SWISS IPv6 COUNCIL

ERNW providing security.

IPv6 in Virtualized Data Centers

Christopher Werny, cwerny@ernw.de

Enno Rey, erey@ernw.de

Who We Are

- Network (IPv6) geeks, working for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: www.insinuator.net

Motivation

- Increasingly customers are asking us whether they can use IPv6 within their virtualized environments.

- Mainly these questions center around:
  - Can we use IPv6 within the virtual machines?
  - What kind of security services can be implemented for IPv6?
    - E.g. IPv6 *First Hop Security* features in virtual switches.

Motivation

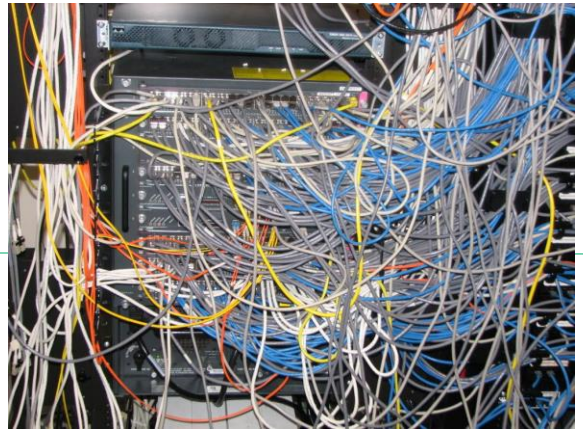
- Can we perform management operations of the virtual infrastructure over IPv6?
  - E.g. for an IPv6-only datacenter deployment.
- What kind of IPv6 support do these “new” network virtualization platforms have?
  - Microsoft HNV, VMware NSX etc.

Agenda

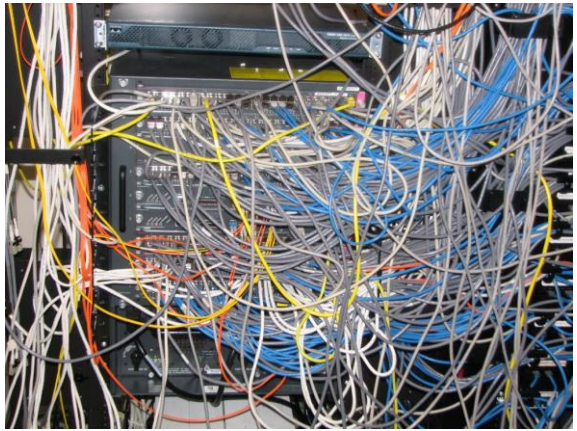
- This presentation is split into two parts.
- Part 1 is focusing on “traditional” hypervisors used for server virtualization and their respective virtual switches.
- Part 2 is focusing on network virtualization platforms.

Starting with Part 1...

