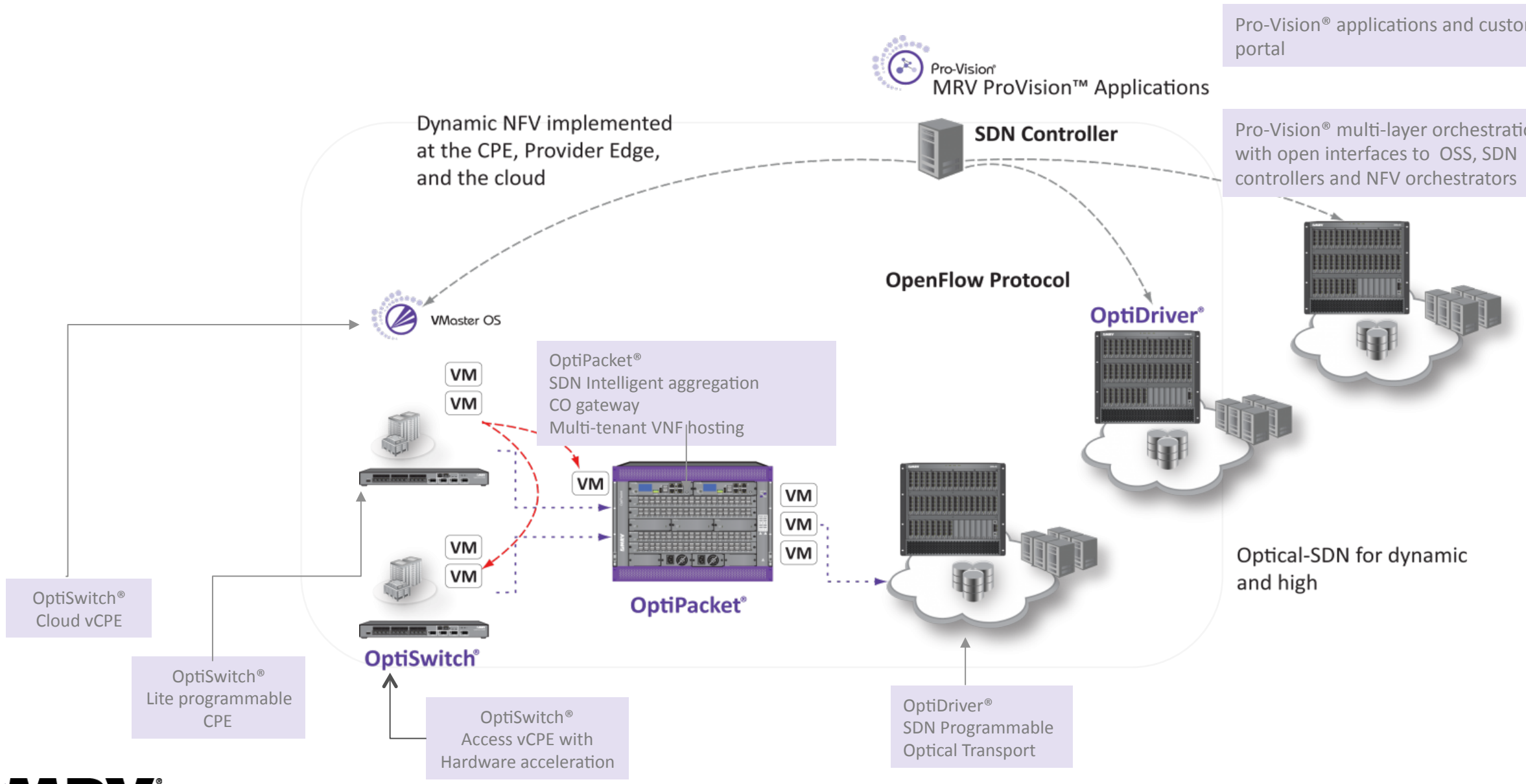
Overview

- MRV NFV POC with Charter in Denver, Colorado.

- We took an MRV Carrier Ethernet switch, which has a silicon based packet processor for 1 and 10 Gbps wire speed Carrier Ethernet services, and we added an x86 board where we ran managed router, managed security, and managed SIP services.

- The advantage to performing NFV at the CPE is that these virtualised network functions can be hardware accelerated using the packet processor on the CPE itself.

