Networking Guide for Lenovo Converged HX Series Nutanix Appliances (CNOS Switch Firmware)

Last Update: October 2019

Describes the recommended networking topology using Lenovo RackSwitch top-of-rack switches

Shows how to configure Lenovo RackSwitches using CNOS firmware

Explains methods to connect the cluster switches to core network switches

Describes vSwitch settings for VMware vSphere

William Lloyd Scull

B. Scott Lorditch

LENOVO PRESS

Abstract

This paper details preferred network designs and topologies for use with the Lenovo® Converged HX Series Nutanix Appliance hyperconverged platform. This platform is based upon Nutanix software and Lenovo System x servers with direct-attached storage.

The network designs in this paper use Lenovo's Ethernet switching products and the new Cloud Networking Operating System (CNOS) firmware with which they operate. This document is based on the Lenovo Press paper, *Networking Guide for Lenovo Converged HX Series Nutanix Appliances*, which presented designs based on the previous Enterprise Network Operating System (ENOS) generation of Lenovo switching firmware.

The intended audiences for this paper include server, storage, and networking engineers and salespeople, working for Lenovo as well as for its customers and business partners.

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

http://lenovopress.com

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction

Lenovo Converged HX Series is a highly resilient Nutanix software-based hyperconverged compute and storage platform, designed to support virtual environments, such as VMware vSphere, Microsoft Hyper-V, and AHV. AHV (Acropolis Hypervisor) is the virtualization solution built into Nutanix Acropolis, based on KVM, Linux's Kernel-based Virtual Machine.

Figure 1 The Lenovo Converged HX5510 Nutanix appliance

The partnership announced between Lenovo and Nutanix for the Lenovo HX systems will bring reduced complexity in server, storage, networking and virtualization in data centers of all sizes. By combining the industry-leading reliability of Lenovo enterprise hardware systems with Nutanix, the software market-leader in hyperconvergence, enterprises will be able to bring greater efficiency and agility to their data centers.

The Lenovo Converged HX Series portfolio will enable you to:

- Simplify IT Infrastructure by integrating server, storage, networking, and virtualization in a centrally managed appliance, with an intuitive, consumer-grade friendly interface.
- Reduce costs and gain quicker ROI by breaking down silos enabling customers to easily add capacity and scale as future needs demand.
- Deliver greater reliability and service with Lenovo enterprise server innovation rated #1 in reliability and customer satisfaction.

Lenovo Converged HX Series hyperconverged architecture

Lenovo Converged HX Series appliances are available in a range of hardware platforms from remote office/branch office (ROBO) to compute-intensive, based on the application requirements of customers.

The HX Series architecture includes a storage controller, running in a virtual machine, called the Controller VM (CVM). This VM is run on every HX Series node in a cluster to form a highly distributed, shared-nothing converged infrastructure. All CVMs actively work together to aggregate storage resources into a single global pool that can be leveraged by user virtual machines running on the HX Series nodes.

The storage resources are managed by the Nutanix Distributed File System (NDFS) to ensure that data and system integrity is preserved in the event of node, disk, application, or hypervisor software failure. NDFS also delivers data protection and high availability functionality that keeps critical data and VMs protected.

Complete hyperconvergence includes the interconnection of the cluster nodes as a basic element of the complete solution – and is critical to both the performance and the availability of the HX Series appliances.

Networking and network design are critical parts of any distributed system in the data center. A resilient network design is important to ensure connectivity between HX CVMs, for virtual machine traffic, and for vSphere management functions, such as ESXi management and vMotion. HX Series appliances come standard with redundant 10 GbE NICs which can be used by the virtualized OS for resilient virtual networking.

Lenovo RackSwitch Ethernet switches are recommended for the interconnection of HX Series cluster nodes. The server links can be either 25 GbE or 10 GbE.

These switches are designed for the data center and have redundancy in both power and cooling. They provide low latency, and implement required data center features, such MC-LAG (or Lenovo Networking's Virtual Link Aggregation Group - VLAG) for the creation of a single logical switch from a pair of physical switches.

The basic design overview of the switches for interconnecting HX Series nodes is shown in Figure 2.

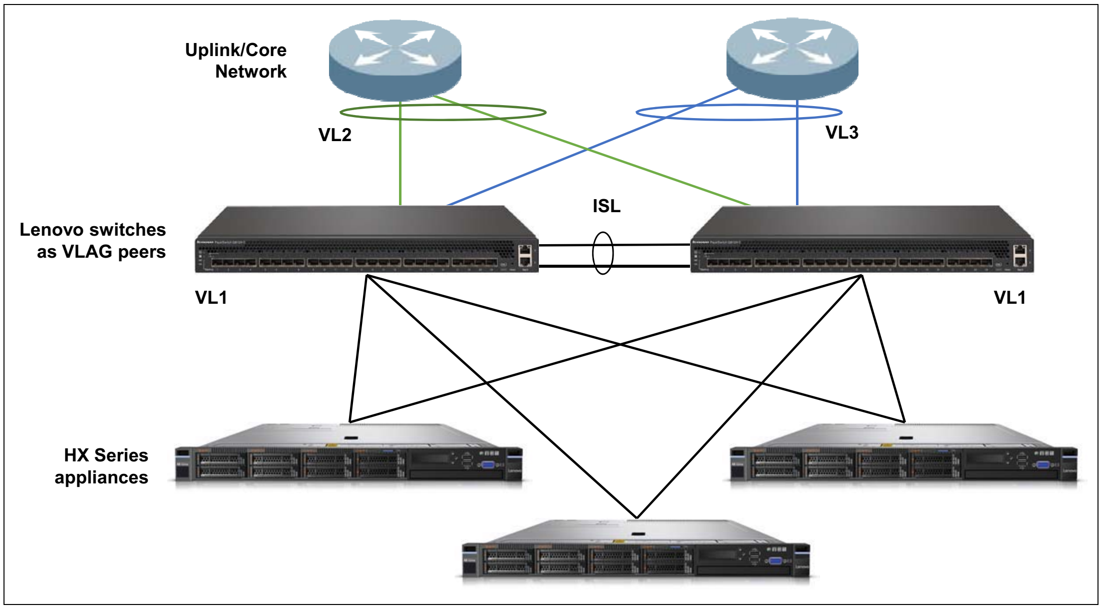


Figure 2 Basic design overview

For the basic interconnect, two Lenovo switches are placed in an MC-LAG configuration (called VLAG, similar to Cisco Nexus vPC) which enables this switch pair to act as a single logical switch over which single link aggregations can be formed between ports on both hardware switches. The HX Series appliances are connected redundantly to each of the VLAG peer switches and rely on VMware vSwitch features to spread the traffic over the two VLAG peers.

Connection to the uplink core network is facilitated by the VLAG peers, which present a logical switch to the uplink network, enabling connectivity with all links active and without a hard requirement for spanning-tree protocol (STP). The link between the two VLAG peers is an inter-switch link (ISL) and provides excellent support of east-west cluster traffic between HX nodes. The VLAG presents a flexible basis for interconnecting to the uplink/core network, ensures the active usage of all available links, and provides high availability in case of a switch failure or a required maintenance outage. (The remaining switch carries all the traffic.)

About this paper

This paper is intended to describe the best practices for interconnection of HX nodes running VMware vSphere as the operating system. While other variants are available on the HX Series appliances, such as Hyper-V and Acropolis AHV, vSphere is still the most common OS in the data center and thus will be the focus of this paper. Considerations for Hyper-V and AHV are included in the appendices.

This document is based on the Lenovo Press paper, *Networking Guide for Lenovo Converged HX Series Nutanix Appliances*, LP0546, available from:

https://lenovopress.com/lp0546

This new paper revised from LP0546 to show the commands necessary to implement this design using a Lenovo switch running the new Cloud Networking Operating System (CNOS) software, with versions starting with 10.x. The command syntax in the new CNOS software is different from what has been used to this point, although the features are mostly identical.

G8124 removed: CNOS will not be available on the G8124 switch and so configurations with that switch have been removed from this paper.

The paper takes you through the following steps:

1. "Preparing the switches"

   Verify that the prerequisites for network connectivity are in place, including identifying required existing infrastructure servers, preparing IP addresses, and verifying switch firmware levels and proper vSwitch configuration.

2. "Configuring the switches as VLAG peers" on page 12

   Configure the pair of identical Lenovo RackSwitch switches (NE1032 or G8272 for 10 GbE on the server links; NE2572 for 25 GbE server links) as MC-LAG/VLAG peers such that they behave as a single logical switch for the purposes of external connections, and provide an inter-switch link (ISL) which can also be used for intra-cluster communication.

3. "Connect the VLAG to your existing core network" on page 18

   In this section, we provide considerations and best practices for connecting the interconnected HX cluster to an existing customer network infrastructure.

This document provides a number of design examples. Find the design which best fits your environment, fill in the locally relevant parameters (such as IP addresses, system names according to local naming rules, and relevant VLANs, if required), if necessary with the cooperation of your networking administrator, and follow the configuration steps described for the appropriate design.

Additional configuration details for using multiple VLANs for the guest VMs can be found in "Appendix D: Considerations for multiple VLANs for guest virtual machines" on page 25. Details on a Layer 3 (routed) configuration can be found in "Appendix E: Connecting to the upstream network – L3 considerations" on page 26. Customers may require topologies using these features but this is not a Lenovo or Nutanix requirement.

Commands with blue text: Some of the commands have **`text in blue`**. This refers to configuration variables which need to be configured according to your local environment.