"Traditional" Server Virtualization on several Hypervisor Platforms

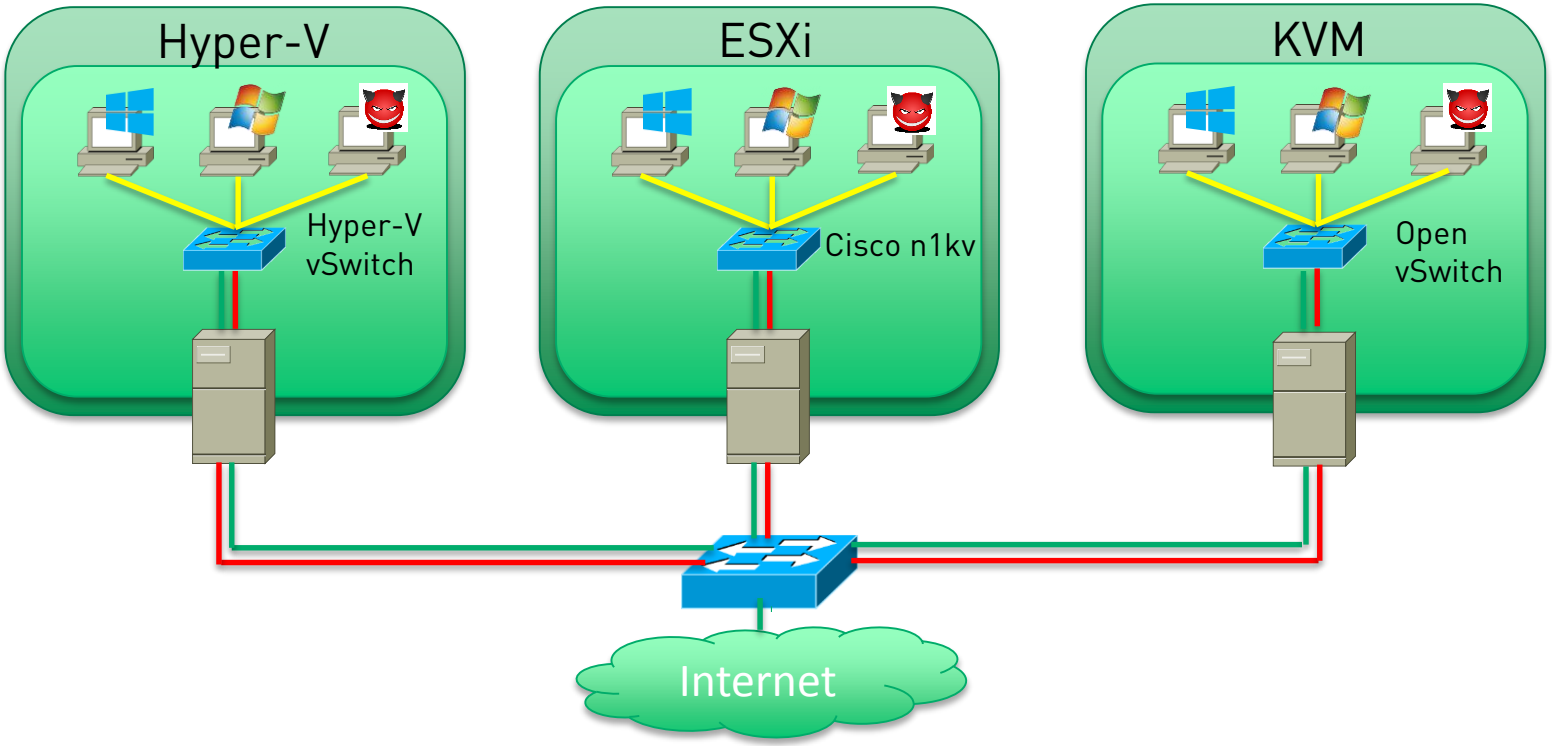


Lab Setup



- Three different types of Hypervisors
  - Windows Server 2012 R2 Hyper-V 3.0
  - VMware vSphere 6.0
  - Kernel-based Virtual Machine (KVM)
- … with three different types of virtual switches
  - Hyper-V vSwitch
  - Cisco Nexus 1000V
  - Open vSwitch

Lab Environment Overview



SWISS IPv6 COUNCIL

ERNW providing security.

