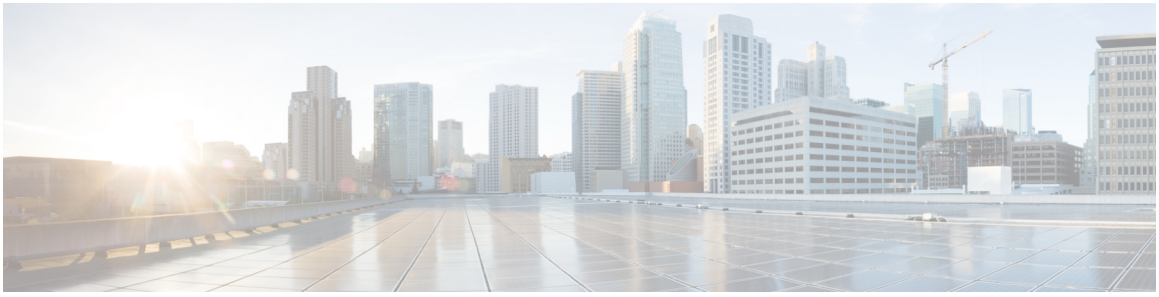


Deploying Cisco Catalyst 8000V Edge Software on Microsoft Azure

First Published: 2020-09-25

Last Modified: 2024-12-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Preface** 1

- Audience and Scope 1
- Feature Compatibility 1
- Document Conventions 2
- Communications, Services, and Additional Information 3
- Documentation Feedback 4
- Troubleshooting 4

CHAPTER 2 **Overview of Cisco Catalyst 8000V Edge Software on Microsoft Azure** 5

- Prerequisites for Deploying Cisco Catalyst 8000V on Microsoft Azure 5
- Microsoft Azure Resources 6
- Supported Instance Types 7
- Cisco Catalyst 8000V with 2 Network Interfaces - Example 7
- Information about Availability Sets 8
- Frequently Asked Questions About Deploying Cisco Catalyst 8000V 9
- Licensing 10

CHAPTER 3 **Deploy Cisco Catalyst 8000V in Microsoft Azure** 11

- Limitations 11
- Customize the Microsoft Azure Portal 11
- Deploy a Cisco Catalyst 8000V with a Single Interface 12
- Deploy Cisco Catalyst 8000V with Multiple Interfaces 14
- Access the Cisco Catalyst 8000V CLI 16

CHAPTER 4 **Configure Cisco Catalyst 8000V on Microsoft Azure** 19

Update Route Tables 19

Update Security Group 20

Configuring IPsec VPN 20

Best Practices and Caveats 21

SSH Connectivity Issues 21

CHAPTER 5 **Usage Guidelines for User-Defined Routes** 23

User Defined Routes in the Same Virtual Network 23

Routing between Virtual Networks or On-Premises Networks 23

User Defined Routes for High Availability 24

CHAPTER 6 **Configure Accelerated Networking** 25

Enable Accelerated Networking 26

Disable Accelerated Networking 28

Verifying Accelerated Networking 28

CHAPTER 7 **Deploy Azure Transit VNET DMVPN Solution** 33

Prerequisites for Deploying the Transit VNet Solution 33

Restrictions for Deploying the Transit VNet Solution 33

How to Deploy Azure Transit VNET DMVPN 33

Create a Transit VNet Hub 33

Create an Azure DMVPN Spoke VNET 35

Verifying the Configuration 36

Verifying on the Transit VNET Hubs 36

Verifying the Connectivity Between the Spokes and the Hub 38

Verifying Spoke to Spoke Connectivity 40

Troubleshooting 42

CHAPTER 8 **Configure LISP Layer 2 Extension** 43

Prerequisites for configuring LISP Layer 2 Extension 44

Restrictions for configuring LISP Layer 2 Extension 44

How to configure LISP Layer 2 Extension 44
Deploy Cisco Catalyst 8000V with Multiple Interfaces 45
Configure a tunnel between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the enterprise system 47
Configure LISP xTR on the Cisco Catalyst 8000V Instance Running on Azure 48
Verify the LISP Layer 2 Traffic Between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the Enterprise System 49

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

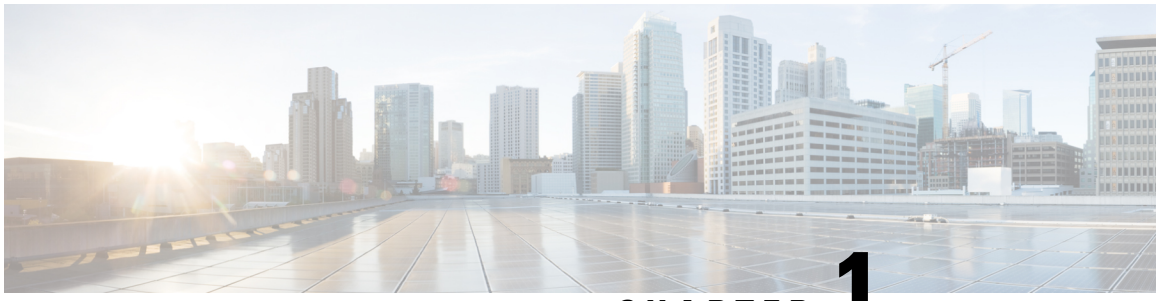
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2024 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

- Audience and Scope, on page 1
- Feature Compatibility, on page 1
- Document Conventions, on page 2
- Communications, Services, and Additional Information, on page 3
- Documentation Feedback, on page 4
- Troubleshooting, on page 4

Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the Cisco Feature Navigator tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

The command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.



Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

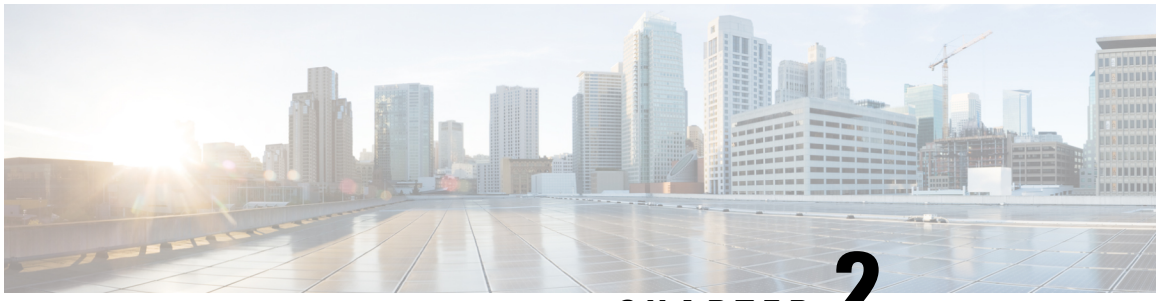
Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.



CHAPTER 2

Overview of Cisco Catalyst 8000V Edge Software on Microsoft Azure

Cisco Catalyst 8000V Edge Software is a full-featured Cisco IOS XE router, enabling IT departments to deploy enterprise-class networking services in the Microsoft Azure cloud. Most Cisco IOS XE features are also available on the virtual Cisco Catalyst 8000V.

You can choose to deploy Cisco Catalyst 8000V software on new or existing infrastructure such as a virtual network.

The following VPN features are supported on Cisco Catalyst 8000V: IPsec, DMVPN, FlexVPN, and SSLVPN. You can use dynamic routing protocols such as EIGRP, OSPF, and BGP to construct multi-tier architectures within Azure, and interconnect with corporate locations or other clouds.

You can secure, inspect, and audit hybrid cloud network traffic with application-aware Zone Based Firewall. You can also use IP SLA and Application Visibility and Control (AVC) to find out about performance issues, fingerprint application flows, and export detailed flow data for real-time analysis and network forensics.

- Prerequisites for Deploying Cisco Catalyst 8000V on Microsoft Azure, on page 5
- Microsoft Azure Resources, on page 6
- Supported Instance Types, on page 7
- Cisco Catalyst 8000V with 2 Network Interfaces - Example, on page 7
- Information about Availability Sets, on page 8
- Frequently Asked Questions About Deploying Cisco Catalyst 8000V, on page 9
- Licensing, on page 10

Prerequisites for Deploying Cisco Catalyst 8000V on Microsoft Azure

These are the main three prerequisites for deploying a Cisco Catalyst 8000V:

- You must have a user account/subscription with Microsoft Azure. For more information about creating an account with Microsoft Azure, see Get started with Azure.
- You must deploy a number of resources before or during the deployment of the Cisco Catalyst 8000V. For a description of the required resources, see Microsoft Azure Resources.

- You must either obtain a BYOL software license or opt for the Pay-As-You-Go licensing model for the Cisco Catalyst 8000V instance. For more information, see the *Licensing* section in this guide.

Microsoft Azure Resources

To deploy a Cisco Catalyst 8000V on Microsoft Azure, the following resources are required. You must create the required resources when you deploy Cisco Catalyst 8000V if they do not already exist in the Azure network.

- Resource group - container for resources. Resources include virtual machines, interfaces, virtual networks, routing tables, public IP addresses, security groups and storage accounts. These resources are described in detail below.



Note You must deploy a Cisco Catalyst 8000V with a Single Interface within an existing resource group. The resource group can already contain other resources.

If you create an object in a resource group that depends upon an object in a second resource group, the second resource group cannot be deleted until you delete your object in the first resource group. Create a new resource group for a new deployment. For more information about resource groups, see: Azure Resource Manager overview.