MRV's Metro-Optimized SDN/NFV Vision



Edge NFV – vCPE at the Customer's Premises

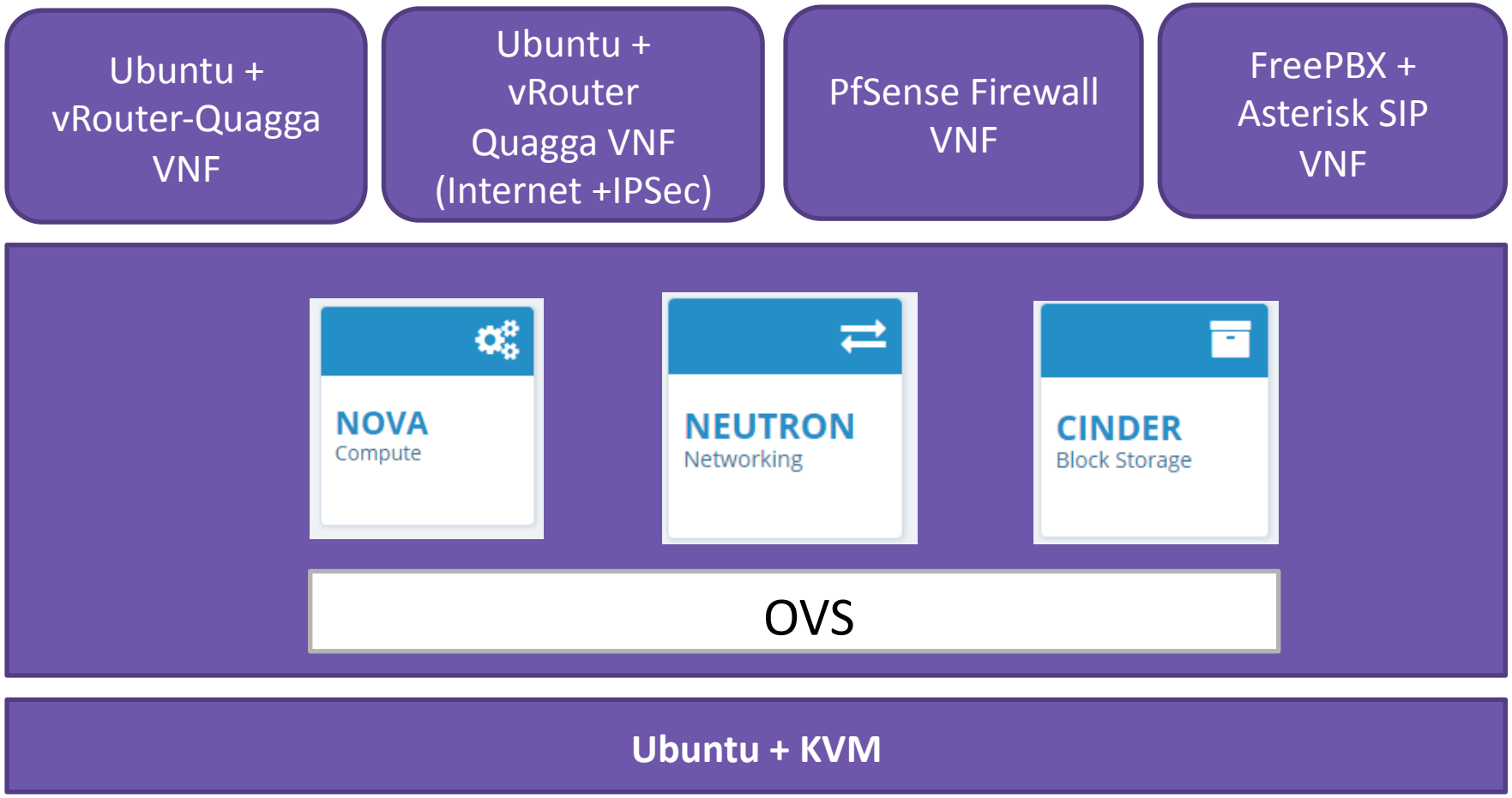
- Access-optimized server coupled with packet processor hardware assist.
- Latest Intel server processors - less power, more processing power
  - Performance options: Low (ATOM) / Medium (I7) / High (XEON +DPDK, SR-IOV)
  - Extendable RAM, SSD
- Latest packet processing hardware assist, 100M-10G platform capable of bringing up to 44G full wire speed to the NFV environment
- Based on OPNFV latest release – Brahmaputra
  - Linux (Ubuntu 14.10 LTS cloud server)
  - KVM, OVS for improved virtual networking
  - OpenStack Liberty Release
- Service Chaining Support
- Intelligent offload of VNF forwarding to the hardware
- Option for 4G/LTE wireless backup