Preparing the switches

To connect the HX Series nodes in a local cluster using the Lenovo Networking switches, the following preparation steps are required:

1. Ensure you have a minimum of three HX Series appliances running VMware ESXi with minimum 2x10 GbE NIC ports on each node.
2. Ensure you have the required physical and virtual IP address information and additional IP addresses for each node
3. Configure the vSwitches on the cluster connections as “Route based on originating virtual port” and connect them to the VMNICs of the 10/25 GbE network
4. Ensure you have two of the same model of Lenovo Networking switches with Lenovo CNOS firmware 10.0 or later. Required OS and Boot image can be downloaded from `http://support.lenovo.com`.

The following subsections take you through the details of each of these steps.

Lenovo Converged HX Series appliances imaged with VMware ESXi

The following versions of VMware ESXi are supported:

- VMware ESXi 5.5 U2
- VMware ESXi 5.5 U3
- VMware ESXi 6.0 U1

Lenovo installs the Acropolis hypervisor (AHV) and the Nutanix Controller VM at the factory before shipping a node to a customer. To use a different hypervisor (ESXi or Hyper-V) on factory nodes or to use any hypervisor on bare metal nodes, the nodes must be imaged in the field.

For information about imaging, see the following documents:

- Reference Architecture for Workloads using the Lenovo Converged HX Series Nutanix Appliances

  `https://lenovopress.com/lp0084`

- Nutanix Field Installation Guide

  `https://portal.nutanix.com/#/page/docs/details?targetId=Field_Installation_Guide-v3_3:Field_Installation_Guide-v3_3`

Acropolis Hypervisor or Hyper-V? This document will concentrate on the interconnection of VMware vSphere nodes. For AHV, see “Appendix B: Acropolis Hypervisor considerations” on page 24.

Obtain the required IP address information

The appropriate network (gateway and DNS server IP addresses), cluster (name, virtual IP address), and node (Controller VM, hypervisor, and IPMI IP address ranges) parameter values needed for installation.

Network addresses

You will need the following existing information for the network during the cluster configuration:

- Default gateway
- Network mask
- DNS server
- NTP server

You should also check whether a proxy server is in place in the network. If so, you will need the IP address and port number of that server when enabling Nutanix support on the cluster.

Node IP addresses

Each node in the cluster requires three IP addresses, one for each of the following components:

- IPMI/IMM interface (recommended to be a separate physical network and IP range)
- Hypervisor host (same layer 2 network as the controller VM)
- Controller VM (same layer 2 network as the hypervisor host)

Hypervisor host and CVM IP addresses need to be in the same Layer 2 network. IPMI/IMM should be in a separate management network, if possible.

All Controller VMs and hypervisor hosts must be on the same subnet. No systems other than the Controller VMs and hypervisor hosts can be on this network, which must be isolated and protected.

System management

The HX Series appliances also require an IMM/IPMI connection to the management network. It is recommended to connect the switch management ports to this same network, which ideally is physically separated from the 10/25 GbE networking production traffic (at a minimum in a different IP address range).

You will need to provide two switch IP addresses:

- Switch 1 management IP address
- Switch 2 management IP address

It is recommended that you access the switches over the out-of-band (OOB) management ports from a separate management network address range. Normally, these addresses will be provisioned in the management network to which the HX node IMM and other management systems are connected.

Configure the vSwitches on the cluster connections

There is no specific VMware ESXi NIC bonding requirement for the NICs on the HX Series appliances in this configuration. Instead, the NICs are left un-bonded and the traffic distribution over the NICs is controlled by the vSwitches connected to the VMNICs configured as described in this section.

The available options in ESXi for NIC load balancing are as follows:

- Route based on originating virtual port (default, recommended)
- Route based on IP hash

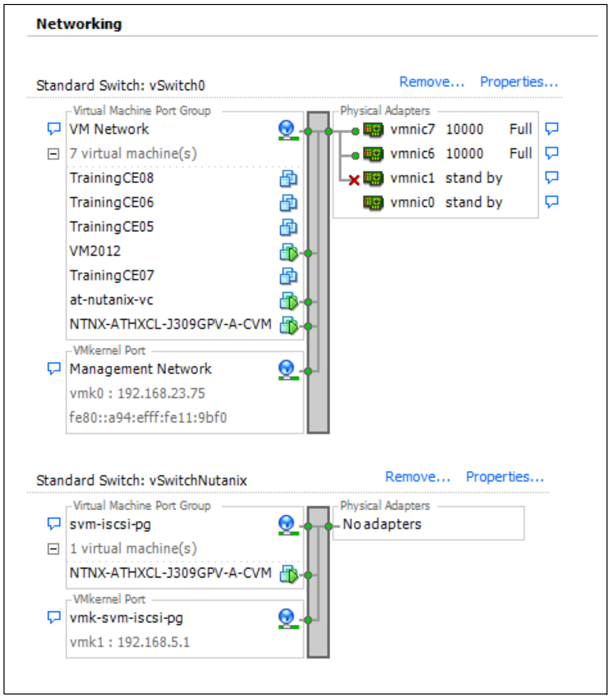
- Route based on source MAC hash
- Route based on physical NIC load – called load-based teaming or LBT (VDS only)
- Explicit failover order

The recommended option for vSwitch VSS is “Route based on originating virtual port”.

The route based on originating virtual port option is the default load balancing policy and has no requirement for advanced switching configuration, such as LACP. These attributes make it simple to implement, maintain, and troubleshoot. A route based on the originating virtual port requires 802.1q VLAN tagging for secure separation of traffic types.

The main disadvantage of this option is that there is no load balancing based on network load. This results in traffic from a single VM always being sent to the same physical NIC, unless there is a failover event caused by a NIC or upstream link failure. This is less of an issue with the high throughput 10GbE network interfaces of the HX Series platform.

Figure 3 on page 8 shows the default NIC configuration in ESXi:



Networking

Standard Switch: vSwitch0 — Remove... Properties...

Virtual Machine Port Group
VM Network
7 virtual machine(s)
TrainingCE08
TrainingCE06
TrainingCE05
VM2012
TrainingCE07
at-nutanix-vc
NTNX-ATHXCL-J309GPV-A-CVM

VMkernel Port
Management Network
vmk0 : 192.168.23.75
fe80::a94:efff:fe11:9bf0

Physical Adapters
vmnic7 10000 Full
vmnic6 10000 Full
vmnic1 stand by
vmnic0 stand by

Standard Switch: vSwitchNutanix — Remove... Properties...

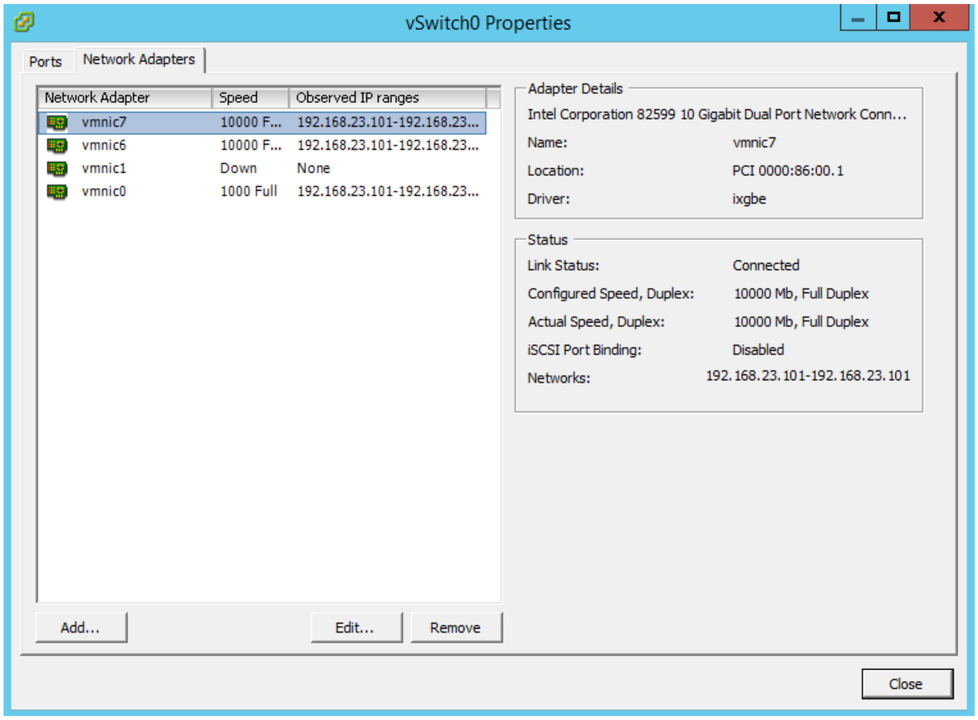
Virtual Machine Port Group
svm-iscsi-pg
1 virtual machine(s)
NTNX-ATHXCL-J309GPV-A-CVM

VMkernel Port
vmk-svm-iscsi-pg
vmk1 : 192.168.5.1

Physical Adapters
No adapters

Figure 3 ESXi default NIC configuration

Figure 4 shows the physical 10 GbE NICs connected to vSwitch0.



Network Adapter	Speed	Observed IP ranges
vmnic7	10000 F...	192.168.23.101-192.168.23...
vmnic6	10000 F...	192.168.23.101-192.168.23...
vmnic1	Down	None
vmnic0	1000 Full	192.168.23.101-192.168.23...

Adapter Details

Intel Corporation 82599 10 Gigabit Dual Port Network Conn...