- Virtual network - a Cisco Catalyst 8000V with a 2-, 4-, or 8- Network Interface Cards (NICs), requires a virtual network with a set of defined subnets. Cisco Catalyst 8000V with a single interface requires a new or an existing virtual network with 1 subnet. For more information about virtual networks, see Azure Virtual Network.
- Route table - contains user defined routes (UDRs) for subnetworks.
- Security group - contains security rules for the virtual network.
- Public IP address - IP address of the Cisco Catalyst 8000V instance.
- Storage account - required for the Cisco Catalyst 8000V image, VM disk files and boot diagnostics. The storage account type `Standard_LRS` is the only currently supported type. For more details about creating a storage account, see: About Azure storage accounts.
- Boot Diagnostics - useful for debugging issues found during the operation of the Cisco Catalyst 8000V.
- Availability Set - contains a group of VMs. The VMs are logically separate and can run across multiple servers, racks and switches in a data center. For more information on availability sets, see Information about Availability Sets, in this document. Also search for Availability Set in the Microsoft Azure Documentation.
- Managed Disks - manage the storage accounts of VM disks. When you create a managed disk, specify the disk type (Premium or Standard) and the size of disk that you require. Azure Storage Service Encryption (SSE) is used by default for all managed disks. For more information on managed disks, see Azure Managed Disks Overview.
- Interfaces - For a Cisco Catalyst 8000V VM with 2, 4, or 8 network interfaces, you can assign a public IP address to any interface. Commonly, the public IP address is assigned to the first interface. All Cisco Catalyst 8000V VM interfaces are in a private subnet. You can assign the IP address of each private interface using the **ip address dhcp** command in the interface configuration or assign a static IP address

using the **ip address** command. For example, `ip address 1.1.1.1 255.255.255.0`. If you use a static IP address, ensure that the IP address is the same as the IP address assigned by Microsoft Azure. View the IP address of an interface by looking at the VM network settings in the Azure marketplace.

Cisco Catalyst 8000V Deployments in the Microsoft Azure Marketplace

Cisco has published a set of deployments in the Microsoft Azure marketplace to help create and manage resources. The following templates are currently supported:

- Cisco Catalyst 8000V solution template - Using this template, you can deploy a Cisco Catalyst 8000V with 2-, 4-, or 8- NICs, with other required resources.
- Cisco Catalyst 8000V Virtual Machine template - Using this template, you can deploy a Cisco Catalyst 8000V with a single interface, with pre-existing resources.

If you are deploying a Cisco Catalyst 8000V instance in a new network with no existing resources, Cisco recommends that you use a full solution template. For more information, see the *Cisco Catalyst 8000V Public Cloud Deployments* section.

For a government cloud deployment, see the *Cisco Catalyst 8000V Government Cloud Deployments* section.

When you deploy a Cisco Catalyst 8000V instance with 2-, 4-, or 8- NICs solution template, many resources are automatically created. Ensure that you select a solution template based on the number of interfaces or subnets that you want in the virtual network. To know how to deploy the instance, see the *Deploy a Cisco Catalyst 8000V with Multiple Interfaces* in this guide.

To deploy a Cisco Catalyst 8000V instance and use the resources that already exist in Microsoft Azure, deploy the instance using a single interface template. For more information, see the *Deploy a Cisco Catalyst 8000V with a Single Interface* section. After you deploy a Cisco Catalyst 8000V instance with a single interface, you can manually add further interfaces using Powershell or Azure CLI commands. From Cisco IOS XE 17.15.1a release, Cisco Catalyst 8000V supports Microsoft Azure CLI version 2.9.1.

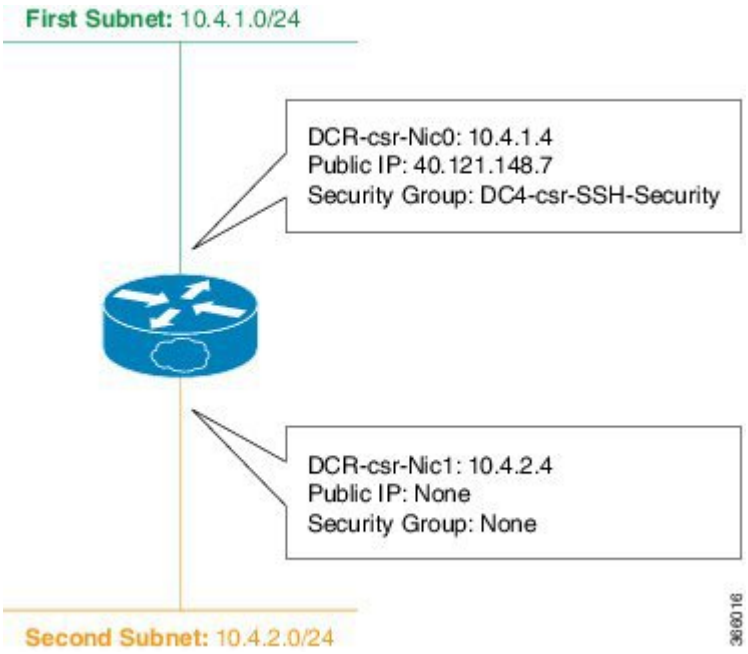
Supported Instance Types

To see the list of supported instances that support the deployment of Cisco Catalyst 8000V in Microsoft Azure, refer to the Compatibility Matrix.

Cisco Catalyst 8000V with 2 Network Interfaces - Example

This example shows the configuration that results after deploying a 2 network interface solution template from the Azure Marketplace.

A Cisco Catalyst 8000V virtual machine (2 vCPU, 7G RAM) is set up with 2 interfaces. There is a public IP address attached to the interface on the first subnet (NIC0). The first subnet (NIC0) has a security group with inbound rules for the interface. A default routing table is set up on the Microsoft Azure hypervisor router for the Cisco Catalyst 8000V. You can deploy a Cisco Catalyst 8000V instance on a new or existing virtual network.



Subnetting Limits

The Cisco Catalyst 8000V on Microsoft Azure supports a subnet mask between /8 and /29 (CIDR definition).

The subnet /29 is the smallest available in Microsoft Azure which supports 8 IP host addresses. 4 IP host addresses per subnet are reserved by Microsoft Azure. Therefore, for a /29 subnet, you have 4 IP host addresses available.

Information about Availability Sets

If you are deploying a Cisco Catalyst 8000V using a solution template for 2, 4 or 8 network interfaces from the Azure Marketplace, and you choose to use the availability set feature, you must use a new availability set.

Availability sets are only available in solution templates for the public cloud and not for solution templates in the government cloud.

For more information, see Azure Managed Disks Overview.

Availability Sets for a Cisco Catalyst 8000V with 2, 4 or 8 Network Interfaces

The logical grouping of VM resources in an availability set helps to keep groups of VMs isolated from one another. The VMs in an availability set can run across multiple physical servers, compute racks, storage units, and network switches. If you use availability sets and a hardware or Microsoft Azure software failure occurs, only a subset of your VMs are affected. You must use a new availability set if you are deploying a Cisco Catalyst 8000V using a solution template for 2, 4 or 8 network interfaces . An availability set is only available for Cisco Catalyst 8000V public cloud deployments. Availability sets are not available for Cisco Catalyst 8000V government cloud deployments.

When you choose to use an availability set and you are deploying a Cisco Catalyst 8000V with 2, 4 or 8 network interfaces using a solution template, you are asked to enter the following parameters:

- **Availability Set Name** - name of the new availability set. You cannot use the name of an existing availability set.
- **Platform Fault Domain Count** - count of the fault domains. VMs that are in the same fault domain share common storage as well as a common power source and network switch. Value: 1 or 2 (the default value is 2).
- **Platform Update Domain Count** - count of the update domains which are a group of VMs and underlying physical hardware that can be rebooted simultaneously. Value: 1 to 20 (the default value is 20).

Availability Sets for a Cisco Catalyst 8000V with a Single Interface

To use an existing availability set, you must deploy a Cisco Catalyst 8000V with a Single Interface.

Frequently Asked Questions About Deploying Cisco Catalyst 8000V

1. When I search for C8000V in Azure Marketplace, I am presented with a list of Cisco Catalyst 8000V solution templates/deployments. Which one should I pick?

The best practices for deciding whether to pick a solution template (for 2-, 4- or 8- NICs) or to pick an individual Cisco Catalyst 8000V are as follows:

If you are creating a new virtual network, use one of the solution templates (for 2-, 4- or 8- NICs). This saves you the time and effort of manually creating all the resources.

If any of the following conditions are true, use an individual Cisco Catalyst 8000V.

- You have an existing resource group which does not contain a Cisco Catalyst 8000V and you want to deploy Cisco Catalyst 8000V in the resource group.
- You have an existing resource group which already contains a Cisco Catalyst 8000V and you want to deploy another one in the same availability set.

2. I want to create multiple Cisco Catalyst 8000V instances in my subscription and I want them all to be deployed in a single availability set. How can I do this?

Perform the following steps:

1. Deploy the first Cisco Catalyst 8000V using a 2, 4, 8 NIC solution template. Create a new availability set for this Cisco Catalyst 8000V instance.
2. Deploy an individual Cisco Catalyst 8000V. Select the same availability set that you created in step 1. Using this Bring Your Own License individual Cisco Catalyst 8000V allows you to reuse existing resources in existing non-empty resource groups.
3. Repeat step 2 for all of the remaining Cisco Catalyst 8000V instances.

Licensing

The Cisco Catalyst 8000V supports the following license models:

Bring Your Own License Model

The Bring Your Own License (BYOL) licensing model for Cisco Catalyst 8000V on Microsoft Azure is supported through Cisco Smart Licensing Usage Policy. This licensing model allows you to assign licenses to Cisco Catalyst 8000V instances dynamically. You can manage licenses across different Cisco Catalyst 8000V instances without having to lock each license to a specific Cisco Catalyst 8000V UDI serial number.

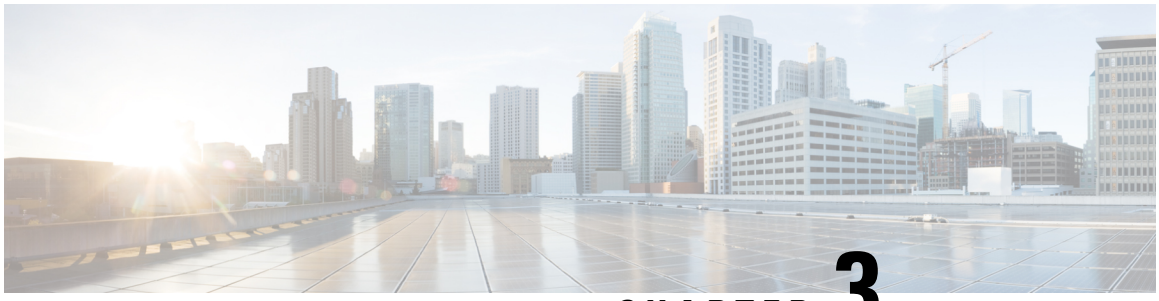
Note In addition to paying for a Cisco Catalyst 8000V license, you have to pay for a Microsoft VM instance.