Differentiating elements:

- Hardware acceleration for VM L2-L4 forwarding
- Fine-grained QoS
- Hardware-based flow classifier for efficient service chaining
- Zero-touch , remote deployment and service provisioning

OS-V Series

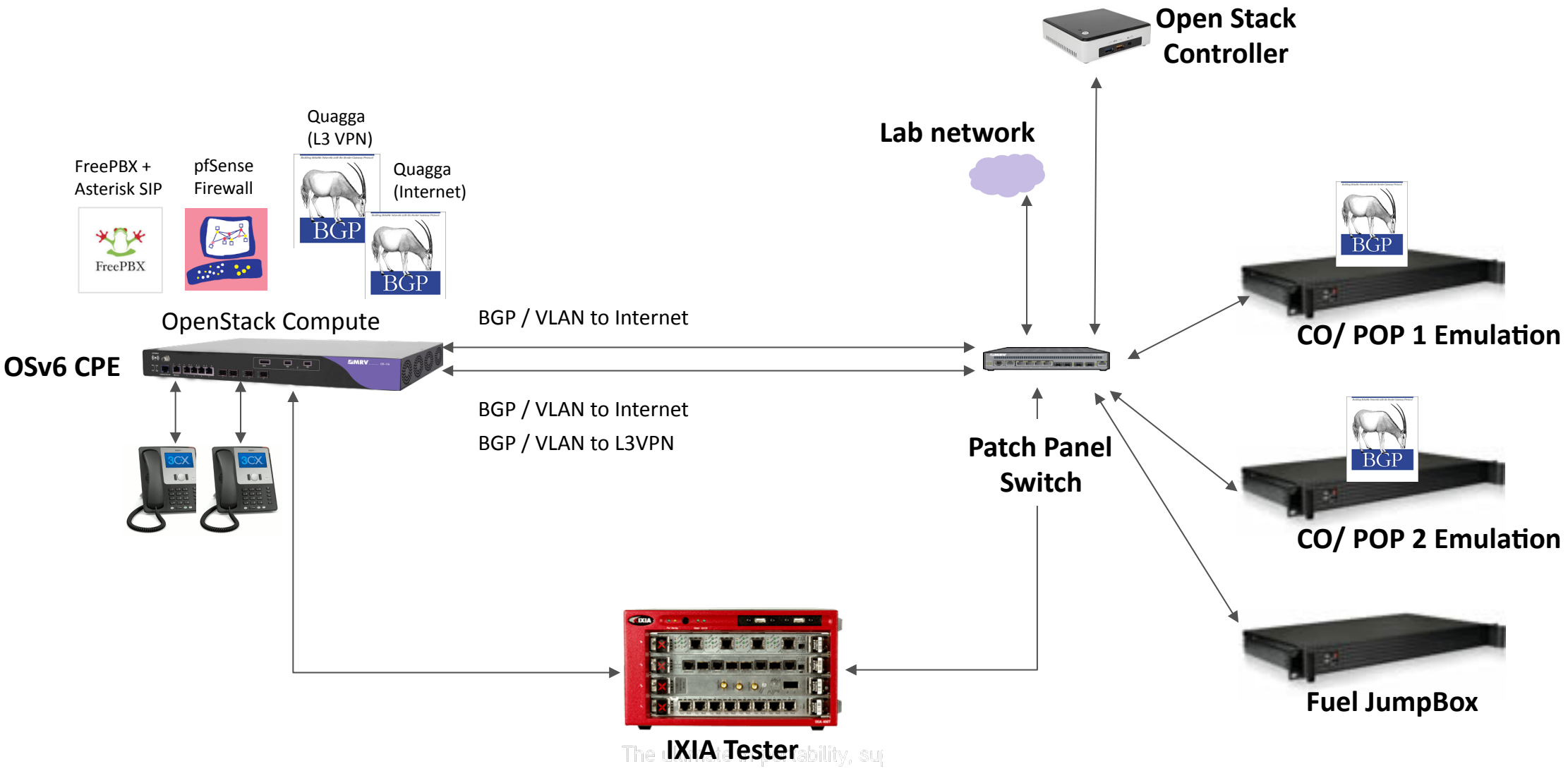
OS-V6 Compute Node Environment



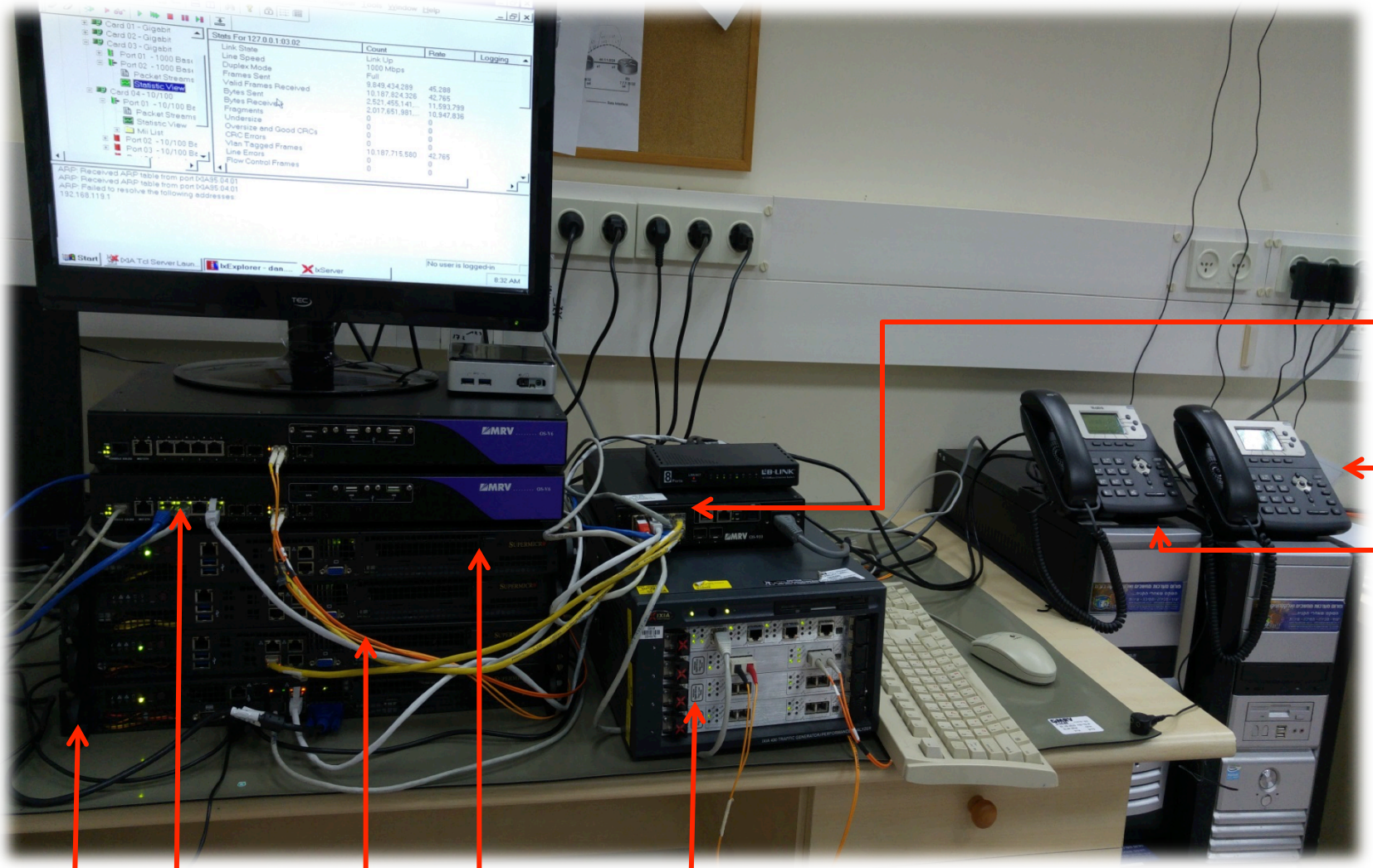
Charter vCPE Use Case

- **Managed WAN (router)**
  - Multiple hub and spoke sites via L3VPN services provided at Charter PE
  - Multiple WAN connections; combination of Charter and third-party connections
  - BGP
  - OSPF/IS-IS
  - Dual-homed internet services
  - An eye toward/to SD-WAN concepts/capabilities, e.g., via SD-WAN VNF suite (future)
- **Managed security**
  - Unified threat management capabilities
    - Antivirus
    - Content filtering
    - Anti-spam
  - Off-footprint IPSec tunnels, e.g., over the Internet
- **Managed voice services**
  - SIP trunk support, e.g., to Charter voice services
  - Others requirements TBD
- **Managed Carrier Ethernet MEF services (optional)**
  - Value add over the above layer 3 and security functions, e.g., via HW acceleration to MRV OptiSwitch
    - MEF CE 2.0 Services – EPL, E-LINE, E-LAN, E-Access