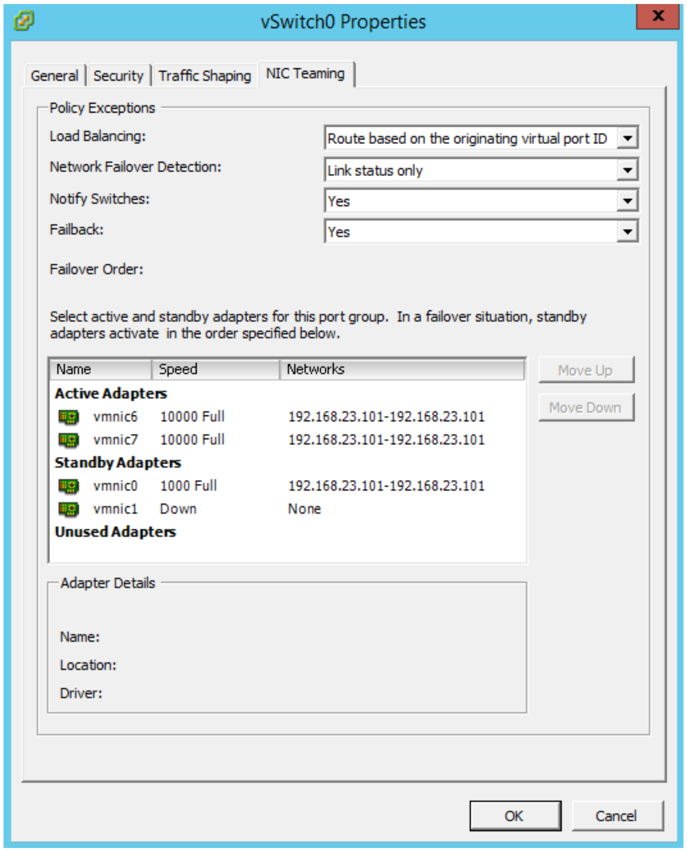
Name:	vmnic7
Location:	PCI 0000:86:00.1
Driver:	ixgbe

Status

Link Status:	Connected
Configured Speed, Duplex:	10000 Mb, Full Duplex
Actual Speed, Duplex:	10000 Mb, Full Duplex
iSCSI Port Binding:	Disabled
Networks:	192.168.23.101-192.168.23.101

Figure 4 vSwitch0 properties showing connected network adapters

Figure 5 on page 9 shows the required load balancing option for vSwitch0, to which the HX Series appliances are connected to.



Policy Exceptions

Load Balancing:	Route based on the originating virtual port ID
Network Failover Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes

Failover Order:

Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.

Name	Speed	Networks
Active Adapters		
vmnic6	10000 Full	192.168.23.101-192.168.23.101
vmnic7	10000 Full	192.168.23.101-192.168.23.101
Standby Adapters		
vmnic0	1000 Full	192.168.23.101-192.168.23.101
vmnic1	Down	None
Unused Adapters		

Adapter Details

Name:

Location:

Driver:

Figure 5 vSwitch0 NIC teaming

For configuration using the VMware Virtual Distributed Switch (VDS), see “Appendix C: VMware Virtual Distributed Switch considerations” on page 24.

Prepare the switches for implementation

Lenovo recommends the following switches for interconnection of HX Series appliances:

- For clusters up to 16 nodes:

  Two Lenovo ThinkSystem NE1032 switches which have 32 ports of 10Gb Ethernet using SFP+ transceivers. (Note that there are no high-bandwidth uplink ports and so several of the 10Gb ports will need to be aggregated together to provide upstream connectivity.)

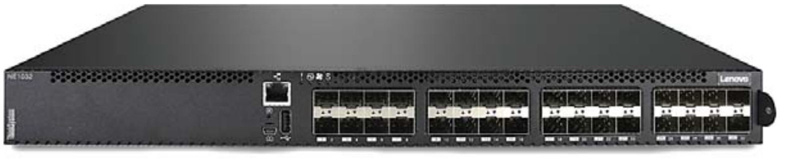


Figure 6 Lenovo ThinkSystem NE1032

- For clusters up to 35 nodes:

  Two Lenovo RackSwitch G8272 switches running the latest CNOS software (a minimum of version 10.0).

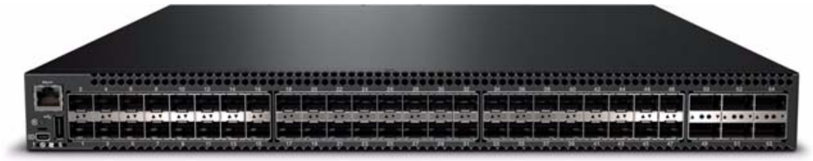


Figure 7 Lenovo RackSwitch G8272

  The RackSwitch G8272 is a datacenter-class 72-port SFP+ switch/router with 6 QSFP+ 40GE ports. It can support either 1 GbE or 10 GbE links on the SFP+ ports and 40GbE or 4x 10 GbE on the QSFP+ ports. It’s also available in rear-to-front and front-to-rear airflow models as with the NE1032. It has hot-swappable redundant power supplies and fans by default, and boosts power usage.

- For clusters of up to 25 nodes with 25Gb NICs.

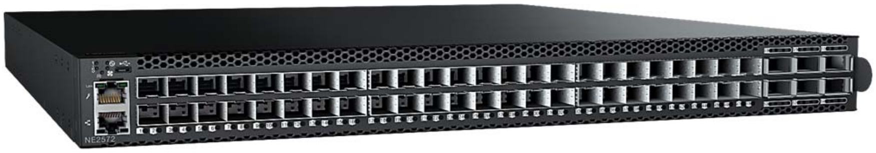


Figure 8 Lenovo ThinkSystem NE2572

  The NE2572 has 48 ports which can be configured to run at 10Gb or 25Gb (in groups of four adjacent ports). It also has six 100Gb uplink ports. Support for using some or all of these uplink ports at 40Gb is planned for later in 2018.

- Clusters beyond 35 nodes

  Even larger HX cluster configurations can be supported using larger products, such as the RackSwitch G8296 and/or combinations of Lenovo switches in scalable spine-leaf configurations. Such configurations are supported but are beyond the scope of this document. Please contact your local Lenovo networking team for support.

The CNOS software is available on the G8296 and also on the G8332 (from February 2017) 40Gb switch, which can be used as a spine switch in a large cluster.

Figure 9 Lenovo RackSwitch G8296

Figure 10 shows an example of a spine-leaf configuration, which - thanks to the high port-density of Lenovo RackSwitch switches - enables low-latency interconnect of a large number of HX Series appliances using a minimal number of switches.

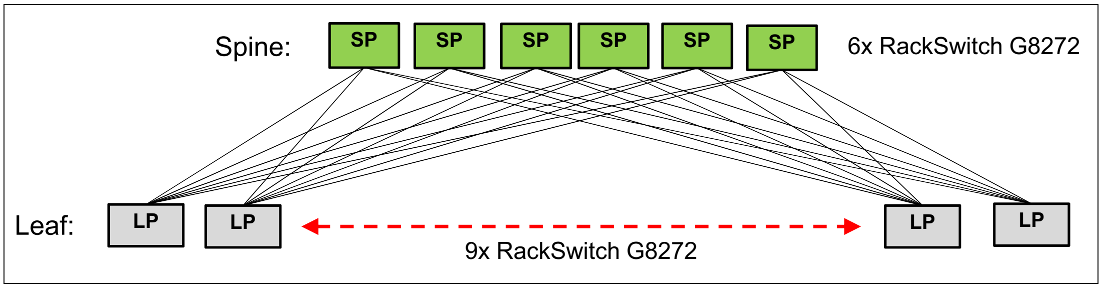


Figure 10 Example spine-leaf configuration

First-time access of the Lenovo switches requires initial setup. The factory default settings permit initial switch administration through only the built-in serial port. All other forms of access require additional switch configuration before they can be used. Remote access using the network requires the accessing terminal to have a valid, routable connection to the switch interface. The client IP address may be configured manually, or an IPv4 address can be provided automatically through the switch, using a service such as DHCP or BOOTP relay.

To manage the switch through the management ports, you must configure an IP interface for each management interface, as follows:

1. Connect to the switch via the serial port and log in.
2. Enter Global Configuration mode.

   ```
   RS G8272> enable
   RS G8272# configure terminal
   ```

3. Configure a management IP address and mask from the management network range

   ```
   RS G8272(config)# interface mgmt 0
   RS G8272(configigipif)# ip address <management interface IPv4 address>/mask bits
   RS G8272(configigipif)# vrf context management
   RS G8272(configigipif)# ip route 0.0.0.0/0 <management gateway IP address>
   RS G8272(configigipif)# exit
   ```

Enable Discovery of newly deployed Nutanix nodes

As part of the preparation of the switches, the following commands should be entered into the configuration to allow multicast traffic to be flooded throughout the environment. This is used by Nutanix to automatically discover newly installed nodes in a cluster.

```
ip igmp enable
ip igmp snoop enable
ip igmp snoop vlan <VLAN ID (1-4094)>
```

The last command above will need to be entered multiple times, once for each VLAN in use in the environment. Also, these commands must be entered on each switch that is part of that environment. There are similar but not identical commands that are required on other vendors' switching hardware if it is in use as part of the cluster network.

Configuring the switches as VLAG peers

Both the clustering of HX Series nodes (server-to-server communication, including the storage networking and vSphere functions) and the connection of the clustered HX Series nodes and the customer uplink/core network can take place on the same switches.