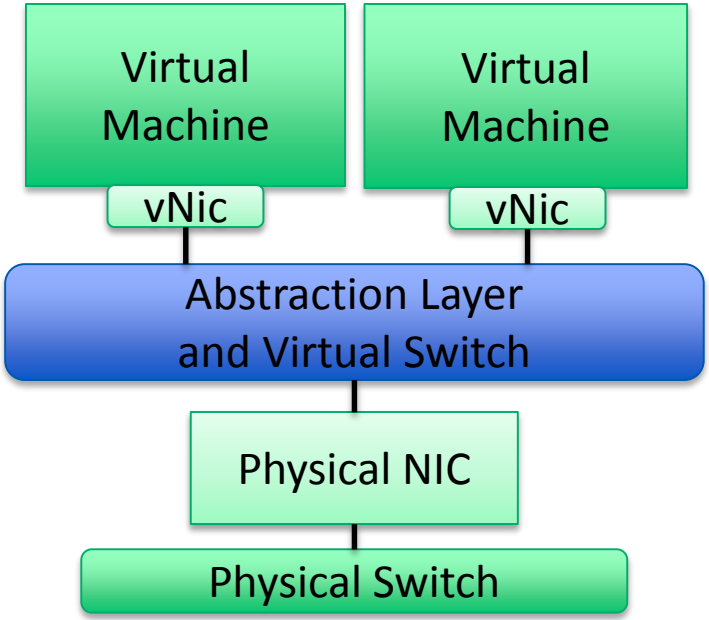
Microsoft Hyper-V 3.0

On Windows Server 2012 R2

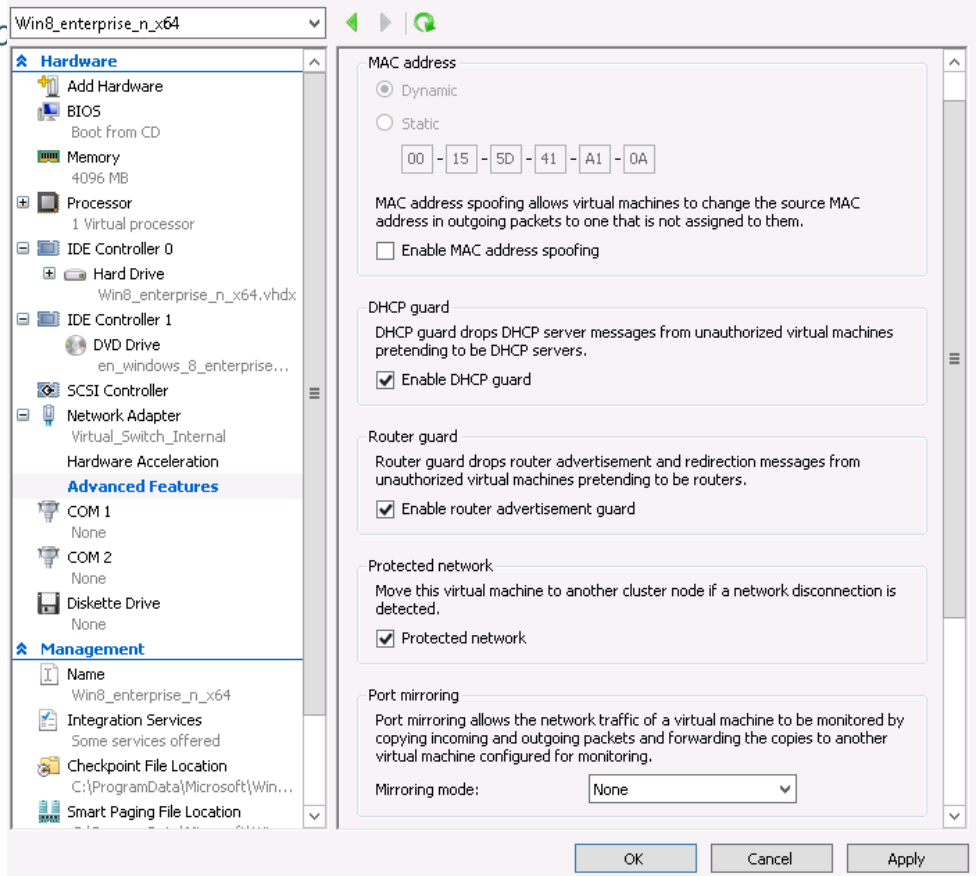
Management Capabilities

- Microsoft Hyper-V 3.0 has quite solid support of IPv6 for managing the hypervisor.
- Failover can be implemented over IPv6.
- Communication between the Virtual Machine Manager and the hypervisor can be realized over IPv6.

Hyper-V vSwitch FHS



- The Hyper-V vSwitch supports:
  - RA-Guard
  - DHCPv6 Guard
  - NDP Snooping capabilities
  - Extended/Stateful (IPv6) ACLs
    - Configurable via PowerShell.
- Details about the effectiveness of those features can be found in [1].