Demo setup



Setup


POP Patch Panel Switch
SIP Phone1
SIP Phone2
Fuel
vCPE
POP1
POP2
Ixia

OpenStack VIM

Open Stack used as the Virtual Infrastructure Manager (VIM) of the setup. Using Open Stack Horizon dashboard:

- Define locations per each customer and PoP site
- Images – which images are installed and can be instantiated as VMs
- Running instances – which VM instance runs on which compute node in which location,

  Show that on the OS-V6 we have 4 VMs running :
  Two instances of Quagga, pfsense FW and FreePBX
- Network topology – how the virtual topology looks like

Demo – Virtual Firewall Functionality

Connection to the management console of the pfSense firewall VM:

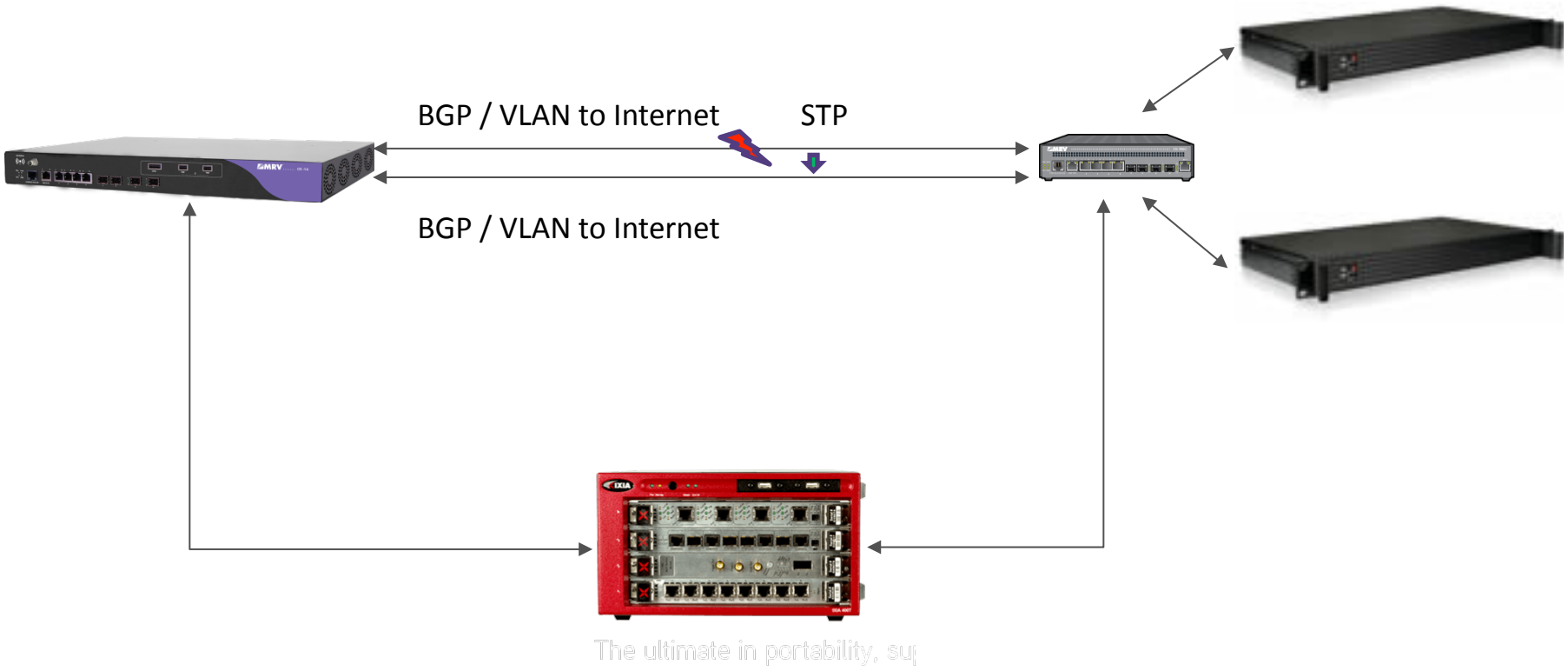
- Show the rules
- Show the IPSec tunnel
- Disable/Enable the IPSec tunnel
- Enable/Disable the rules

Demo – Virtual PBX Functionality

Demonstrate FreePBX functionality by dialing to the IP phones connected to the setup