Pay-As-You-Go Licensing

Pay-As-You-Go or PAYG is a licensing model that is supported by Cisco Catalyst 8000V running on Microsoft Azure. In this licensing model, you can launch hourly Cisco Catalyst 8000V instances from the Azure Marketplace and consume the instances for a defined period of time based on your requirements. This allows you to pay only for the time you've used the instance instead of paying for an annual or multi-year billing. A Cisco Catalyst 8000V PAYG instance supports all the existing deployment models that are available in the BYOL licensing model.

Note PAYG is not supported in SD Routing devices.

To enable the throughput license performance, you must enable the Accelerated Networking functionality.



CHAPTER 3

Deploy Cisco Catalyst 8000V in Microsoft Azure

This chapter provides information on deploying Cisco Catalyst 8000V in Microsoft Azure.

- Limitations, on page 11
- Customize the Microsoft Azure Portal, on page 11
- Deploy a Cisco Catalyst 8000V with a Single Interface, on page 12
- Deploy Cisco Catalyst 8000V with Multiple Interfaces, on page 14
- Access the Cisco Catalyst 8000V CLI, on page 16

Limitations

This list provides the limitations for deploying Cisco Catalyst 8000V in Microsoft Azure.

- Console access to Cisco Catalyst 8000V is not available when deployed on Microsoft Azure in NVA environment.

Customize the Microsoft Azure Portal

You can customize the Microsoft Azure portal GUI by adding frequently used objects such as virtual machines or virtual network to the left-hand side panel.

Note You only need to perform these optional steps if you are going to deploy a Cisco Catalyst 8000V instance using a single interface where you need to manually add the resources. You don't have to create these resources manually if you are deploying a Cisco Catalyst 8000V instance with 2, 4, or 8 interfaces using a solution template.

Before you begin

To customize the portal, you must have a Microsoft Azure subscription.

Procedure

Step 1 Sign in to the Microsoft Azure portal.

Step 2 Click **Browse** and select an object to be added to the left hand side panel.

Step 3 In the drop-down menu, click the star symbol for your chosen object.
The details of this object are saved for future use. Repeat steps 2 and 3 to add a series of objects to the left-hand side panel.

Deploy a Cisco Catalyst 8000V with a Single Interface

Perform the following steps to deploy a Cisco Catalyst 8000V with a single interface.

Note If you are deploying Cisco Catalyst 8000V with a 2-, 4- or 8- NICs solution template, the following steps are not required. Instead, go to the Microsoft Azure portal and determine the public IP address of the Cisco Catalyst 8000V. Then, **ssh** into the Cisco Catalyst 8000V as described in the *Access the Cisco Catalyst 8000V CLI* section.

Procedure

Step 1 Select **Virtual machines** in the left hand side panel.

Step 2 Click **Add**.

Step 3 Enter `c8000v`. A search starts, to find any Cisco Catalyst 8000V VM deployments in the Azure Marketplace.

Step 4 Choose a deployment.

Step 5 Click **Create**.

The **Basics** sub-menu is highlighted.

Step 6 **Name** - Enter the name of the virtual network.

The virtual network is a cloud-based network used by Microsoft Azure to represent the private network.

Step 7 **VM disk type** - Select a VM disk type.
The VM disk type is either SSD or HDD.

Step 8 **User name**

Username for the Cisco Catalyst 8000V virtual machine. This is the username that you will use to log into the CCisco Catalyst 8000V instance.

Step 9 **Authentication type** - Enter a Password (default) or SSH public key.

Step 10 **Subscription** - Select the name of a subscription.

A default name based on the name of the virtual machine is provided. You can change the default name.

Step 11 **Resource Group** - Create a new group by selecting **Create new** or select an existing group by selecting **Use existing**.

The **Size** sub-menu is highlighted.

Specifies the name of a new or existing resource group.

Step 12 Click **OK**.

Step 13 Click **Virtual machine size**

For further information on virtual machine size, see Sizes for Windows virtual machines in Azure.

Step 14 Click **OK**.

The **Settings** sub-menu is highlighted.

Step 15 **High Availability** - Select an existing availability set or create a new availability set.

To use High Availability, select an existing availability set or create a new availability set.

Step 16 **Storage** - Enter the storage account name.

Enter the storage account name if you are using Managed Disks to manage the storage accounts of VM disks.

Step 17 **Virtual network** - Enter the virtual network address.

Enter the address of the virtual network using Classless Inter-Domain Routing (CIDR) notation. Example: `10.4.1.0/16`

Step 18 **Subnet** - Enter the subnet IP address.

Step 19 **Public IP address** - Enter the public IP address name.

The IP address is provided by Azure.

Step 20 **Network Security groups** - Enter the name of a network security group.

Step 21 **Auto-shutdown**

To enable auto-shutdown, set Enable to **On**. To disable auto-shutdown set Enable to **Off**. For more information on auto-shutdown, search for auto-shutdown in the Microsoft Azure Documentation.

Step 22 (Optional) **Monitoring** - Select **Monitoring** to enable monitoring.

Enables Cisco Catalyst 8000V monitoring using boot diagnostics. If you enable monitoring, you must also enter the boot diagnostics account name.

Step 23 Click **OK**.

The **4 Summary** sub-menu is highlighted. The system displays the summary details of the VM that is about to be deployed.

Step 24 Click **Create**.

The VM is created and the purchase is confirmed.

Step 25 Click **Virtual machines** on the left hand panel.

Verifies the VM status. After a few minutes, the VM status changes from Creating to Running. Make a note of the Public IP address name.

What to do next

Go to the *Access the Cisco Catalyst 8000V CLI* section which explains how to **ssh** into Cisco Catalyst 8000V.

Deploy Cisco Catalyst 8000V with Multiple Interfaces

Perform the following steps to deploy Cisco Catalyst 8000V with multiple interfaces.

Procedure

Step 1 Select **Virtual machines** in the left hand side panel.

Step 2 Click **Add**.

Step 3 Enter "C8000V".

Finds the Cisco Catalyst 8000V VM deployments in the Azure Marketplace.

Step 4 Choose the deployment of your choice, with 2,4, or 8 NICs.

Step 5 Click **Create**.

Step 6 **Virtual Machine name** - Select the **Basics** sub-menu and enter a name for the virtual machine.

Name of the cloud-based network used by Microsoft Azure to represent a private network.

Step 7 **Username** - Select a user name.

The Username for the Cisco Catalyst 8000V virtual machine which you can use to log into the Cisco Catalyst 8000V instance.

Step 8 **Authentication type** - Enter a Password (default) or SSH public key.

Step 9 **Cisco IOS XE Image Version** - Select the Cisco IOS XE version.

Step 10 **Subscription** - (Optional) Change the subscription name.

A default subscription name is provided, based on the name of the virtual machine. You can change this default subscription name.

Step 11 **Resource Group** - Select either **Create new** or **Use existing**.

You can only create a Cisco Catalyst 8000V in a new Resource Group (or in a completely empty existing resource group). To remove a Resource Group, first delete the Cisco Catalyst 8000V VM and then delete the Resource Group.

Step 12 Click **OK**.

Step 13 Select the **Cisco C8000V Settings** sub-menu and then select **Number of Network Interfaces in C8000V**.

Step 14 Select the number of interfaces: 2, 4, or 8.

Step 15 **License Type** - Select either **BYOL** or **PAYG** as the license type.

Note
PAYG licensing type is not supported in SD Routing devices.

Step 16 **Managed Disk** - Select **Enabled**.

Step 17 **Storage Account** - Enter a name for the storage account.

For more information on storage accounts, see the Microsoft Azure Resources section in this guide.

Step 18 **Virtual machine size** - Select the appropriate virtual machine size.

Based on the number of interfaces that you are using, select the appropriate virtual machine size. Microsoft Azure supports different image types with different performance expectations. To view the supported instance types and the virtual machine sizes, see the following links:

- Dv2 and DSv2 series
- Fsv2 series

Step 19 **Custom Data** - Select **Yes** if you want to provide a bootstrap configuration file.

For further information about providing a bootstrap configuration file for the Cisco Catalyst 8000V instance, see *Deploying a Cisco Catalyst 8000V VM Using a Day 0 Bootstrap File* section and the *Customdata-examples* section.

Step 20 **Availability Set** - Select **Yes**.

Step 21 **Availability Set name** - Enter a name for the availability set.

Step 22 **Availability Set fault domain count** - Enter the availability set fault domain count.

Fault domains define the group of VMs that share a common power source and network switch. Availability sets arrange virtual machines across fault domains.

Step 23 **Availability Set update domain count** - Enter the availability set update domain count.

An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

Step 24 **Boot diagnostics** - Enter the boot diagnostics.

For more information on boot diagnostics, see the *Information About Deploying Cisco Catalyst 8000V in Microsoft Azure* section.

Step 25 **Diagnostics Storage account** - Enter the storage account name.

Step 26 **Public IP Address** - Enter the public IP address name.

For more information on the public IP address, see the *Microsoft Azure Resources* section.

Step 27 **DNS label** - (Optional) Change the name of the DNS label.

The DNS label is the name of the public IP address to be assigned to the Cisco Catalyst 8000V. A default value for the DNS label is shown in the text box, which is the VM name followed by "`-dns`".

Step 28 **Virtual network** - Choose one of the following: **Create New** or **Use existing**.

For a new virtual network, enter the name and the IP address.

Step 29 Click **Subnets** - Enter the subnet names and the IP addresses.

Step 30 Check that all the Cisco Catalyst 8000V Settings are acceptable, and then click **OK**.

The **3 Summary** sub-menu is highlighted.

Step 31 Click **OK**.

The **4 Buy** sub-menu is highlighted.

Step 32 Click **Create**

The VM is created and the purchase is confirmed.

Step 33 Click **Virtual machines** on the left hand panel.

After a few minutes, the status of the recently created VM changes from Creating to Running. Make a note of the Public IP address name.

Access the Cisco Catalyst 8000V CLI

Access the CLI of the Cisco Catalyst 8000V VM through a terminal server.

Before you begin

Before you access the CLI, perform the steps in one of the preceding deployment procedures Deploy a Cisco Catalyst 8000V With a Single Interface, or Deploy a Cisco Catalyst 8000V With Multiple Interfaces.

Procedure

Enter the **ssh** command using a command syntax from one of the two substeps below.