While 1 GbE cluster connections are officially supported, Lenovo recommends the use of dual-port 10 GbE or 25 GbE NIC bandwidth for the interconnection of HX Series nodes. Nutanix best practices documents also recommend leaving the 1Gb ports (if any) idle.

The examples in this document show single 10 GbE links to the HX Series nodes from each of the pair of switches, but multiple 10 GbE connections to each switch can be implemented using the same design.

The central element of our recommended topology for the interconnected HX Series cluster are two Lenovo 10 or 25 GbE Ethernet switches set up to behave as a single logical switch, using the Virtual Link Aggregation protocol. For a physically separate management network, Lenovo offers a number of datacenter-class 1 GbE switches, such as the G8052 or G7028/52, which can implement the 1 GbE IMM/IPMI server links and the 1 GbE management links of the Lenovo 10 GbE switches.

Virtual Link Aggregation Group (VLAG) is Lenovo Networking's proprietary implementation of the MC-LAG protocol, similar to vPC on Cisco Nexus switches.

A full VLAG implementation consists of the following three elements:

- A pair of the same type of switches joined with a redundant inter-switch link (ISL) and configured with the VLAG protocol to form a single logical switch, on which aggregations can be implemented over ports on both physical switches.

  The formation of a single logical switch from two physical ones using VLAG is done using the MAC address tables of both switches being synchronized over the ISL. The two members of this pair of switches actively running the VLAG protocol are referred to as *VLAG peers*.

- A third element which supports link aggregation protocol such as LACP.

  This device need not support the VLAG protocol directly, but only standard link aggregation. An aggregation is formed on this device by taking at least two ports of the NIC or switch and "bundling" them together locally. The remote end of the link aggregation is then "split" over the two VLAG peers. This device connecting to our VLAG peers using link aggregation is referred to as a *VLAG client*.

> **Note:** It is recommended that you *do not* connect the HX Series nodes running vSphere as VLAG clients. This is because such a configuration requires the use of the VMware distributed virtual switch (DVS) to configure LACP on the NICs, and the standard vSwitch cannot do LACP.
>
> The VLAG is, however, important for the connectivity to the uplink/core network, as we will see in "Connect the VLAG to your existing core network" on page 18

VLAG ensures that all links are active and that the traffic is balanced over the links using link aggregation features, without the need for implementing the spanning-tree protocol (which would block any links causing a loop). As a result, while every VLAG implementation is in fact a triangle, and thus a loop, the VLAG protocol ensures that a loop will not occur, thus making the use of spanning-tree optional in such environments.

Figure 11 shows an example of 2 VLAG instances with two other switches as the VLAG clients (on the bottom).

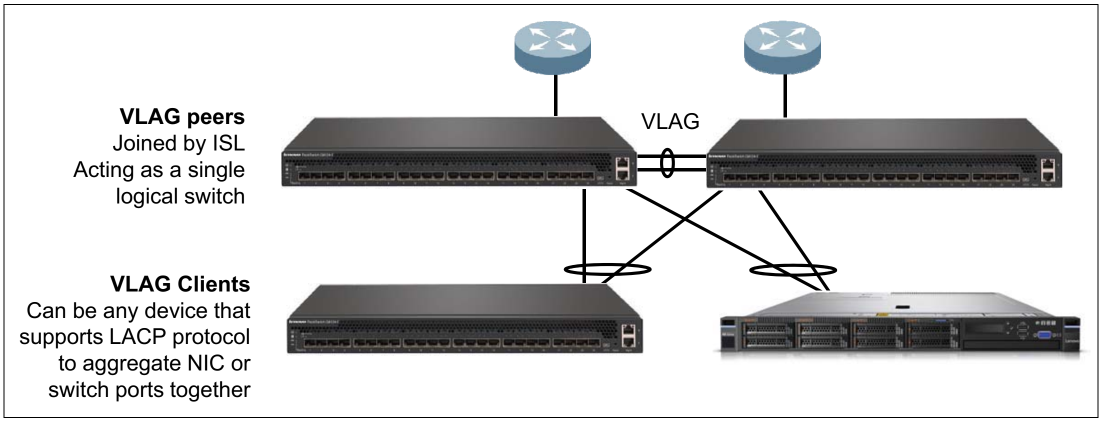
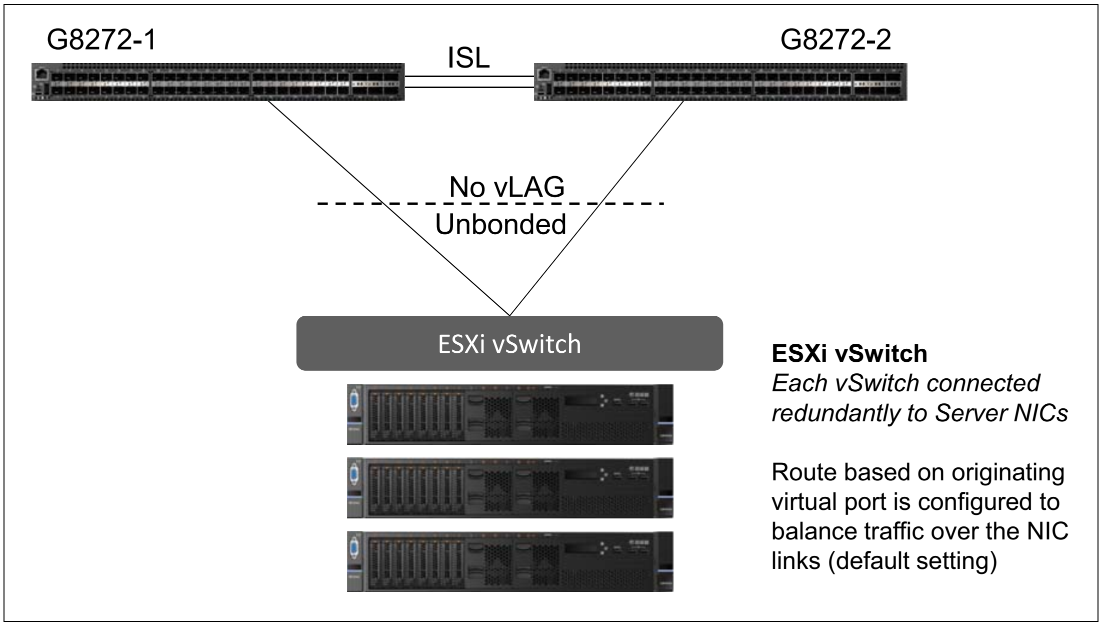


Figure 11 VLAG example topologies to both servers and switches

Configure the host side of the switch configuration

For our HX Series cluster connection we will configure our two Ethernet switches as VLAG peers to ensure redundant connection points from the HX host, but not place the NIC ports in a team or bond, as is shown in Figure 12 on page 14.



ESXi vSwitch
Each vSwitch connected redundantly to Server NICs

Route based on originating virtual port is configured to balance traffic over the NIC links (default setting)

Figure 12 VLAG peers providing redundant uplinks to the HX Series host

The first step is to configure the pair of Lenovo switches as VLAG peers so that both switches are interconnected and act as a logical single switch for the purposes of connecting other switches. This will also provide a direct connection between the switches to ensure the traffic can efficiently be transferred between HX Series cluster nodes ("east-west" traffic), and well as enabling the ability to do a link aggregation across physical switches, which is a great advantage for the uplink connection to the core network. With VLAG, the loss of one of the switches and/or the ISL will force all HX traffic over the remaining switch in standalone mode.

The steps to set up VLAG between the two identical Lenovo switches are as follows:

Commands with blue text: Some of the commands have **`text in blue`**. This refers to configuration variables which need to be configured according to your local environment.

1. Choose a minimum of 2x 10 GbE (or 25 GbE) SFP+ ports on each switch for the redundant inter-switch link (ISL).

   Sizing tip: In normal VLAG operation, the ISL is used only for synchronization of MAC address tables of the VLAG peers. However, in case of the loss of an uplink to the uplink/core network, the ISL can in some cases be used to carry the production traffic, and thus needs to be sized accordingly. Therefore it is recommended that you size the ISL according to the number of HX nodes connected to the VLAG peers. A good rule of thumb is half the total downlink bandwidth for the ISL.

   For example, if there are eight HX nodes connected (totaling 80 Gb/sec) then the ISL should have at least 40 Gb/sec of bandwidth. Or if there are eight HX nodes connected at 25 GbE (totalling 200GbE) then the ISL should be at least 100 GbE

   Remember that all VLANs configured toward the HX nodes also must be added to the ISL ports, in case of redirection of uplink traffic over the ISL.

2. Connect these ports in parallel, using copper or fiber components. For example, connect port 3 on switch1 to port 3 on switch2, and port 4 on switch1 to port 4 on switch2.

For details on the cabling and distance requirements, please see the Lenovo Networking Products and Options Catalog:

http://www.lenovo.com/images/products/system-x/pdfs/datasheets/lenovo_networking_catalog_ds.pdf

3. Access the switch and log in.
4. Access Enable Privilege:

```
G8272-1 # enable
```

5. Enter Global Configuration Mode:

```
G8272-1 # configure terminal
```

6. Disable spanning tree protocol *globally* on both switches (not on a per-port basis)[1]

```
G8272-1 (config)# spanning-tree mode disable
```

7. To test that STP is disabled, run:

```
G8272-1 # show span
```

The STP BPDUs from the uplink core network will continue to be forwarded through the Lenovo switches. In this case we are STP passive. The VLAG protocol will ensure the absence of STP loops as long as it is configured correctly.