Win8_enterprise_n_x64
Hardware
Add Hardware
BIOS
Boot from CD
Memory
4096 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Win8_enterprise_n_x64.vhdx
IDE Controller 1
DVD Drive
en_windows_8_enterprise...
SCSI Controller
Network Adapter
Virtual_Switch_Internal
Hardware Acceleration
Advanced Features
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
Win8_enterprise_n_x64
Integration Services
Some services offered
Checkpoint File Location
C:\ProgramData\Microsoft\Win...
Smart Paging File Location
MAC address
Dynamic
Static
00 - 15 - 5D - 41 - A1 - 0A
MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.
Enable MAC address spoofing
DHCP guard
DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
Enable DHCP guard
Router guard
Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.
Enable router advertisement guard
Protected network
Move this virtual machine to another cluster node if a network disconnection is detected.
Protected network
Port mirroring
Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.
Mirroring mode:
None
OK
Cancel
Apply

SWISS IPv6 COUNCIL

ERNW providing security.

vSphere 6 with Nexus 1000v

Management Capabilities

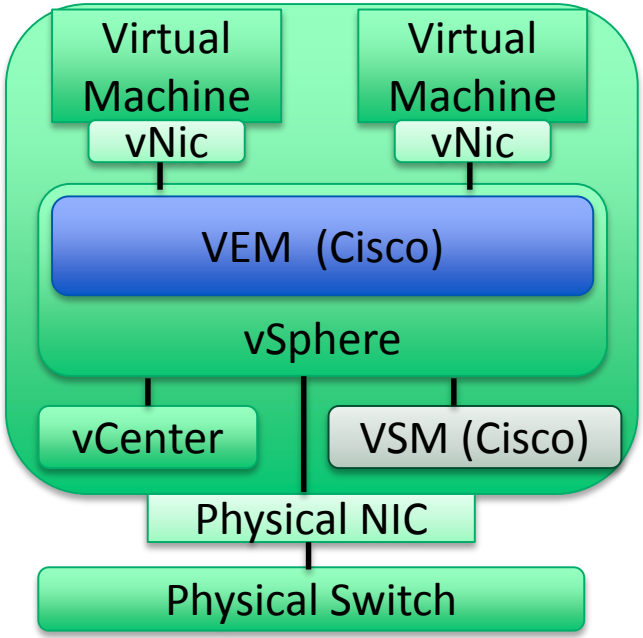
- VMware made huge improvements in regards to IPv6 support for management functionality in the vSphere 6.0 release.

- Overall most of the features can be run over IPv6, but there are still some limitations:
  - vSphere Authentication Proxy works only over IPv4 [2].
  - Management interfaces used for HA must be configured with IPv4 _or_ IPv6. Running both in parallel is not supported [3].
  - Virtual SAN transport network is IPv4-only[4].

IPv6 Feature Capability Overview

Feature	vSphere 5.5	vSphere 6.0
PSC/SSO, Inventory Services	not supported	supported
Common Logging Infrastructure	not supported	supported
vCenter Converter	not supported	supported
vMotion	Supported	supported
vCLI	not supported	supported
vAPI	not supported	supported
Host Profiles	not supported	supported
vSphere Management Assistant	not supported	supported
vSphere Update Manager	not supported	supported