Enter the **ssh** command in a terminal server of your choice to access the CLI .

- If you did not previously use an SSH public key (you did not specify a username of "azureuser", you can access the Cisco Catalyst 8000V CLI using the following command: **ssh –o ServerAliveInterval=**60 *username@c8000v_ip_address*
- If you previously used an SSH public key (you did specify a user name of "azureuser"), you can access the Cisco Catalyst 8000V CLI using the following command: **ssh –i***key***-o ServerAliveInterval=**60 azureuser*@c8000v_ip_address*

Example

In the following example, user name="azureuser", public IP address = 40.121.148.7 and password=xxx are used as parameters in the **ssh** command, before other commands such as **show ip route**. No ssh public key was previously specified.)

```
$ ssh –o ServerAliveInterval=60  azureuser@40.121.148.7
               The authenticity of host '40.121.148.7 (40.121.148.7)' can't be established.

                RSA key fingerprint is 94:79:e9:d2:2e:85:93:d6:52:41:cc:a3:d9:14:7f:5f.
                Are you sure you want to continue connecting (yes/no)? yes
               Warning: Permanently added '40.121.148.7' (RSA) to the list of known hosts.

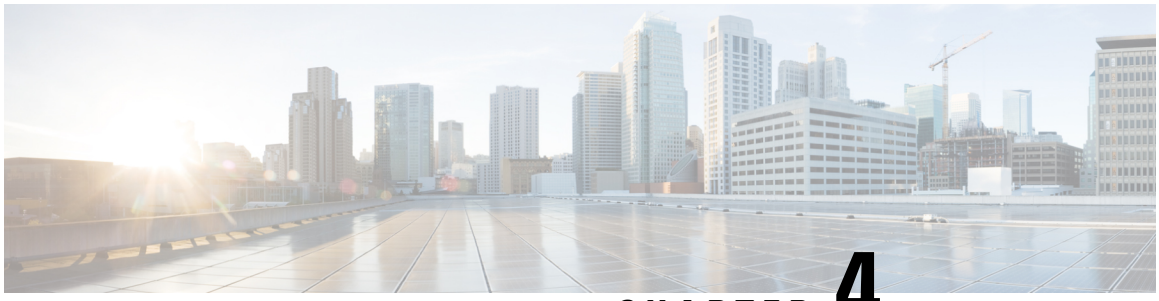
                Password: mypassword

# show ip int br
                Interface              IP-Address      OK? Method Status
  Protocol
                GigabitEthernet1       10.4.1.4        YES DHCP   up
  up
                GigabitEthernet2  unassigned     YES unset  administratively down     down
```

```
# configure terminal
                Enter configuration commands, one per line.  End with CNTL/Z.
                # interface g2
                # ip address dh
                # ip address dhcp
                # no shutdown
                # end
                # show run interface g2
                Building configuration...
                Current configuration : 69 bytes
                !
                interface GigabitEthernet2
                ip address dhcp
                negotiation auto
                end
                # show ip interface brief
                Interface              IP-Address      OK? Method Status
Protocol
                GigabitEthernet1       10.4.0.4        YES DHCP   up                    up
                GigabitEthernet2       10.4.1.4        YES DHCP   up                    up

                # show ip route
                <output snipped for brevity>
                Gateway of last resort is 10.4.1.1 to network 0.0.0.0

                S*    0.0.0.0/0 [1/0] via 10.4.1.1
                10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
                C        10.4.1.0/24 is directly connected, GigabitEthernet1
                L        10.4.1.4/32 is directly connected, GigabitEthernet1
                C        10.4.2.0/24 is directly connected, GigabitEthernet2
                L        10.4.2.4/32 is directly connected, GigabitEthernet2
                168.63.0.0/32 is subnetted, 1 subnets
                S        168.63.129.16 [254/0] via 10.4.1.1
```



CHAPTER 4

Configure Cisco Catalyst 8000V on Microsoft Azure

The following chapter tells you how to configure your Cisco Catalyst 8000V instance for Microsoft Azure.

- Update Route Tables, on page 19
- Update Security Group, on page 20
- Configuring IPsec VPN, on page 20
- Best Practices and Caveats, on page 21
- SSH Connectivity Issues, on page 21

Update Route Tables

In Microsoft Azure, all VMs send packets to a hypervisor router, and the hypervisor forwards the packets based on the routing table associated with that subnet.

When a Cisco Catalyst 8000V VM is created, a route table is created for each subnet. For a 2 vNIC Cisco Catalyst 8000V VM, a default route is created for a second (internally facing) subnet that points to the Cisco Catalyst 8000V. All the VMs created on this subnet use the Cisco Catalyst 8000V as the default gateway. For Cisco Catalyst 8000V VMs that have more than two vNICs, you need to define the default routes and apply them to the subnets.

Procedure

Step 1 Click **Route Tables**.

Expands the Settings pane.

Step 2 Navigate to the Route Tables pane and select the target route table.

Step 3 Click **All Settings**.

Step 4 In the **Settings** pane, click **Routes**.

Add or modify routes.

Update Security Group

A Security Group controls which ports/destinations the hypervisor allows/denies for certain interfaces. When creating a Cisco Catalyst 8000V, a new Security Group is created for the first subnet inbound interface by default. For Cisco Catalyst 8000V virtual machines deployed through this deployment, the following ports are added for inbound internet traffic: TCP 22, UDP 500 and UDP 4500. Use of other ports is denied.

Procedure

Step 1 Click Network security groups on the left hand side panel.

The Network security groups pane appears, and shows a list of security groups.

Step 2 Click the target network security group.

The system displays the pane that shows the details of the security group.

Step 3 Click **All Settings**.

Step 4 From the **Settings** pane, click **Inbound Security Rules**.

Step 5 From **Network Security Rules**, click **Add** to add additional rules.

Configuring IPsec VPN

The following example shows an IPsec VPN configured for a Cisco Catalyst 8000V instance running on Microsoft Azure.

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 3.3.3.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 104.45.154.184
 tunnel protection ipsec profile P1
end
!!!! To test, create loop back interface and static route!!!!!
interface Loopback1
 ip address 5.5.5.5 255.255.255.255
end
ip route 6.6.6.6 255.255.255.255 Tunnel0
```

Best Practices and Caveats

1. Cisco recommends that you keep resources in a Resource Group. To clean up all the resources in a group, you can remove the relevant Resource Group.
2. When a Cisco Catalyst 8000V VM is deleted, not all the resources for the VM are deleted (route table, security group, public IP, network interfaces). Subsequently, if you create a new Cisco Catalyst 8000V with the same name as before, the previous resources may be re-used. If you do not want to re-use these resources, choose one of the following actions:
   - Manually remove each resource.
   - Remove the Resource Group containing the individual resources.
   - Create a new Cisco Catalyst 8000V VM with a different name.
3. If you use the deployment template to create a Cisco Catalyst 8000V instance, make sure that the public IP address is configured as static on Microsoft Azure. To do this, in Microsoft Azure, navigate to the public IP address. In the configuration settings, see if the address is shown as Dynamic or Static. Select the **Static** option. Note that the default option is Dynamic.

SSH Connectivity Issues

You may fail to establish an SSH connection to a Cisco Catalyst 8000V on Microsoft Azure after you initially deploy the Cisco Catalyst 8000V, or after you reload or restart the Cisco Catalyst 8000V. In the Azure portal, the Cisco Catalyst 8000V instance is in the running state. The following three scenarios suggest workarounds for when you fail to connect using SSH.

Scenario 1. Attempted SSH access soon after booting up Cisco Catalyst 8000V

You may fail to establish an SSH connection if you tried to gain access to the Cisco Catalyst 8000V soon after boot up. After starting the deployment of the instance, it takes about 5 minutes for SSH connectivity to become available.

Scenario 2. Binding problem in the Microsoft Azure Infrastructure

Microsoft Azure support recommends that you perform the following steps:

1. On the Cisco Catalyst 8000V interface that has a public IP address, reassign the private IP address to a new static IP address within the subnet.
2. Open the PowerShell in the Azure portal.
3. Update the ARM VM.

   Refer to this Azure documentation: https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/update-azurermvm?view=azurermps-5.6.0.
4. In the powershell, enter the following commands:

   $vm = Get-AzureRmVM -Name "reload-lnx" **-ResourceGroupName** "reload-rg"

   Update-AzureRmVM -VM $vm -ResourceGroupName "reload-rg"
5. Reset the network interface to which the public IP address is attached.

For further information on resetting the network interface, see: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/reset-network-interface.

6. Select **VM** > **Networking** and select the Network Interface.
7. Go to **IP configurations** and select the IP name.
8. If the private IP address that is assigned to the interface is statically configured, write down the address for use in step **13**.
9. Under **Assignment**, click **Static**.
10. In the IP address field, use an available IP address. Choose an available IP address within the subnet to which the network interface is connected.
11. Click **Save** and wait for the save to complete.
12. Retry connecting to the router using SSH.
13. After you add (or change) a static IP address and gain access to the VM, if the IP address that you originally assigned to this interface (see step **8.**) is statically configured, you can either change the IP address from static to dynamic, or you can reconfigure the IP address to the original address (the address you noted in step **8**).

Scenario 3. Misconfiguration of idle terminal timeouts

When you start an SSH session to the Cisco Catalyst 8000V, ensure that you do not configure the terminal VTY timeout as infinite - do not configure: `exec-timeout 0 0`. Use a non-zero value for the timeout; for example, `exec-timeout 4 0`. This command specifies a timeout of four minutes and zero seconds.

The reason why the `exec-timeout 0 0` command causes an issue is as follows:

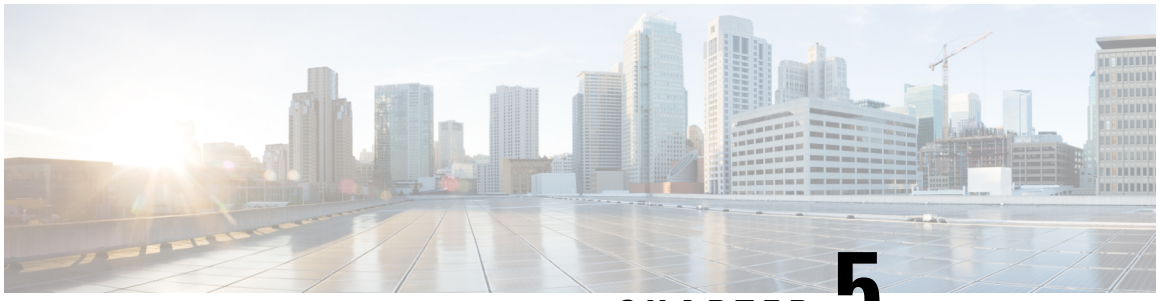
Azure enforces a timeout for the console idle period of between 4 and 30 minutes. When the idle timer expires, Azure disconnects the SSH session. However, the session is not cleared from the point of view of the Cisco Catalyst 8000V as the timeout was set to infinite by the `exec-timeout 0 0` configuration command. The disconnection causes a terminal session to be orphaned. The session in the Cisco Catalyst 8000V remains open indefinitely. If you try to establish a new SSH session, a new virtual terminal session is used. If this pattern continues to occur, the number of allowed simultaneous terminal sessions is reached and no new sessions can be established.

In addition to configuring the `exec-timeout` command correctly, it is also a good practice to delete idle virtual terminal sessions using the commands that are shown in the following example:

```
Router# show users
Line User Host(s) Idle Location
2 vty 0 cisco idle 00:07:40 128.107.241.177
* 3 vty 1 cisco idle 00:00:00 128.107.241.177

Router# clear line 2
```

If the workarounds in the preceding scenarios are ineffective, as a last resort, you can restart the Cisco Catalyst 8000V instance from the Azure portal.



CHAPTER 5

Usage Guidelines for User-Defined Routes

Introduction to the Cisco Catalyst 8000V Route Tables

This section provides guidelines which will help you to decide user-defined routes to add to the route tables. When you deploy a Cisco Catalyst 8000V in a Virtual Network using the Microsoft Azure Marketplace template, a route table is created for each subnet to which the Cisco Catalyst 8000V has a network connection. For example, if you deploy a 4-NIC version of the Cisco Catalyst 8000V from the Microsoft Azure Marketplace, 4 subnets are created. Each subnet has an associated route table. No routes are automatically installed in the route table.

For further information on defining user-defined routes, see the *User Defined Routes* section in this Microsoft Azure documentation: https://docs.microsoft.com/en-us/azure/.

- User Defined Routes in the Same Virtual Network, on page 23
- Routing between Virtual Networks or On-Premises Networks, on page 23
- User Defined Routes for High Availability, on page 24

User Defined Routes in the Same Virtual Network

By default, the Microsoft Azure network infrastructure provides a basic routing service which interconnects all the subnets within a virtual network. Packets can be passed between any virtual machines within the same virtual network without the assistance of the Cisco Catalyst 8000V instance.

However, if you need inter-subnet packets to be delivered to the Cisco Catalyst 8000V (to implement advanced services such as filtering and QoS) you need to install a user-defined route in the routing table for the subnet that designates the Cisco Catalyst 8000V instance as the next hop router.

Routing between Virtual Networks or On-Premises Networks

The Microsoft Azure network infrastructure does not, by default, interconnect different virtual networks or connect virtual networks to on-premises networks. To connect to these networks, you must create a user-defined route in each route table to specify the Cisco Catalyst 8000V as the next hop router to each remote network. The user-defined route can be either a default route or a specific destination route. To force traffic through Cisco Catalyst 8000V, either install a default route or a specific destination route in the route table that points to Cisco Catalyst 8000V.

Note If a default route is installed in a route table, all the traffic is diverted to the specified next hop. This causes a problem if you have virtual machines with an allocated public IP address (used for management access to the VM). If you have a default route in the route table associated with the subnet, the virtual machine is not reachable through its public IP address.

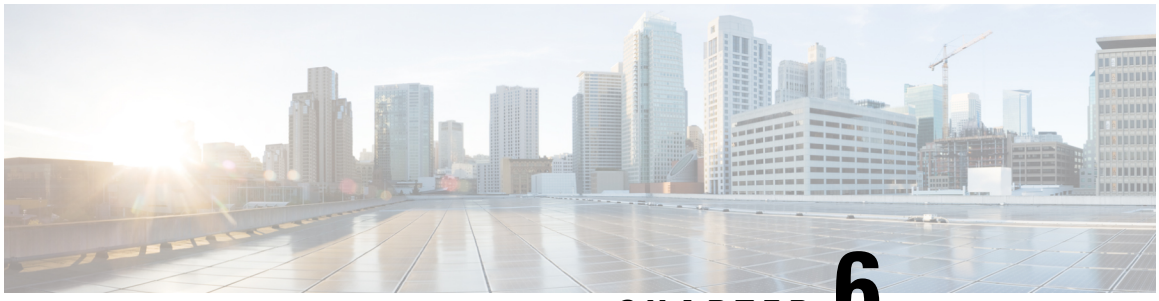
Note Microsoft Azure supports a feature called VNET Peering which can interconnect virtual networks as long as they are hosted in the same region. In order to use VNET Peering and utilize services within Cisco Catalyst 8000V, you must add a user-defined route to force the traffic through Cisco Catalyst 8000V.

User Defined Routes for High Availability

You can deploy two Cisco Catalyst 8000V instances in the same virtual network to provide 1:1 redundancy for high availability. When you configure a Cisco Catalyst 8000V instance with high availability, it monitors the reachability of its peer router. If Cisco Catalyst 8000V believes that the peer router has gone down, it installs its own IP address in the route table. This causes the traffic to be routed through the "working" Cisco Catalyst 8000V instance.

When you configure user-defined routes, you need to decide if you want the entries in the route table to be updated when there is a failure of one of the Cisco Catalyst 8000V peer routers. You must configure a redundancy node for each user-defined route table if the route table is one in which the high availability feature needs to redirect traffic to the “working” Cisco Catalyst 8000V.

All the routes in the route table specified by a redundancy node are updated in the case of a Cisco Catalyst 8000V peer failure.



CHAPTER 6

Configure Accelerated Networking

What is Accelerated Networking

Accelerated networking enables single root I/O virtualization (SR-IOV) on VMs such as a Cisco Catalyst 8000V VM. The accelerated networking path bypasses the virtual switch, increases the speed of network traffic, improves the networking performance, and reduces the network latency and jitter.

Usually, all the networking traffic in and out of the VM traverses the host and the virtual switch. However, with accelerated networking, the network traffic arrives at the virtual machine's network interface (NIC), and is then forwarded to the VM. Thus, all the network policies that the virtual switch applies are now offloaded and applied in the hardware.

For more information about the accelerated networking functionality that is available in Microsoft Azure, see Create a Linux VM With Accelerated Networking Using Azure CLI.

Accelerated networking is available in Cisco Catalyst 8000V public cloud deployments and in government cloud deployments.

Support for Azure-PMD

The Azure-PMD (Poll Mode Driver) functionality on Azure offers a faster, user-space packet processing framework for performance-intensive applications. This framework bypasses the virtual machine's kernel network stack. In a typical packet processing that uses the kernel network stack, the process is interrupt-driven. When the network interface receives the incoming packets, there is an interruption to the kernel to process the packet and a context switch from the kernel space to the user space. Azure-PMD eliminates the context switching and the interrupt-driven method in favor of a user-space implementation that uses poll mode drivers for fast packet processing.

You can enable the Azure-PMD functionality for Cisco Catalyst 8000V running on Microsoft Azure. This functionality increases the performance of the Cisco Catalyst 8000V instance when compared to the previous versions that use accelerated networking.

Supported VM Instance Types

The following VM instance types support the Accelerated Networking functionality:

IOS XE Version	Supported VM Instance Types
17.4.x and later	DS2_v2 / D2_v2 DS3_v2 / D3_v2 DS4_v2 / D4_v2

IOS XE Version	Supported VM Instance Types
	F16s_v2 F32s_v2

Support for Mellanox Hardware

Microsoft Azure cloud has two types of hardware that support the accelerated networking functionality. The following table specifies the Mellanox versions supported for the accelerated networking functionality.

Table 1: Compatibility Matrix of IOS Versions and Accelerated Networking

IOS XE Version	Support for Accelerated Networking	Support for MLX4	Support for MLX5	Support for Azure-PMD
17.4.x and later	Yes	Yes	Yes	Yes

Note Currently, Mellanox ConnectX-3 (CX3) vNIC uses the MLX4 drivers, and ConnectX-4 vNIC (CX4) uses the MLX5 drivers. You cannot specify which NIC Azure must use (MLX4 or MLX5) for your VM deployment.

In the Cisco IOS XE 17.4.1 release, support for the Azure DPDK failsafe/TAP/MLX IOD model was added for both CX3 and CX4 drivers. From the Cisco IOS XE 17.8.1 release, the DPDK failsafe/TAP/MLX I/O model has been replaced with the DPDK NETVSC PMD I/O model. With this update, you experience less overhead while using the accelerated networking functionality.

Note To enable the throughput license performance, you must enable the accelerated networking functionality.

- Enable Accelerated Networking, on page 26
- Disable Accelerated Networking, on page 28
- Verifying Accelerated Networking, on page 28

Enable Accelerated Networking

To enable accelerated networking on a Cisco Catalyst 8000V instance, run the `router# show platform software system hypervisor` command.