8. Enable Link-layer Discovery Protocol on both the switches. This is useful for verifying device connectivity using the `show lldp remote-device` command.

Note: Ideally this will be done for all ports, not only for the link between the peer vLAG switches. VMware virtual switches can participate in LLDP as do hardware switches from most vendors.

```
G8272-1 (config)# interface Ethernet 1/1-53
G8272-1 (config)# lldp receive
G8272-1 (config)# lldp transmit
```

9. Create ISL LACP aggregation switch 1

The VLAG peer switches share a dedicated ISL for synchronizing VLAG information and cross-connect. Use of a single ISL link is possible, but not recommended. The use of the VLAG health check over the management network is optional, but recommended.

```
/* first create the aggregated interface and set it to block all traffic until
lacp is up*/
G8272-1 (config)# interface port-channel 1000
G8272-1 (config-if)# shut
G8272-1 (config-if)# lacp suspend-individual
G8272-1 (config-if)# no shut
G8272-1 (config-if)# exit

/* then add ports to it and configure it */
G8272-1 (config)# interface Ethernet 1/53-54
G8272-1 (config-if)# switchport mode trunk
G8272-1 (config-if)# channel-group 1000 mode active
G8272-1 (config-if)# exit
```

[1] In normal VLAG operation, the spanning-tree protocol is not required, because the connection is a logical point-to-point connection of two elements. However, without spanning tree there is no protection in case of misconfigured aggregations or an incomplete VLAG configuration which can lead to a loop and possible broadcast storm and network outage. Please proceed with caution and follow local networking policies. Spanning-tree is compatible with VLAG and can be configured if network security policies require it – please see the application guide for the switch for further details.

10. Create VLAG tier and health check for switch 1

```
G8272-1 (config)# vlag tier-id 1
G8272-1 (config)# vlag hlthchk peer-ip 10.0.0.2 vrf management
G8272-1 (config)# vlag isl port-channel 1000
G8272-1 (config)# exit
```

11. Create ISL LACP aggregation switch 2

    This is done with the identical commands as those used on switch 1 (step 9)

12. Create VLAG tier and health check for switch 2

```
G8272-2 (config)# vlag tier-id 1
G8272-2 (config)# vlag hlthchk peer-ip 10.0.0.1 vrf management
G8272-2 (config)# vlag isl port-channel 1000
G8272-2 (config)# exit
```

    Now the two switches are configured as VLAG peers, and are thus acting as a single logical switch. This enables high-availability active-active connections between the switches and other devices, while maintaining two separate control instances (in contrast with switch stacking, in which a single control instance is used over all participating switches). This means that when one of the switch peers is lost (for example, during a reboot after a firmware update), the other will continue to forward all the remaining traffic until the peer returns to the VLAG.

13. Enable VLAG on both switches:

```
G8272-1 (config)# vlag enable
G8272-2 (config)# vlag enable
```

14. Verify that the VLAG peers are configured:

```
G8272-1 # show vlag info
```

    The output should resemble Figure 13.

Figure 13   Output from the show vlag info command

```
Global State    : enabled
VRRP active     : disabled
vLAG system MAC : 08:17:f4:c3:dd:64
ISL Information:
PAG     Ifindex     State       Previous State
-------+-----------+-----------+---------------------------------
100     100100      Active      Inactive

Mis-Match Information:
               Local                      Peer
-------------+---------------------------+-----------------------
Match Result : Match                      Match
Tier ID      : 100                        100
System Type  : G8272                      G8272
OS Version   : 10.2.x.x                   10.2.x.x

Role Information:
               Local                      Peer
-------------+---------------------------+-----------------------
Admin Role   : Secondary                  Primary
Oper Role    : Primary                    Secondary
Priority     : 100                        0
System MAC   : a8:97:dc:de:4d:01          a8:97:dc:de:5a:01

Consistency Checking Information:
    State             : enabled
    Strict Mode       : disabled
    Final Result      : pass

  FDB refresh Information:
  FDB is doing refresh with below setting:
    FDB refresh is configured
    Bridge FDB aging timer is 1800 second(s)

  FDB synchronization Information:
  FDB is being synchronized.

 Auto Recovery Interval 300s (Finished)

 Startup Delay Interval 120s (Finished)

 Health Check Information:
  Health check Peer IP Address: 10.0.0.2
  Health check Local IP Address: 10.0.0.1
  Health check retry interval: 30 seconds
  Health check number of keepalive attempts: 3
  Health check keepalive interval: 5 seconds
  Health check status: UP

  Peer Gateway State    : enabled


vLAG status: enabled
vLAG Tier ID: 1
vLAG system MAC: 08:17:f4:c3:dd:09
Local Priority: 0
ISL Information: Trunk 0, LACP Key 200
Health check Peer IP Address: 10.0.0.2
Health check connection retry interval: 30 seconds
Health check number of keepalive attempts: 3
Health check keepalive interval: 5 seconds
vLAG Auto Recovery Interval: 300  seconds
vLAG Startup Delay Interval: 120  seconds
```

We strongly recommend that you configure the Lenovo switch VLAG to check the health status of its VLAG peer (step 12, above). Although the operational status of the VLAG peer is generally determined via the ISL connection, configuring a network health check provides an alternate means to check peer status in case the ISL links fail. Use an independent link (normally over the management network) between the VLAG switches to configure health check.

Because the HX host NIC connections are un-bonded and use the vSwitch setting for traffic load balancing, the HX nodes are not fully participating in VLAG as VLAG clients. As we will see in the next section, VLAG is of great use for connectivity of our HX cluster to the network core by our VLAG peer switches.

At this time, the HX node NIC ports can be connected to the configured ports on the switches and the HX nodes will have connectivity to each other – this can be verified over the Nutanix PRISM interface.

Note: If the HX nodes are to use a VLAN other than the default, it would need to be configured at this point.

Connect the VLAG to your existing core network

Now that the switches are set up as VLAG peers, and our HX Series cluster is up and running over the server-side ports, we can turn our attention to the connection of our cluster switch to the uplink core network. There are two scenarios regarding connectivity to the core network:

- Scenario 1: A pair of switches acting as a single logical switch (as with our VLAG peers)
- Scenario 2: A pair of switches that are not virtualized (two standalone switches which are acting independently)

In both cases, the connection needs to be approached with care, as this represents an activity that can affect the production network. Please work with the responsible core network administrator to ensure that they are aware of, and involved with, this connection of the HX cluster. It could, for example, cause a spanning-tree recalculation and thus affect production traffic. Also, the core network administrator needs to be aware of any VLANs configured on the HX system and match the port aggregation components (ports, port speeds, copper/fiber, etc). Activation of the connection to the core network would typically be done during a scheduled maintenance window.

In general, we recommend using fiber transceiver technology between Lenovo switches and the uplink/core switches to ensure interoperability. Copper DAC cables can also be used; this will reduce the connection cost but can sometimes lead to compatibility issues, due to support of active/passive DACs and possible blocking of certain DACs due to quality or testing issues.

For more details on cabling options for Lenovo switches, please refer to the Lenovo Networking Products and Options Catalog:.

http://www.lenovo.com/images/products/system-x/pdfs/datasheets/lenovo_networking_catalog_ds.pdf

Scenario 1: The core uplink switches function as one logical switch

This is a common scenario, because many switches today implement a proprietary version of the MC-LAG feature. For Lenovo switches it's called VLAG, for Cisco Nexus: vPC, Cisco Catalyst: VSS, Arista and Mellanox: MLAG, Juniper: MC-LAG. These all function the same way as VLAG – a pair of vendor switches of the same type are connected using an ISL and the MAC address tables of both systems are synchronized to enable the formation of a single LACP aggregation over ports on both switch peers. Stacking functionality which is offered by several vendors will also present two or more upstream devices as a single logical switch and can also be used.

In this case we can implement MC-LAG on both sides of our interconnect: our VLAG facing the MC-LAG of the other vendor - see Figure 14 on page 19. In this section, we use Cisco Nexus vPC as the example.

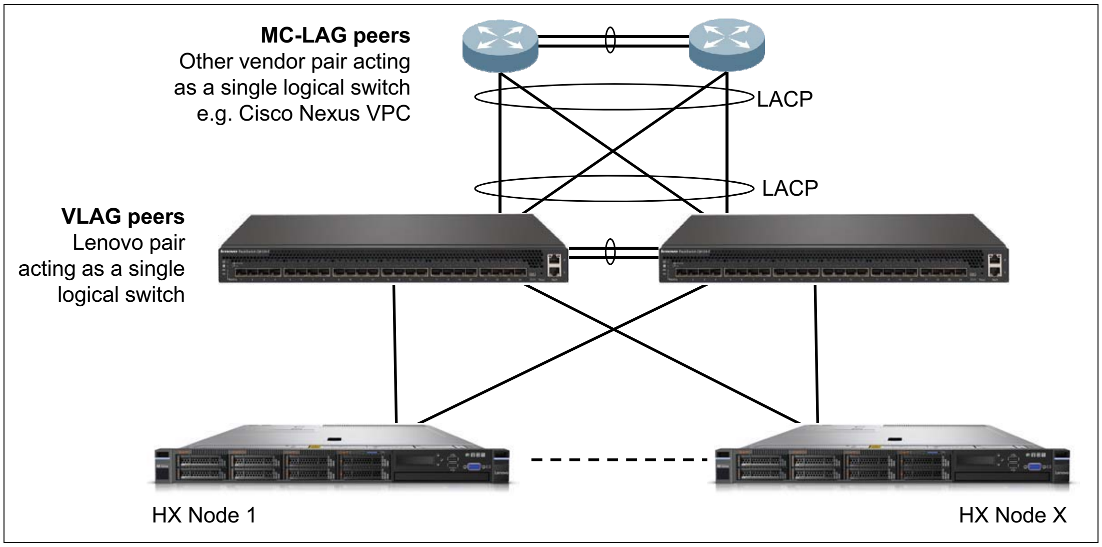


Figure 14 Scenario 1 design

On the Nexus side we will create an aggregation over the vPC peers and we will connect that directly to an aggregation formed over our VLAG peers as shown in Figure 15.