Nexus 1000v IPv6 FHS



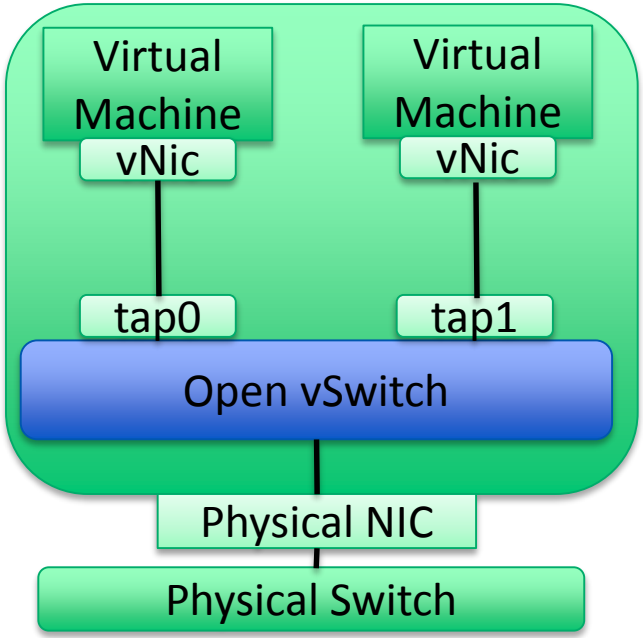
- Unfortunately, no IPv6 FHS features available on the Nexus 1000v.
- The only option you have is using port based ACLs for filtering IPv6 traffic
  - IPv6 ACLs were introduced in 5.2(1)SV3(1.1).
- Will be coming "soon".

SWISS IPv6 COUNCIL

ERNW providing security.

KVM with Open vSwitch

KVM & Open vSwitch

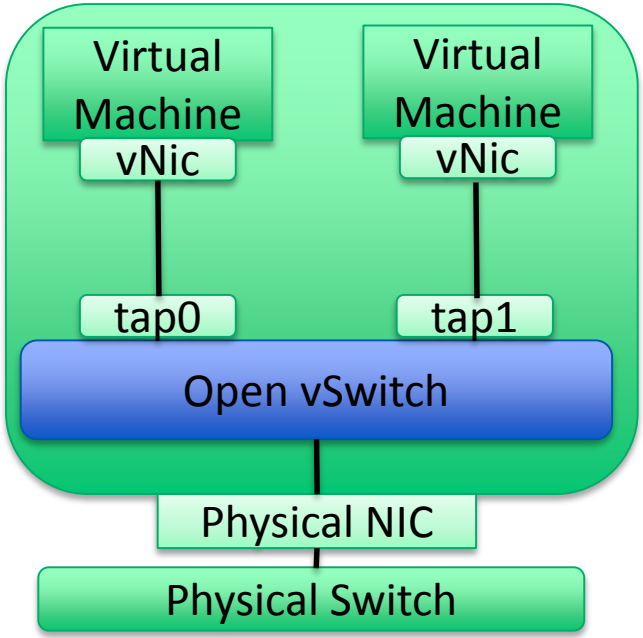


- Ubuntu 14.04.2 LTS
  - 3.13.0-32-generic
- QEMU
  - Version 2.0.0
- OpenFlow
  - 1.4
- Open vSwitch
  - 2.3.1

Management Capabilities

- The management capabilities heavily depend on the specific management platform used for KVM.
  - E.g. in Cloudstack environments the KVM agent can only communicate over IPv6 with the management server beginning in 4.5.0 [5].

Open vSwitch FHS



- Unfortunately, no IPv6 FHS features available.
- Only IPv6 ACL based behavior based on flow entries matching could be configured.
  - E.g. to block malicious RAs.

Interim Conclusion

- IPv6 support for the management plane gets closer to IPv4.

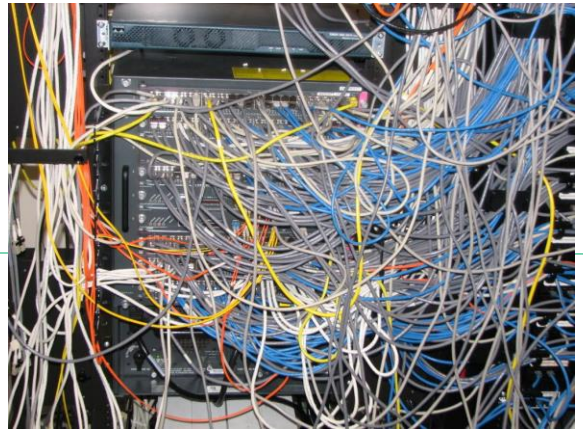
- IPv6 security capabilities are slowly increasing in virtual switches but it is still a long way to go until we have (IPv6 security) feature parity with the physical world.