```
Router#show platform software system hypervisor
Hypervisor: AZURE
Manufacturer: Microsoft Corporation
Product Name: Virtual Machine
Serial Number: 0000-0016-9163-0690-4834-7207-16
UUID: 80cbc2ea-29e6-cc43-93e9-f541876836f2
Image Variant: None

Cloud Metadata
-------------------
Region: eastus
```

```
Zone:
Instance ID: eac2cb80-e629-43cc-93e9-f541876836f2
Instance Type: Standard_DS4_v2
Version:
Image ID:
Publisher:
Offer:
SKU:

Interface Info
------------------
Interface Number : 0
IPv4 Public IP: 192.168.61.135
IPv4 Private IP: 10.0.0.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.0.3
IPv4 Gateway: 10.0.0.1
MAC Address: 000D3A103B48

Interface Number : 1
IPv4 Public IP:
IPv4 Private IP: 10.0.1.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.1.3
IPv4 Gateway: 10.0.0.1
MAC Address: 000D3A103348

Interface Number : 2
IPv4 Public IP:
IPv4 Private IP: 10.0.4.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.2.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827BA0F

Interface Number : 3
IPv4 Public IP:
IPv4 Private IP: 10.0.3.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.3.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827B2A6

Interface Number : 4
IPv4 Public IP:
IPv4 Private IP: 10.0.4.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.4.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827B5CB
```



Caution Due to a Microsoft Azure limitation, enabling accelerated networking on all the interfaces of a Cisco Catalyst 8000V router might cause a significant performance drop if packets greater than 1500 bytes are sent across the Azure infrastructure. The performance degradation occurs because Azure starts fragmenting the packets at 1438 bytes and drops out the sequence packets. This is a known issue and a support case is currently opened with Microsoft.

To enable accelerated networking, create or modify a vNIC using the **az network nic** command and the `--accelerated-networking` option. See the Microsoft Azure documentation for the az network nic command and also refer to the following examples.

Note Depending on how you created the Cisco Catalyst 8000V instance, accelerated networking might initially be disabled on the Cisco Catalyst 8000V NICs. If accelerated networking is disabled on the NIC and you want to enable accelerated networking on an interface, use one of the commands as shown in the following examples.

Example 1

This example shows how to create a vNIC "mynic1" and enable accelerated networking using the **az network nic create** command with the `--accelerated-networking true` option.

```
az network nic create -n mynic1 -g "RG1" --accelerated-networking true -l "east us"
--vnet-name "vnetname" --subnet "subnet1"
```

Example 2

This example shows how to create a vNIC "mynic2" and enable accelerated networking using the **az network nic create** command with the `--accelerated-networking true option` option.

```
az network nic create -n "mynic2" -g "RG1" --accelerated-networking true -l "east us"
--vnet-name "vnetname" --subnet "subnet1"
```

Example 3

This example shows how to modify a vNIC "mynic3" to enable accelerated networking using the **az network nic update** command with the `--accelerated-networking true` option.

```
az network nic update -n mynic3 -g rg1 --accelerated-networking true
```

Disable Accelerated Networking

To disable accelerated networking for Cisco Catalyst 8000V, you can create or modify a vNIC using the **az network nic** command and the `--accelerated-networking` option.

For more information about the command, see the Microsoft Azure documentation for the az network nic command.

Example

This example shows how to modify a vNIC "mynic1" to disable Accelerated Networking using the **az network nic update** command with the `--accelerated-networking false` option.

```
az network nic update -n "mynic1" -g rg1 --accelerated-networking false
```

Verifying Accelerated Networking

After Enabling accelerated networking on the NICs, use the following IOS commands to verify whether accelerated networking is enabled on the NIC. The Azure infrastructure uses Mellanox NICs to achieve SR-IOV or accelerated networking.

You can use the following commands to verify Cisco Catalyst 8000V NICs by using the Mellanox kernel drivers as the NIC's I/O drivers to process the packets. In addition, the Mellanox NICs in the HyperV server

of the Azure infrastructure presents a bonded interface to the Cisco Catalyst 8000V guest VM. This VM is used for accelerated networking, and the VM is in a bonded state whenever accelerated networking is enabled.

Verifying Accelerated Networking for Cisco Catalyst 8000V 17.4.x (With Azure-PMD)

After enabling accelerated networking on the NICs, use the following IOS commands to verify whether accelerated networking with Azure-PMD is enabled on NIC. The Azure infrastructure uses Mellanox NICs to achieve SR-IOV or accelerated networking.

Use the following commands to verify the Cisco Catalyst 8000V NICs by using the Mellanox Azure-PMD drivers as the NIC's I/O drivers to process the packets. In addition, the Mellanox NICs in the HyperV server of the Azure infrastructure presents a bonded interface to the Cisco Catalyst 8000V guest VM. This VM is used for accelerated networking, and the VM is in a bonded state while accelerated networking is enabled. Note that the bonded interfaces share the same MAC address. The aggregate counters appear on Gi interfaces, while the non-accelerated packets counters appear on the net_tap interfaces. The accelerated packets counters appear on the net_mlx interfaces.

In the following example, the interface Gi2 indicates that a majority of the packets are flowing over the net_mlx interface.

```
Router#show platform hard qfp act dat pmd controllers | inc NIC|good_packets
NIC extended stats for port 0  (Gi1) net_failsafe 000d.3a8f.1bf1 xstats count 13
  rx_good_packets: 411
  tx_good_packets: 326
NIC extended stats for port 1  (Bonded) net_mlx5 000d.3a8f.1bf1 xstats count 35
  rx_good_packets: 389
  tx_good_packets: 326
NIC extended stats for port 2  (Bonded) net_tap 000d.3a8f.1bf1 xstats count 13
  rx_good_packets: 22
  tx_good_packets: 0
NIC extended stats for port 3  (Gi2) net_failsafe 000d.3a8f.1040 xstats count 13
  rx_good_packets: 10638289
  tx_good_packets: 3634525
NIC extended stats for port 4  (Bonded) net_mlx5 000d.3a8f.1040 xstats count 35
  rx_good_packets: 10639534.  ==>>> This verifies Accelerated Networking is working properly
 for RX
  tx_good_packets: 3636099    ==>>> This verifies Accelerated Networking is working properly
 for TX
NIC extended stats for port 5  (Bonded) net_tap 000d.3a8f.1040 xstats count 13
  rx_good_packets: 291
  tx_good_packets: 0
NIC extended stats for port 6  (Gi3) net_failsafe 000d.3a8f.1a90 xstats count 13
  rx_good_packets: 3637187
  tx_good_packets: 10522981
NIC extended stats for port 7  (Bonded) net_mlx5 000d.3a8f.1a90 xstats count 35
  rx_good_packets: 3638631
  tx_good_packets: 10524554
NIC extended stats for port 8  (Bonded) net_tap 000d.3a8f.1a90 xstats count 13
  rx_good_packets: 28
  tx_good_packets: 0
```

Verifying Accelerated Networking for Cisco Catalyst 8000V 17.8.x (With Azure PMD)

From the Cisco IOS XE 17.8.1 release, the previous DPDK failsafe/TAP/MLX I/O model has been replaced with the DPDK NETVSC PMD I/O model. Use the following commands to verify the accelerated networking functionality on a Cisco Catalyst 8000V running on Cisco IOS XE Release 17.8.x.

The **show platform hardware qfp act dat pmd controllers** command displays the devices that are bonded to the net_netvsc ports.

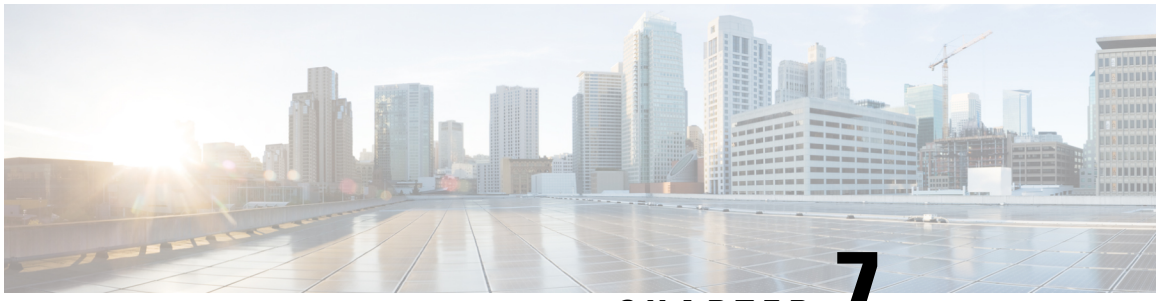
```
Router#show platform hardware qfp active datapath pmd controllers | inc NIC |good_packets
NIC extended stats for port 0 (Gi2) net_netvsc 000d.3a10.3348 xstats count 56
rx_good_packets: 411
tx_good_packets: 350
tx_q0_good_packets: 311
rx_q0_good_packets: 100
vf_rx_good_packets: 487
vf_tx_good_packets: 350
NIC extended stats for port 1 (Gi1) net_netvsc 000d.3a10.3b48 xstats count 56
rx_good_packets: 60359
tx_good_packets: 55464
tx_q0_good_packets: 6579
rx_q0_good_packets: 5633
vf_rx_good_packets: 53780  ==>>> This verifies Accelerated Networking is working properly
for RX
vf_tx_good_packets: 49831  ==>>> This verifies Accelerated Networking is working properly
for TX
NIC extended stats for port 2 (Gi4) net_netvsc 0022.4827.b2a6 xstats count 56
rx_good_packets: 0
tx_good_packets: 0
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 3 (Gi5) net_netvsc 0022.4827.b5cb xstats count 56
rx_good_packets: 0
tx_good_packets: 0
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 4 (Gi3) net_netvsc 0022.4827.ba0f xstats count 56
rx_good_packets: 0
tx_good_packets: 0
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 5 (Bonded) net_mlx4 0022.4827.b2a6 xstats count 13
rx_good_packets: 0
tx_good_packets: 0
NIC extended stats for port 6 (Bonded) net_mlx4 0022.4827.b5cb xstats count 13
rx_good_packets: 0
tx_good_packets: 0
NIC extended stats for port 7 (Bonded) net_mlx4 000d.3a10.3b48 xstats count 13
rx_good_packets: 54726
tx_good_packets: 65464
NIC extended stats for port 8 (Bonded) net_mlx4 0022.4827.ba0f xstats count 13
rx_good_packets: 363863
tx_good_packets: 105245
NIC extended stats for port 9 (Bonded) net_mlx4 000d.3a10.3348 xstats count 13
rx_good_packets: 0
tx_good_packets: 0
```

The **show platform software vnic-if interface-mapping** command indicates that net_netvsc driver is used from the Cisco IOS XE 17.8.1 release.

```
show platform software vnic-if interface-mapping
------------------------------------------------------------
 Interface Name        Driver Name         Mac Addr
------------------------------------------------------------
 GigabitEthernet3       net_netvsc         000d.3a4e.7542
 GigabitEthernet2       net_netvsc         000d.3a4e.7163
 GigabitEthernet1       net_netvsc         000d.3a4e.757d
------------------------------------------------------------
```

The **show platform software vnic database** command indicates whether MLX4 or MLX5 is present and also indicates the PMD that is used.