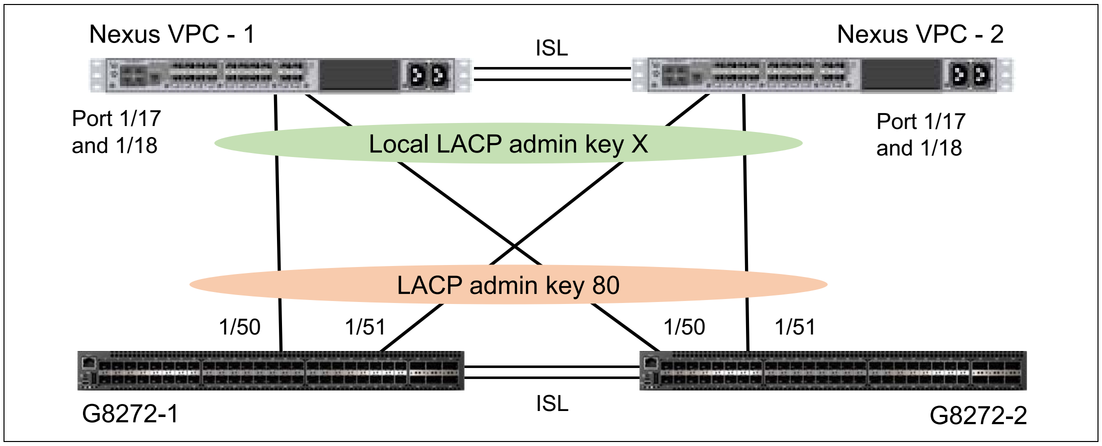


Figure 15 Interoperability between uplink MC-ALG instance, in this case vPC, and VLAG

The steps to configure the switches are as follows:

1. Issue the following commands on the Lenovo switches are as follows:

```
G8272-1#( (config)# int Ethernet 1/50-51
G8272-1#( (config-if)# channel-group 80 mode active
G8272-1#( (config-if)#
G8272-1#( (config)#exit
```

   Status of the aggregation can be shown with this command:

```
G8272-1# show port-channel summary
```

   The output of the `show` command will be similar to Figure 16.

```
Flags:
D - Down        P - Up in port-channel (members)
S - Switched    R - Routed
I - Individual  s - Suspended
U - Up (port-channel)
------+----------------+--------+---------------------------------------------
Group  port-channel Protocol Member Ports
------+----------------+--------+---------------------------------------------
80     po80       (SU)  LACP     Ethernet1/50(P) Ethernet1/51(P).
.
```

Figure 16 Output from show port-channel summary for group 80

2. Configure the same on the corresponding ports on the other VLAG peer, also using ports 50 and 51. Status should be verified with the same `show` command as described in step 1.
3. Define this LACP as a VLAG aggregation extending over both Lenovo switches by entering the following commands on both switches:

   ```
   G8272-1(config)# vlag instance 1 port-channel 80
   G8272-1(config)# vlag instance 1 enable
   ```

   As can be seen using the following command that our VLAG for LACP 80 is up and running, and ready to be connected to the vPC LACP on the Nexus switch:

   ```
   G8272-2# show vlag instance 1 info
   ```

```
 VLAG instance 1 : enabled
  Instance Information
    PAG        ifindex     State          Previous State    Cons Res
    ----------+-----------+--------------+-----------------+--------
    80          100080     Formed          Local UP          pass
```

Figure 17 show vlag instance command output

4. On the Cisco Nexus side, as with VLAG, an identical configuration is required on both vPC peers. The commands enable LACP and vPC.

   ```
   switch# configure terminal
   switch(config)# feature lacp
   switch(config)# show feature
   switch(config)# feature vpc
   switch(config)# show feature
   switch(config)# vpc domain domain-id
   switch(config)# interface port-channel channel-id
   switch(config-if)# vpc peer-link
   switch(config)# interface port-channel channel-id
   switch(config-if)# vpc domain-id
   ```

5. Verify the vPC with the following command

   ```
   switch# show vpc brief
   ```

For more information, see the chapter “Configuring Virtual Port Channels” in the Cisco NX-OS Layer 2 Switching Configuration Guide:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/421_n1_1/b_Cisco_n5k_layer2_config_gd_rel_421_n1_1/Cisco_n5k_layer2_config_gd_rel_421_n1_1_chapter8.html

Scenario 2: The core uplink switches are independent

This scenario requires connecting our VLAG peer LACP aggregation to two separate switches on the far end. These switches are most likely connected somehow in the core network (not shown in Figure 18 on page 21), but are neither directly connected using an ISL nor using a synchronizing MAC table to behave as a single logical switch. In order to prevent loops, the use of spanning-tree protocol on either the core/uplink switches or on both sets of switches is recommended, but not required.

The design is shown in Figure 18 on page 21.

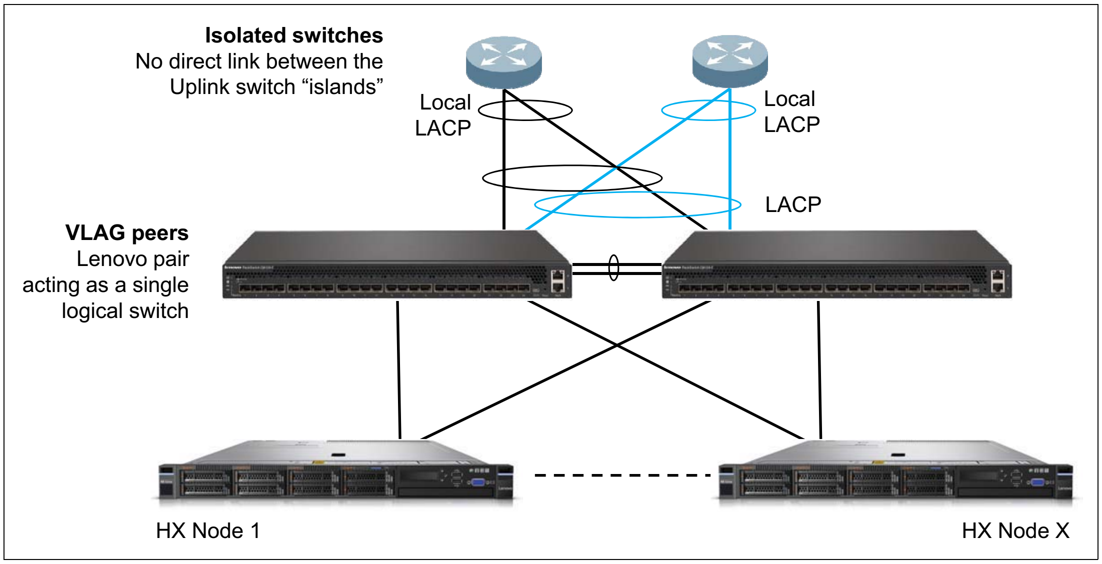


Figure 18 Scenario 2 design

The steps to configure the switches are as follows:

First, form two different VLAG aggregations on our Lenovo switch VLAG peers, in the same manner as in "Scenario 1: The core uplink switches function as one logical switch" on page 18. On each of the uplink switch "islands" we will create a simple LACP aggregation over 2 (or more) ports, which we will terminate on the aggregation split over our VLAG peers.

On the core network "island" switches, only a standard LACP aggregation is required (not active participation in VLAG/MC-LAG). These LACP are terminated over our local VLAG peers.

On the Lenovo VLAG peers, the participating ports in the aggregation need to be added on both switches. For example, if our ports 18 on both switches are joined together in a 2-port, cross-VLAG aggregation using the LACP admin key 80, then the following configuration is required on *both* switches as shown in Figure 19 on page 22.

