Configuring Advanced Hyper-V Network Features

Eli Chang

MSSA Cohort #2

Lab Summary 9

2/25/2020

Configuring Advanced Hyper-V Network Features

The scenario is that the company has already installed the Hyper-V virtualization platform. The administrators should review the Hyper-V networking configuration and create new virtual adapters with Hyper-V virtual switches, which have them in external, internal, and private switches. Once they are set up, the NIC teaming is also the option to configure for the lab. The admins also want to configure the DHCP guard to protect the network clients from unauthorized DHCP servers. Then, they configure VLANs and bandwidth management in the virtual switch manager.

Types of Hyper-V Virtual Switches

There are three types of Hyper-V virtual switches: external, internal, and private. The external type is to map a network to a specific network adapter. It means that this type will let the virtual machines to communicate over the Internet. Another option is the internal type. This only allows the virtual machines to communicate among themselves and between virtual machines and the Hyper-V host. The last type is private, which allows only to communicate among the virtual machines on the single Hyper-V host. The virtual machines cannot communicate with the Hyper-V host.

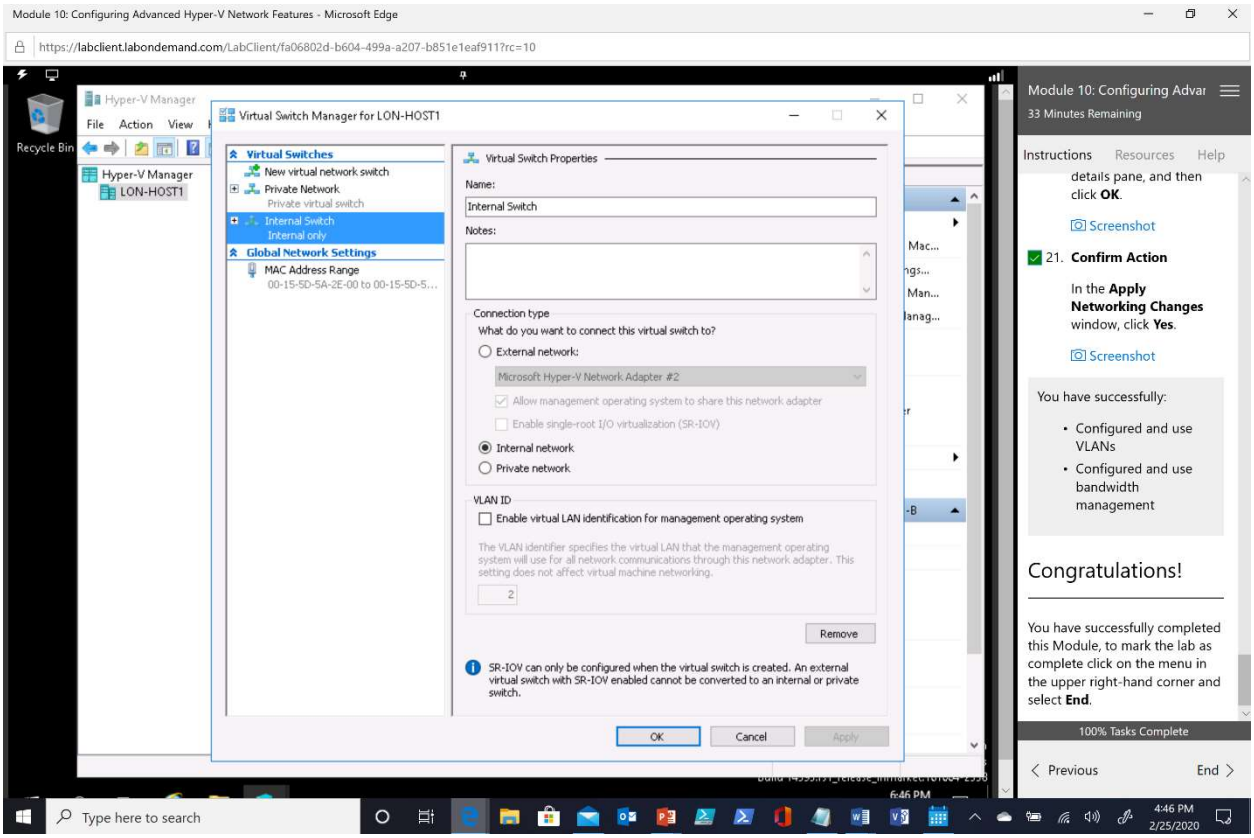
Adding NIC Teaming

The NIC teaming provides redundancy working as a single network interface. Since multiple network adapters combined as one network interface, the bandwidth will increase, compared to the individual network adapter. The administrators decided to deploy the NIC teaming for the Hyper-V virtual machines because they want to make the connectivity fault tolerance and better performance of the Hyper-V host. If one of the network adapters failed, the other network adapters would retain the network. Also, it allows for the separation of network

traffic when they are using virtual local area networks. Also, the load balancing is set as the address hash, which assigns the data flow statically.

Using DHCP Guarding

The DHCP guarding is a useful technology because some VMs might behave as DHCP unauthorized. The option can be enabled on the network adapters for each VM or through the Windows PowerShell with the prompt command, Set-VMNetworkAdapter -VMname XX -DhcpGuard On/Off. The virtual machines should get the IP addresses from the DHCP server in Hyper-V host. If enabled, the packet from a VM, attempting to send it to a DHCP server, will be automatically dropped. Since the admins manage Hyper-V host but do not manage virtual machines directly, the DHCP guarding is an appropriate feature to use in this scenario.


Module 10: Configuring Advanced Hyper-V Network Features - Microsoft Edge
https://labclient.labondemand.com/LabClient/fa06802d-b604-499a-a207-b851e1eaf911?rc=10
Recycle Bin
Hyper-V Manager
File Action View
Hyper-V Manager
LON-HOST1
Virtual Switch Manager for LON-HOST1
Virtual Switches
New virtual network switch
Private Network
Private virtual switch
Internal Switch
Internal only
Global Network Settings
MAC Address Range
00-15-5D-5A-2E-00 to 00-15-5D-5...
Virtual Switch Properties
Name:
Internal Switch
Notes:
Connection type
What do you want to connect this virtual switch to?
External network:
Microsoft Hyper-V Network Adapter #2
Allow management operating system to share this network adapter
Enable single-root I/O virtualization (SR-IOV)
Internal network
Private network
VLAN ID
Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.
OK
Cancel
Apply
Module 10: Configuring Advar
33 Minutes Remaining
Instructions
Resources
Help
details pane, and then click OK.
Screenshot
21. Confirm Action
In the Apply Networking Changes window, click Yes.
Screenshot
You have successfully:
Configured and use VLANs
Configured and use bandwidth management
Congratulations!
You have successfully completed this Module, to mark the lab as complete click on the menu in the upper right-hand corner and select End.
100% Tasks Complete
Previous
End
Type here to search
4:46 PM
2/25/2020