SWISS IPv6 COUNCIL

ERNW providing security.

Continuing with Part 2...

Network Virtualization Platforms



SWISS IPv6 COUNCIL

ERNW providing security.

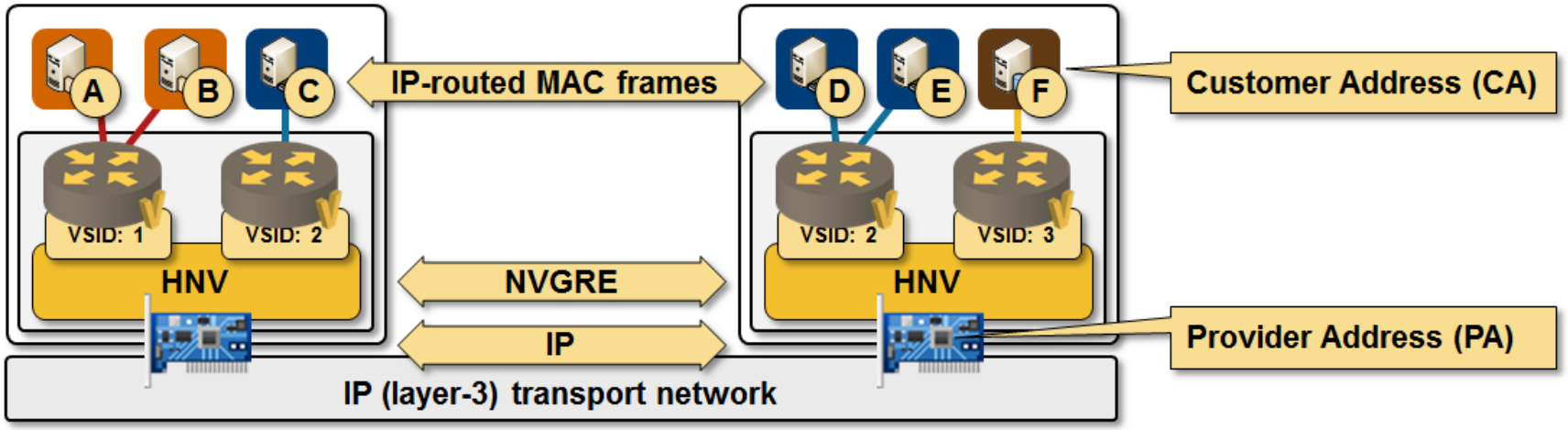
Hyper-V Network Virtualization

On Windows Server 2012 R2

Hyper-V Network Virtualization

- Part of Microsoft's SDN strategy.
- Provides the possibility to present virtualized network architectures to virtual machines.
- Abstracted from the underlying physical network infrastructure.
- Every virtualized network is isolated from each other and can only communicate over a dedicated virtual gateway (if desired).

Hyper-V Network Virtualization



- Picture kindly borrowed from Ivan Pepelnjaks (@ioshints) IPv6 Microsegmentation presentation at the IPv6 Security Summit

IPv6 Capabilities

- HNV has extensive IPv6 support for management and tenant networks and provides nearly full feature parity between IPv4 and IPv6.
- This include management as well as using IPv6 as a transport protocol for the NVGRE tunnels.
- The only restriction is that a VM Network created with HNV can either be IPv4 or IPv6 enabled. Using both protocols in the same VM Network is currently not supported[6].
  - A VM could still use *dual stack*, but then each stack has to be member of a different VM Network.

SWISS IPv6 COUNCIL

ERNW providing security.