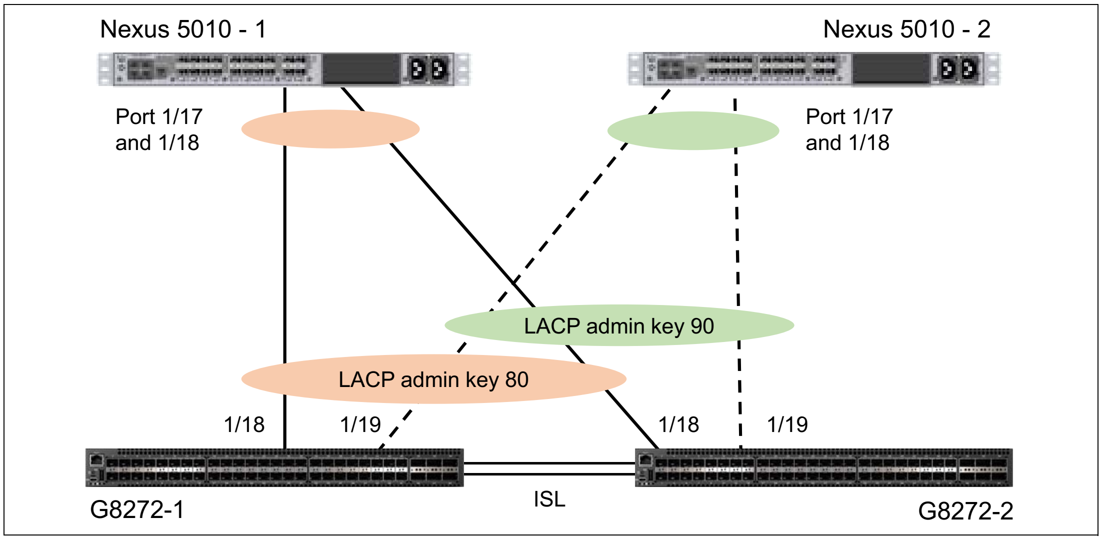


Figure 19   Connection of VLAG peers to independent uplink switches

The steps to configure the switches are as follows:

1. Issue the following commands on the Lenovo switches are as follows:

   ```
   G8272-1(config)# int Ethernet 1/18
   G8272-1(config)# channel-group 80 mode active
   G8272-1 (config)# vlag instance 1 port-channel 80 enable

   G8272-2#(config)# int Ethernet 1/18
   G8272-2#(config)# channel-group 80 mode active
   G8272-2#( (config-if)# vlag instance 1 port-channel 80 enable
   ```

   This aggregation can be connected to a two-port local LACP aggregation on one of the core/uplink switches

2. On the core/uplink switch side, only a simple aggregation is required – in this example with 2 ports on each uplink switch on Cisco Nexus. The commands enable LACP on the Cisco switches:

   ```
   switch# configure terminal
   switch(config)# feature lacp
   switch(config)# show feature
   switch (config)# interface ethernet 1/17-1/18
   switch(config-if)# channel-group 5 mode active
   ```

   For more information, see the “Configuring Port Channels” chapter of the Cisco NX-OS Software Configuration Guide:

   http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/EtherChannel.html

3. For the aggregation to the other core/uplink switch, another port pair must be configured, as above, in this case with port 19 on each VLAG peer:

   ```
   G8272-1(config)#int Ethernet 1/19
   G8272-1(config)#channel-group 90 mode active
   G8272-1(config)#vlag instance 2 port-channel 90 enable

   G8272-2(config)#int Ethernet 1/19
   G8272-2(config)#channel-group 90 mode active
   G8272-2(config)#vlag instance 2 port-channel 90 enable
   ```

4. Check the status of the aggregation:

```
G8272-1#show port-channel summary
G8272-1#show vlag [instance <x>] info
```

Appendix A: VLANs and TCP Port reference

You may want to segregate Hypervisor/ESX internal traffic from HX cluster traffic through the use of VLANs, which in turn can be propagated to the customer uplink network in line with the customer’s own VLAN design/policy.

Figure 20 on page 24 shows the ports that must be open for supported hypervisors. The diagram also shows ports that must be opened for infrastructure services.

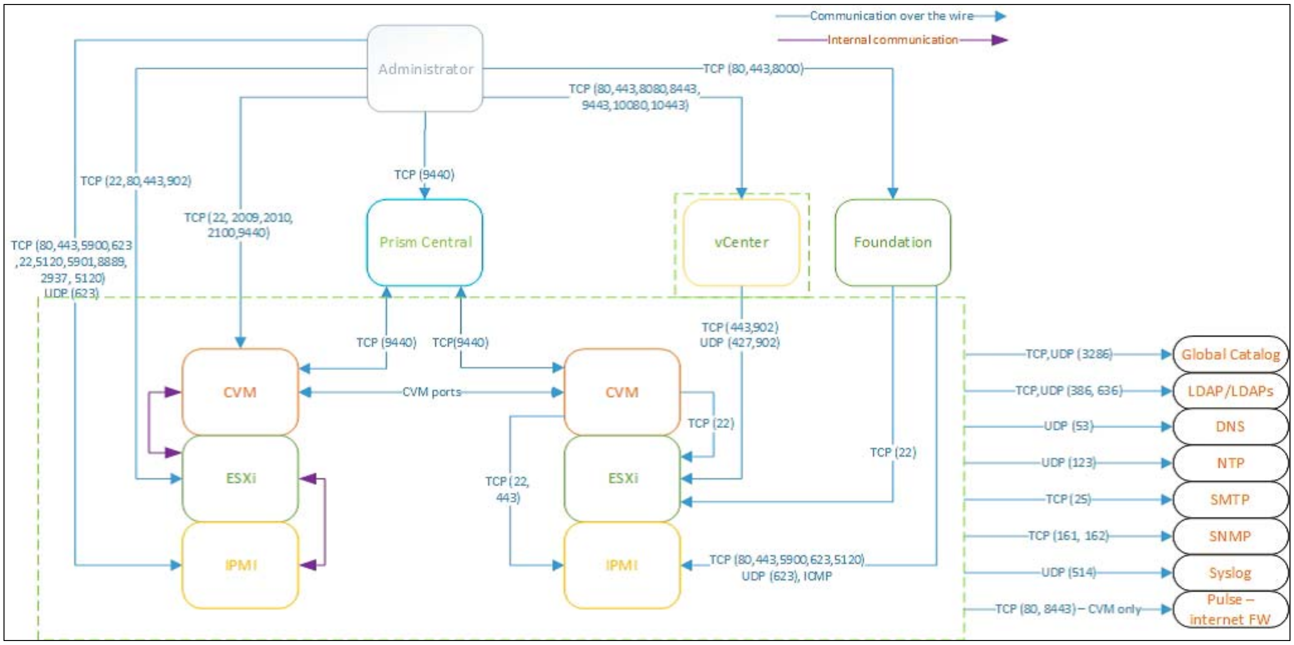


Figure 20 Nutanix Network Port Diagram for VMware ESXi

Appendix B: Acropolis Hypervisor considerations

The corresponding virtual switch setting to vSphere’s “Route based on Originating Port” in the Acropolis hypervisor’s OpenVswitch (OVS) is called Balance-slb.

For details about Balance-slb, see the heading “Balance-slb” in the following blog post:

https://next.nutanix.com/t5/Nutanix-Connect-Blog/Network-Load-Balancing-with-Acropolis-Hypervisor/ba-p/6463

Appendix C: VMware Virtual Distributed Switch considerations

For considerations regarding implementing the Virtual Distributed Switch (VDS), which is an advanced feature of the VMware Enterprise+ license, please refer to:

http://www.mikelaverick.com/2014/02/back-to-basics-migrating-to-enhanced-lacp-part-3-of-5/

Appendix D: Considerations for multiple VLANs for guest virtual machines

All three of the hypervisors supported by Nutanix have the ability to allow guest virtual machines to be segregated on to multiple VLANs. Customers may wish to do this just as they would in another hypervisor environment or in an environment which included bare metal servers.

In order to implement multiple VLANs, they must be configured on the hypervisors and/or the guest virtual machines, and must also be configured on the physical switches which connect to the Nutanix hosts.

The configuration of the ports on the physical switch would be similar to the below:

```
switch# configure terminal
switch(config)# interface ethernet 1/<x>-<y>
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan <list or range>,<list or range>
switch(config-if)# switchport trunk native vlan <z> [this is optional]
```

The ports which connect upstream to other switches in the network must allow all of the VLANs that are allowed on the ports that connect to the Nutanix hosts, with some possible exceptions (e.g. VMware vMotion networks).

The configuration options on the three hypervisors are discussed in the following subsections.

VMware ESXi

VMware ESXi allows multiple modes of managing VLANs and VLAN tagging, which can be performed by the external switches, the internal vSwitches, or the guest operating systems. The most common technique would be to use the internal vSwitches to provision the guest VMs on multiple VLAN. This is done by attaching the guests to different port-groups, each of which has an associated VLAN.

This technique is discussed in VMware Knowledge Base articles 1004074 and 1003825:

- Sample configuration of virtual switch VLAN tagging (VST Mode)

  https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004074

- Configuring a VLAN on a portgroup

  https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003825

Hyper-V

Hyper-V also allows multiple modes of managing VLANs. Hyper-V vSwitches can be associated with a specific VLAN ID, and any guests which then connect to them would have their traffic carried by that VLAN. This would apply to private (VM-to-VM only) and external (includes connectivity outside of the host) virtual networks.

For more information, see the following Nutanix best practices guide:

- Specific guidance for network setting configuration on Windows Server 2012 R2 on Nutanix with Hyper-V in different scenarios http://go.nutanix.com/Microsoft-Windows-Server-Virtual-Networking-Best-Practices-ty.html

Acropolis Hypervisor (AHV)

AHV allows provisioning of multiple VLANs for guest VMs as well as for the Controller VM (CVM) and the hypervisor; this is easily done with the PRISM management tool.

By default, the CVM and hypervisor use the untagged (native) VLAN configured on the switch ports that attach to the hosts; all hosts in a cluster must use the same VLAN for this purpose. If there is a requirement to use tagged VLANs for the CVM and hypervisor, this can be done

This is documented in detail in the Networking and Advanced Networking sections of the Nutanix Acropolis Hypervisor Best Practices Guide:

http://go.nutanix.com/rs/031-GVQ-112/images/acropolis-hypervisor-best-practices-guide.pdf

Appendix E: Connecting to the upstream network – L3 considerations

One key design choice when connecting a Nutanix cluster – or any similar cluster of servers working together to support one or more applications – is whether that connection will be at Layer 2 or Layer 3. This is a design choice for customers; both options will work and each has its merits.