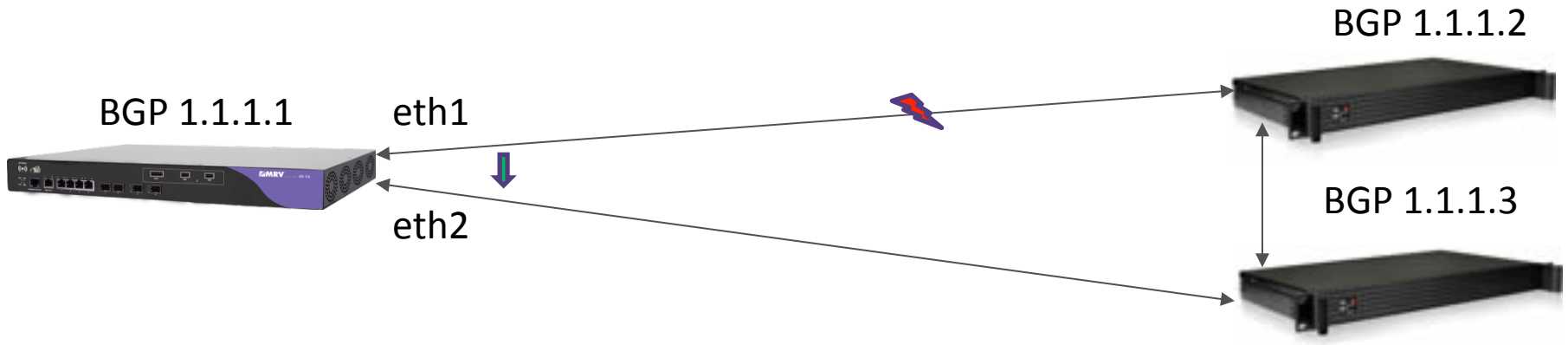
Demo – Layer 2 Protection

Demonstrate L2 protection.
When one of the physical uplinks is disconnected, the L2 protection switch is performed by STP on the OS-V6 and traffic is moved to the remaining uplink



Demo Step 5 – L3 Protection

L3 protection utilizing BGP failover.
When one of the VM's BGP sessions is disconnected, the L3 rerouting is performed by OS-V6 VM Linux and traffic moved to the remaining BGP session

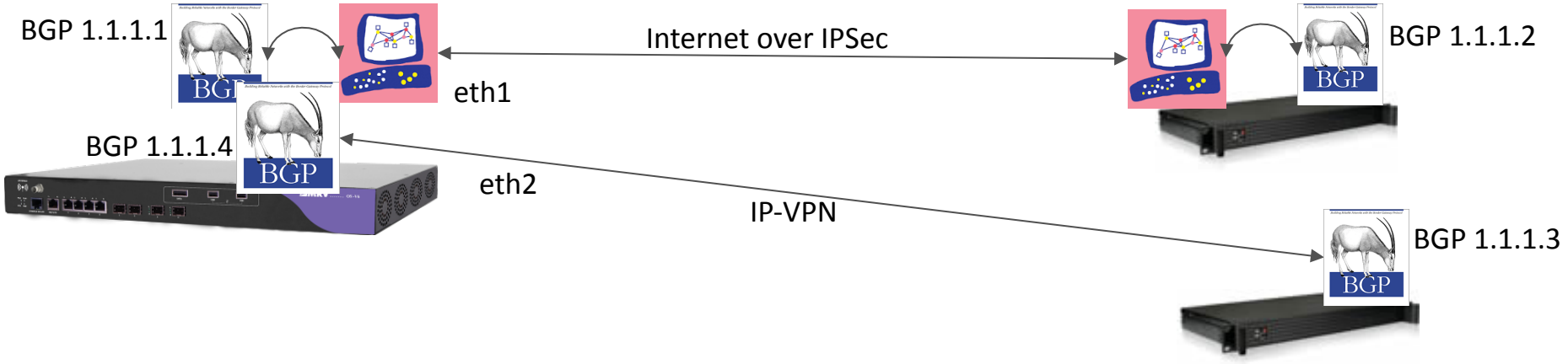


Demo – Multiple vRouters for SD-WAN

Demonstration of the ability to run two independent vRouter instances, each of which builds a different route.

One Quagga instance serves as a L3-VPN endpoint and creates a route via PoP1, whereas the second Quagga instance serves as an Internet connectivity endpoint and create a different route via PoP 2.

Since the Internet connectivity must be secured, the Internet Quagga is chained to the vFirewall that encapsulates the traffic in an IPSec tunnel.



www.mrv.com
info@mrv.com