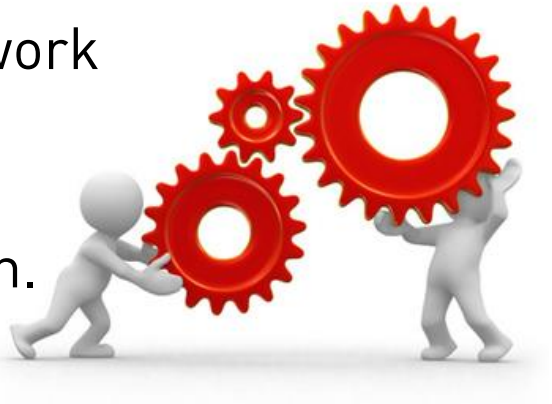
VMware NSX for vSphere Hypervisor 6.x

VMware NSX for vSphere

- Overlay Virtual Networking Solution
  - Provides logical Layer-2 and Layer-3 segments
  - Distributed VM-NIC firewalls
  - Network services (VPN Gateway, NAT, Load balancers)

- Abstracted from the underlying physical network infrastructure.

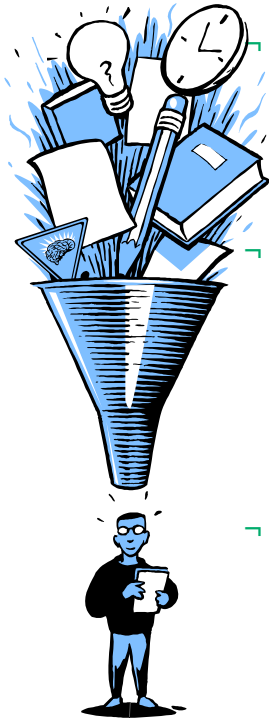
- Similar to HNV but uses VXLAN encapsulation.



IPv6 Capabilities

- As with vSphere 6.0, VMware made huge improvements in regards to IPv6 support in NSX 6.x but there are still some limitations:
  - VMware NSX Edge Router does not support dynamic routing protocols for IPv6 (e.g. OSPFv3).
  - VMware NSX Distributed Router does not support IPv6.
  - A complete list of limitations can be found in [7].

Summary



- Management & control plane (over IPv6) capabilities are getting better and it shouldn't take that long until we have full feature parity.
- IPv6 security features on virtual switches are still behind in comparison with the physical world
  - Microsoft's Hyper-V virtual switch currently provides the best support of FHS features.
- Even though network virtualization platforms are a quite new technology, the overall IPv6 support for management and tenant networks is pretty good, with small limitations on different platforms.

There's never enough time...

THANK YOU...

...for yours!

Thanks to our Sponsors

Infoblox
CONTROL YOUR NETWORK
- and -
FORTINET
FAST. SECURE. GLOBAL.
- with partner -
SIDARION
networking & security

inkon
Get your IT-Expert
BROCADE
ARROW
Five Years Out

DIGICOMP

eb-Qual

pragmaticsolutions gmbh

BLUECAT

SWITCH

NUTANIX

itrain
THE ESSENCE OF IT

asecus
securing your business

Questions & Discussion

References

- [1] https://www.troopers.de/events/troopers15/482_ipv6_first_hop_security_in_virtualized_environments/
- [2] https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.install.doc/GUID-EA920335-2608-4127-9B57-DB3809BA4BB9.html
- [3] https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.avail.doc%2FGUID-A7F75A33-7FA8-480E-BDF8-4C5D672F08DD.html

References

- [4] https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.virtualsan.doc/GUID-AFF133BC-F4B6-4753-815F-20D3D752D898.html
- [5] https://issues.apache.org/jira/browse/CLOUDSTACK-7121
- [6]http://blogs.technet.com/b/privatecloud/archive/2013/11/18/hyper-v-network-virtualization-architecture-and-key-concepts.aspx

References

- [7] https://www.edge-cloud.net/2015/03/ipv6-in-vsphere-6/

Guys, we would love to see you in Heidelberg!

March, 14-18 2016
Heidelberg, Germany
Make the world a safer place.

FOLLOW THE NEWS
@WEareTROOPERS

MORE INFO, EXTENSIVE ARCHIVE & REGISTRATION @ WWW.TROOPERS.DE

Questions?

- You can reach us at:
  - erey@ernw.de, www.ernw.de
  - cwerny@ernw.de, www.ernw.de
- Our blog:
  - www.insinuator.net
- Follow me at:
  - @Enno_Insinuator