Layer 2 upstream connections are discussed in the body of this document. Such a topology should have the following attributes:

- One or two vLAG instances for the upward links, depending on whether the upstream devices are aggregated using a feature like vLAG or Cisco vPC.
- Multiple physical uplinks to the upstream device(s).
- Two distinct upstream physical devices are strongly recommended.
- All VLANs used for hosts or for guest virtual machines should be carried on the uplinks, with the possible exception of those used for virtual machine mobility (e.g. vMotion), or “private” internal switches using Acropolis Hypervisor.

The benefits of the Layer 2 approach include:

- It is simpler than the Layer 3 approach
- Routing can be centralized in switches within the core network if this is desired.
- VLANs and subnets can include devices which are outside of the cluster if desired.

Layer 3 upstream connections are different in that the host and guest VLANs are not carried out of the cluster. Instead, “north-south” traffic is routed out of the cluster. The differences include:

- The upward links will not use vLAG. Instead, router ports – with distinct IP addresses – will be used on the boundary switches within the cluster and on the immediate upstream switches.
- Static or dynamic routes must be established in both directions (“north” and “south”). This means:

- Hosts and guests within the cluster need to have default gateways pointing at the boundary switches within the cluster.
- The switches within the cluster must have a default route (or specific routes) that point to the upstream network. Lenovo switches support OSPF (including OSPFv3 for IPv6) and BGP, but they do not support Cisco's proprietary EIGRP protocol.
- There must be a route configured or learned within the upstream network that points to the boundary switches within the cluster.

Benefits of the Layer 3 approach include:

- Routed traffic does not need to leave the cluster to be forwarded.
- VLANs and subnets are entirely contained within the cluster.

Figure 21 shows a Layer 3 topology.

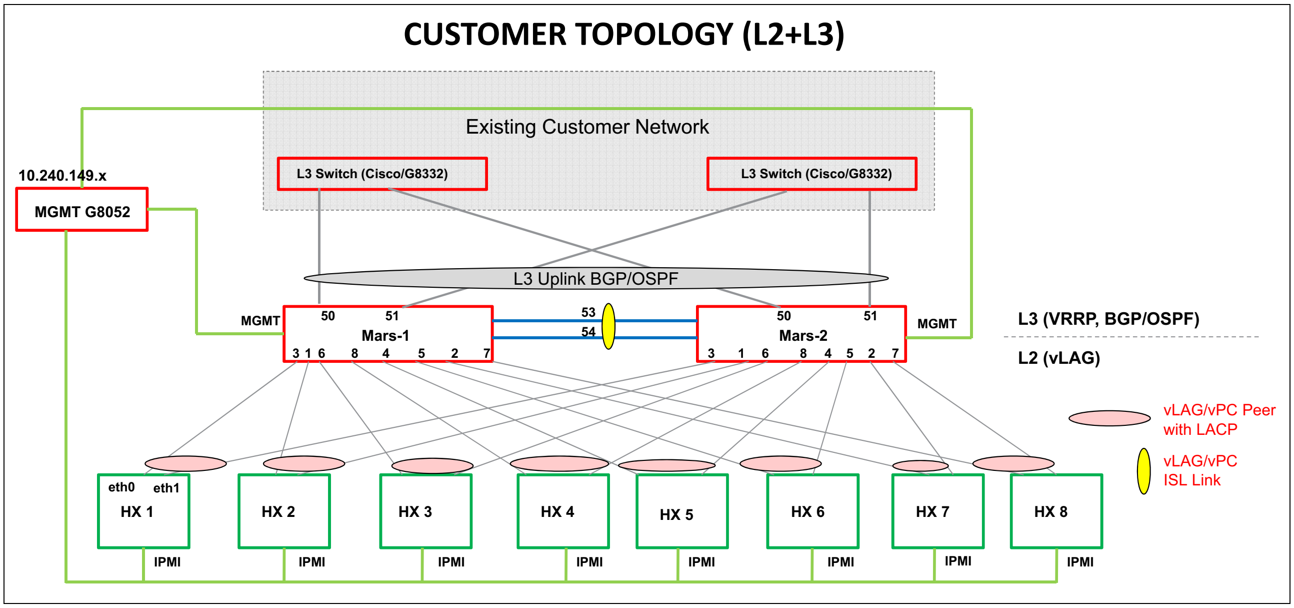


Figure 21 Layer 3 topology

Key configuration commands to enable this topology are:

- Router port configuration for uplink ports

  The uplink ports will be configured as "no switchport", which means that the port itself will carry an IP address and it will not be a member of any VLAN.

  An example is:

```
interface Ethernet1/1
 no switchport
 ip address 1.1.1.2/24
```

- Dynamic routing protocol configuration

  Each supported routing protocol has its own configuration options and requirements, which are beyond the scope of this document. The dynamic routing protocols have many options; they should be configured in a manner consistent with the customer's existing network.

  A sample BGP configuration is shown below; it is strongly recommended to use a loopback interface as the router identifier for dynamic routing protocols.

```
interface loopback1
```

```
 no switchport
 ip address 11.11.11.11/32

router bgp 10000
 router-id 11.11.11.11
 bestpath as-path multipath-relax
 address-family ipv4 unicast
  redistribute direct
 neighbor 1.1.1.1 remote-as 10000
  address-family ipv4 unicast
```

A similar sample OSPF configuration is below, and will also use the loopback1 interface.

```
router ospf 0
redistribute direct

interface e 1/1
ip router ospf 0 area 0.0.0.0
```

All router port ("no switchport") physical or port-channel interfaces as well as all VLAN interfaces would also be included in the OSPF configuration:

```
interface vlan 10
ip router ospf 0 area 0.0.0.0
```

- VRRP configuration for robustness

  VRRP is used so that the upstream network can send traffic to either of the two boundary switches within the cluster, using the same next-hop address in routing tables. This allows the environment to survive the failure of one of the two boundary switches with only a momentary (typically sub-second) loss of traffic.

  The IP addresses assigned to the VLANs in the example shown in Figure 22 on page 28 ending in .2, have counterparts in the other switch which are the same except that they end in .1. The two switches share the VRRP virtual addresses shown which end in .100. The up-stream network will have the .100 addresses in routing tables in the switches there.

  Each VLAN used by hosts/guests will need an interface like the ones below to allow routing be-tween the VLAN and the router ports that connect to the upstream network.

```
interface Vlan10
 no switchport
 ip address 50.50.50.2/24
 no ip redirects
 vrrp 10
  address 50.50.50.100
  no shutdown
!
interface Vlan11
 no switchport
 ip address 52.52.52.2/24
 no ip redirects
 vrrp 11
  address 52.52.52.100
  no shutdown
```

Figure 22 VRRP configuration

References and further reading

- Lenovo Networking and Options Catalog:

  http://www.lenovo.com/images/products/system-x/pdfs/datasheets/lenovo_networking_catalog_ds.pdf?menu-id=networking_options
- Nutanix TechNote – VMware vSphere Networking with Nutanix:

  http://go.nutanix.com/rs/nutanix/images/Nutanix_TechNote-VMware_vSphere_Networking_with_Nutanix.pdf
- Nutanix TechNote – Network Load Balancing with Acropolis Hypervisor:

  https://next.nutanix.com/t5/Nutanix-Connect-Blog/Network-Load-Balancing-with-Acropolis-Hypervisor/ba-p/6463
- Nutanix Field Installation Guide (imaging to VMware or Hyper-V from AHV)

  https://portal.nutanix.com/#/page/docs/details?targetId=Field_Installation_Guide-v3_1:Field_Installation_Guide-v3_1
- Lenovo Press – Lenovo Networking Best Practices

  https://lenovopress.com/sg248245
- Switch Application Guide and Switch Command Reference are two essential documents for Lenovo switches and can be found here, for each of the major firmware versions:

  http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp
- More general information on Lenovo Networking Switches:

  http://shop.lenovo.com/us/en/systems/networking/ethernet-rackswitch/

Change history

- 22 October 2019:
  - New section, “Enable Discovery of newly deployed Nutanix nodes” on page 12
- 22 May 2018:
  - Added references to ThinkSystem NE2572 switch for 25 GbE connectivity
  - Sample configuration commands are updated to reflect the changes introduced in CNOS 7.1
- 24 January 2018:
  - Corrected commands in “Configure the host side of the switch configuration” on page 13

Authors

This paper was written by the following subject matter experts:

William Scull is a 30-year veteran of the IT industry and has been supporting x86 server connectivity since before IBM acquisition of BNT in 2010. He is currently the product manager for Lenovo networking in EMEA, based in Munich, Germany.

Scott Lorditch is a Consulting System Engineer for Lenovo. He performs network architecture assessments and develops designs and proposals for solutions that involve Lenovo Networking products. He also developed several training and lab sessions for technical and sales personnel. Scott joined IBM as part of the acquisition of Blade Network Technologies and joined Lenovo as part of the System x acquisition from IBM. Scott spent almost 20 years working on networking in various industries, as a senior network architect, a product manager for managed hosting services, and manager of electronic securities transfer projects. Scott holds a BS degree in Operations Research with a specialization in computer science from Cornell University.

Thanks to the following people for their contributions to this project:

- Mark T. Chapman, Lenovo
- Silvio Erdenberger, Lenovo
- Marijn Joosten, Nutanix
- Aksh Mittal, Lenovo
- David Watts, Lenovo Press

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document was created or updated on October 22, 2019.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp0595

Trademarks