```
show platform software vnic-if database
vNIC Database
  eth00_1572882209232255500
    Device Name : eth0
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.757d
    PCI DBDF    : b421:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth01_1572882212261074300
    Device Name : eth1
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.7542
    PCI DBDF    : 83e2:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth02_1572882215293497600
    Device Name : eth2
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.7163
    PCI DBDF    : be1d:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth_15__1572882218326526600
    Device Name : Gi1
    Driver Name : hv_netvsc
    MAC Address : 000d.3a4e.757d
    PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
    Server      : IFDEV_SERVER_UIO
    Management  : no
    Status      : supported
  eth_16__1572882223436559900
    Device Name : Gi2
    Driver Name : hv_netvsc
    MAC Address : 000d.3a4e.7163
    PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
    Server      : IFDEV_SERVER_UIO
    Management  : no
    Status      : supported
  eth_17__1572882228553741500
    Device Name : Gi3
    Driver Name : hv_netvsc
    MAC Address : 000d.3a4e.7542
    PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
    Server      : IFDEV_SERVER_UIO
    Management  : no
    Status      : supported
```



CHAPTER 7

Deploy Azure Transit VNET DMVPN Solution

- Prerequisites for Deploying the Transit VNet Solution, on page 33
- Restrictions for Deploying the Transit VNet Solution, on page 33
- How to Deploy Azure Transit VNET DMVPN, on page 33
- Troubleshooting, on page 42

Prerequisites for Deploying the Transit VNet Solution

- You must have an Azure account for your Cisco Catalyst 8000V instance.
- Ensure that your licenses are registered and valid.
- Ensure that the hub is up and running before you configure the spokes.

Restrictions for Deploying the Transit VNet Solution

- You cannot deploy a Spoke VNet in another Cloud Service Provider.
- You cannot configure the transit VNet solution for all locations. To view the list of locations that are supported, after you create an instance, see all the options in the **Location** field from the Configure Basic Settings page.

How to Deploy Azure Transit VNET DMVPN

Create a Transit VNet Hub

This procedure is the first step in configuring the transit VNet solution. This is a very important part of the deployment where you have to configure the Transit VNet settings. These settings correspond to the DMVPN IPsec parameters that are stored as metadata in the Transit-VNet storage account with an Access-Key. When configuring the spoke templates, you need to configure the TVNET Storage account and the Access-key only. The relevant DMVPN IPsec parameters required for spokes are automatically selected from the device.

Procedure

Step 1 Sign in to the Microsoft Azure portal.

Step 2 Click **Create a Resource**, search for your Cisco Catalyst 8000V deployment, and press **Enter**. The system searches and displays the Transit VNET templates for DMVPN.

Step 3 Select **Transit VNET DMVPN** > **Create**.

Step 4 In the Basics screen, enter the name of the Virtual machine, the name for the Transit VNet hub, and your username.

Note
Ensure that you use only lower case for **Transit VNet Name**.

Step 5 From the **Authentication Type** drop-down list, select the **SSH Public Key** option.

Step 6 Specify a password and reenter the password to confirm.

Step 7 Select the appropriate image version from the **SKU** drop-down list.

Step 8 From the **Location** drop-down list, select one of the regions where TVNET hub can be deployed.

Step 9 In the Cisco C8000V Settings page, configure the settings. For more information on configuring the Cisco Catalyst 8000V settings, see the *Deploying the Cisco Catalyst 8000V on Microsoft Azure* section.

Step 10 In the Transit VNet Settings, configure the following settings:

a) **TVNET Storage Account** – The storage account name that is derived from the Transit VNet name with the keyword 'strg' added to the name. You require this value while creating a spoke.The value in this field is auto-populated. However, you can edit the value in this field.

b) **Private TVNET Storage Account** – Select the storage account which is required for saving keys. This field is required for Autoscaler deployments.

c) **DMVPN Tunnel ID** - The Tunnel ID used for setting up tunnel in all the Cisco Catalyst 8000V devices – both hub and spoke.

d) **DMVPN Tunnel Key** - The Tunnel Key, which is a 6-8 digit numerical value.

e) **IPSEC Tunnel Authentication** -

f) **IPSEC Tunnel Cipher** -

g) **IPSEC Shared Key** – The keyword for authenticating the tunnel.

h) **DMVPN Tunnel Network** – The tunnel network that is used for the DMVPN overlay.

Note
The default option might clash with the VNet created for the Hub. Ensure that this value does not overlap with the exiting Virtual Networks (VNet).

At this point, you don't have to configure subnets through the **Configure Subnets** section.

Step 11 Verify the parameters in the Summary screen, and click **OK**.

Step 12 From the **Buy** section, click **Create** to deploy the Transit VNet Hub solution. This step creates the following resources:

- 2 Cisco Catalyst 8000V instances (C8000V1 & C8000V2) Virtual-machines deployed in a single Availability-Set
- 2 Storage disks (1 each for each Cisco Catalyst 8000V)
- 4 NICs (2 NICs for each Cisco Catalyst 8000V instance)
- 1 Security-Group for the entire Transit-VNET (which opens up only SSH for inbound)
- 2 Public-IP's (1 PIP for each instance)

- 2 Route-Tables (1 RT for each subnet of the instance)
- 2 Storage Accounts (1 Storage for the Cisco Catalyst 8000V Diagnostics and 1 Storage for Transit-VNET metadata)
- 1 VNET /16 CIDR
- All the above deployed using 1 Resource-Manager group (deleting this RG will delete all the above components)

It takes several minutes for the deployment to be complete and for the resources to be created. You can monitor the deployment by clicking **All Resources** and choosing the **Group By Type** option. After the deployment is complete, the notification panel displays the message *Deployment Succeeded*.

Create an Azure DMVPN Spoke VNET

Before you begin

Ensure that your Hub is created successfully before you create a Spoke for the transit VNet solution.

Procedure

Step 1 From the Microsoft Azure Marketplace, search and select the **Cisco CSR 1000V DMVPN Transit VNet** template.

Step 2 Click the template, and select the appropriate Spoke option that you want, from the drop-down list.

Step 3 Click **Create**.

Step 4 In the Basics settings screen, ensure that you specify the following configuration details:

a) **Filename** – Specify the name of the Transit VNet in this field.

b) **Transit VNet Storage Name** – This is the same as the TVNET Storage Account value from the Hub configuration. This name is derived from the Transit VNet name with ‘strg’ keywork added.

c) **Storage Key** – To access the Storage Key, search and click the public Hub and click the **Access Key** option.

Step 5 Configure the other values in the Basics Settings screen, and click **OK**.

Step 6 In the Cisco Catalyst 8000V Settings screen, you can choose to either configure the fields or leave them as is (default values).

For information about the parameters, see *How to Deploy aCisco Catalyst 8000V on Microsoft Azure*.

Note
Availability Zones are not yet fully supported with all the regions in Microsoft Azure. The solution template hence does not have an option for availability zones, but resiliency is taken care using “Availability-Sets”. For more information, see the Microsoft Azures documentation: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview.

Step 7 Click the arrow next to **Virtual Network** to specify values for the virtual network and click **OK**.

Step 8 In the **Address Space** field, enter the address of the virtual network using Classless Inter-Domain Routing (CIDR) notation.

Note
The VNET CIDR denotes the physical ip-address subnets that will be used for the Cisco Catalyst 8000V devices in the TVNET-HUB. The CIDR block is usually a /16 subnet which will be subnetted further into two /24 subnets. The first 3 IP addresses of each subnet will be reserved for Azure Route-Table and other services. The IP allocations begin from

the 4th ip of the subnet and this will be automatically mapped to the public ip that is assigned dynamically. The public ip enables access to Internet, hence becomes the NBMA address in the DMVPN scenario.

Step 9 Click the arrow next to **Configure the Subnets**, and click **OK**.

Step 10 In the Summary screen, review the configured parameters. After you validate the template, click **OK**.

Step 11 Click **Create** to deploy the TVNet Spoke solution.

Note
For every additional Spoke that you want to create, follow steps 1 through 10.

Verifying the Configuration

Verifying on the Transit VNET Hubs

The following commands show that the spokes have successfully established DMVPN tunnels to Transit VNet Hub1 and are able to exchange EIGRP routes with the Transit VNet Hub1. The solution enables DMVPN-Phase 3 feature - NHRP Shortcut Switching. When these commands are run on Transit VNet Hub2, the command outputs are similar to Transit VNet Hub1. This indicates that the spokes have successfully established DMVPN tunnels to both the Cisco Catalyst 8000V in the Transit VNet hubs and have successfully exchanged EIGRP routes with both the hubs. The hubs are deployed in active-active mode for greater resiliency.

Procedure

Step 1 Run the `show ip interface` brief command.

Example:

```
Transit-Hub# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.1.0.4        YES DHCP   up                    up
GigabitEthernet2       10.1.1.5        YES DHCP   up                    up
Tunnel11               172.16.1.1      YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
p1-tvnet-csr-1#
```

Notice the higlighted portion in the configuration output. This indicates that the Tunnel is up. If the system does not display the Tunnel in this configuration output, you must go to the guestshell and look at the TVNet logs. Run the `show log` command to access the TVNet logs.

Step 2 Run the `show crypto isakmp sa` command to view the IKE sessions for the two DMVPN connections from the spokes.

Example:

```
Transit-Hub# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.0.4        168.62.164.228  QM_IDLE           1042 ACTIVE
10.1.0.4        40.114.69.24    QM_IDLE           1043 ACTIVE
IPv6 Crypto ISAKMP SA
```

Step 3 Run the `show crypto session` command to view the IPsec sessions for the two DMVPN connections from the spokes.

Example:

```
Transit-Hub# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1043 lifetime:18:32:04
  IPSEC FLOW: permit 47 host 10.1.0.4 host 40.114.69.24
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607996/3474
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607998/3474
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 168.62.164.228 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 11.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 168.62.164.228/4500 Active
          Capabilities:DN connid:1042 lifetime:18:02:01
  IPSEC FLOW: permit 47 host 10.1.0.4 host 168.62.164.228
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607970/2427
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607982/2427
```

Step 4 Run the `show dmvpn` command to view the status of the DMVPN on the device.

Example:

```
Transit-Hub# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.114.69.24       172.16.1.137    UP     1w3d    DN
     1 168.62.164.228     172.16.1.147    UP     1w3d    DN
```

Step 5 Run the `show vrf` command to view the display routes from each of the spokes on the transit VNet.

Example:

```
Transit-Hub# show vrf
```

```
  Name                              Default RD            Protocols   Interfaces
  tvnet-Tun-11                      64512:11              ipv4        Tu11
```

Step 6 Run the `show ip eigrp vrf <vrf-name> neighbors` command to view the status of the EIGRP neighbors.

Example:

```
Transit-Hub# show ip eigrp vrf tvnet-Tun-11 neighbors
EIGRP-IPv4 Neighbors for AS(64512) VRF(tvnet-Tun-11)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.1.137            Tu11                     14 1w3d       13  1398  0  12
0   172.16.1.147            Tu11                     10 1w3d       12  1398  0  12
```

Step 7 Run the `show ip route vrf <vrf-name>` command to view the route specific to a VRF.

Example:

```
Transit-Hub# show ip route vrf tvnet-Tun-11
Routing Table: tvnet-Tun-11
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      11.0.0.0/24 is subnetted, 2 subnets
D EX     11.1.0.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
D EX     11.1.1.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
D EX     12.1.1.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Tunnel11
L        172.16.1.1/32 is directly connected, Tunnel11
D EX  192.168.35.0/24 [170/26905600] via 172.16.1.147, 1w1d, Tunnel11
                      [170/26905600] via 172.16.1.137, 1w1d, Tunnel11
```

Verifying the Connectivity Between the Spokes and the Hub

The following commands show that the spokes are connected to both the Cisco Catalyst 8000V TVNET HUBs and have been able to exchange the EIGRP routes from both the hubs. As the DMVPN solution is deployed as DMVPN-Phase3 (NHRP shortcut-switching) and the hubs are deployed in the active-active mode, the EIGRP route towards SPOKE2 points to the tunnel-overlay ip-address of spoke2.

Procedure

Step 1 Run the `show ip interface brief` command to view the interface ip addresses on the device.

Example:

```
Spoke# show ip interface brief
```

```
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       11.1.0.4        YES DHCP   up                    up
GigabitEthernet2       11.1.1.4        YES DHCP   up                    up
Tunnel11               172.16.1.147    YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
```

Step 2 Run the `show dmvpn` command to check the status of the DMVPN on the device.

Example:

```
Spoke# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
```

Notice the configuration output that is highlighted. This indicates that the spokes are up and have established a connection with the hub.

Step 3 Run the `show crypto isakmp sa` command to view the IKE sessions for the two DMVPN connections from the spokes.

Example:

```
Spoke# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
40.117.131.133  11.1.0.4        QM_IDLE           1025 ACTIVE
40.117.128.85   11.1.0.4        QM_IDLE           1026 ACTIVE
IPv6 Crypto ISAKMP SA
```

Step 4 Run the `show crypto session` command to view the IPsec sessions for the two DMVPN connections from the spokes.

Example:

```
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:33:41
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2250 drop 0 life (KB/Sec) 4607927/726
        Outbound: #pkts enc'ed 2251 drop 0 life (KB/Sec) 4607957/726
```

```
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
          Capabilities:DN connid:1026 lifetime:17:33:44
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2252 drop 0 life (KB/Sec) 4607960/2046
        Outbound: #pkts enc'ed 2253 drop 0 life (KB/Sec) 4607976/2046
```

Step 5 Run the `show up eigrp neighbor` command to view the status of the EIGRP neighbors.

Example:

```
Spoke# show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(64512)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.1.2              Tu11                     13 1w3d       24  1362  0  23
0   172.16.1.1              Tu11                     12 1w3d        8  1362  0  23
```

Step 6 Run the show ip route eigrp command to view the EIGRP route information.

Example:

```
Spoke# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 11.1.0.1 to network 0.0.0.0
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
D EX     12.1.1.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
```

Verifying Spoke to Spoke Connectivity

The following commands help in testing connection between two spokes. As the feature supported is DMVPN-Phase 3, the **traceroute** command displays the packets sent from spoke 1 to spoke 2. However, the first packet is lost due to NHRP resolution as Spoke 1 sends the packet to the hub to obtain the address of Spoke 2. When Spoke 1 receives the address, a dynamic IPsec tunnel is established between Spoke 1 and Spoke 2.

```
Spoke1# clear crypto sa counters
Spoke1# ping 12.1.1.4 source gigabitEthernet 2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 12.1.1.4, timeout is 2 seconds:
Packet sent with a source address of 11.1.1.4
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/1/6 ms
Spoke# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
     1 40.114.69.24       172.16.1.137    UP 00:00:07    DN
Spoke# traceroute 12.1.1.4 source gigabitEthernet 2
Type escape sequence to abort.
Tracing the route to 12.1.1.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.137 2 msec *  3 msec
p1spoke1#
p1spoke1#
p1spoke1#sh crypto sess detail | i pkts
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3581
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3581
        Inbound:  #pkts dec'ed 12 drop 0 life (KB/Sec) 4607924/621
        Outbound: #pkts enc'ed 14 drop 0 life (KB/Sec) 4607955/621
        Inbound:  #pkts dec'ed 13 drop 0 life (KB/Sec) 4607957/1941
        Outbound: #pkts enc'ed 13 drop 0 life (KB/Sec) 4607975/1941
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 00:00:36
Session status: UP-ACTIVE
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1027 lifetime:23:59:23
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.114.69.24
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3563
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3563
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:31:38
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 16 drop 0 life (KB/Sec) 4607923/603
        Outbound: #pkts enc'ed 18 drop 0 life (KB/Sec) 4607955/603
```

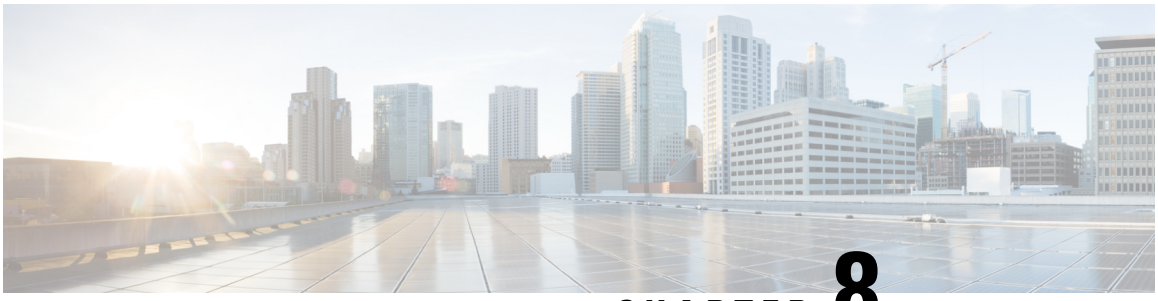
```
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
          Capabilities:DN connid:1026 lifetime:17:31:41
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 17 drop 0 life (KB/Sec) 4607957/1923
        Outbound: #pkts enc'ed 17 drop 0 life (KB/Sec) 4607975/1923
```

Troubleshooting

To view the status of your deployment, log in to your Cisco Catalyst 8000V instance and run the `show log` command. If your depolyment is successful you should see the *[AzureTransitVNET] Success. Configured all the required IOS configs* message.

If you do not see this message and experience any errors while configuring the Transit VNet solution, check whether:

- The DMVPN tunnel is established between the hub and the spoke. In most cases, there might be a problem with the following values: *TransitVNETname*, *TransitVNETStoragename* or *TransitVNETStoragekey*.
- The Guestshell is up and running for the TVNet packages that are to be installed.



CHAPTER 8

Configure LISP Layer 2 Extension

You can deploy Cisco Catalyst 8000V instances on public, private, and hybrid clouds. When enterprises move to a hybrid cloud, they need to migrate the servers to the cloud without making any changes to the servers. Enterprises may want to use the same server IP address, subnet mask, default gateway configurations, and their own IP addressing scheme in the cloud, and not be limited by the addressing scheme of the cloud provider infrastructure.

To fulfill this requirement, you can use LISP, which is an architecture that allows you to separate the location (enterprise data center or public cloud) and the identity (server IP address) so that you can create new servers on the cloud with the same IP address. In the LISP architecture, the endpoint ID-to-router locator (EID-to-RLOC) mapping of the server is updated to reflect the new location that is moved to the cloud. Further, no changes are required to the end systems, users, or servers because LISP handles the mapping between the identity and the location.

LISP operates as an overlay, encapsulating the original packet from the server into a User Datagram Protocol (UDP) packet along with an additional outer IPv4 or IPv6 header. This encapsulation holds the source and destination router locators and allows the server administrators to address the server in the cloud according to their own IP addressing scheme, independent of the cloud provider's addressing structure.

You can configure Layer 2 Extension on Cisco Catalyst 8000V instances running on Microsoft Azure, where the instance acts as the bridge between the enterprise data center and the public cloud. By configuring the Layer 2 Extension, you can extend your Layer 2 networks in the private data center to a public cloud to achieve host reachability between your site and the public cloud. You can also enable the migration of your application workload between the data center and the public cloud.

Benefits

- Move the Public IP addresses between different geographic locations or split them between different public clouds. In either case, the LISP IP-Mobility solution provides optimal routing between clients on the Internet and the public IP address that has moved, regardless of the location. To know more about achieving IP mobility for the Azure cloud, see Achieving IP Mobility.
- Carry out data migration with ease and optimize the workload IP address in your network. Usually, IP address changes cause complexity and additional delays in a solution. By using L2 extension for cloud, you can migrate workloads while retaining the original IP address without any network constraints. To learn more about this use case, see Data Migration Use Case.
- Virtually add a VM that is on the provider site to facilitate cloud bursting to virtually insert a VM in the Enterprise server while the VM runs on the provider site.
- Provide backup services for partial disaster recovery and disaster avoidance.

- Prerequisites for configuring LISP Layer 2 Extension, on page 44
- Restrictions for configuring LISP Layer 2 Extension, on page 44
- How to configure LISP Layer 2 Extension, on page 44
- Verify the LISP Layer 2 Traffic Between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the Enterprise System, on page 49

Prerequisites for configuring LISP Layer 2 Extension

- Ensure that the underlay for your solution is ready before you configure the L2 Extension.
- Since clouds do not support Address Resolution Protocol (ARP), and the cloud infrastructure is not aware of the hosts in the remote site, you must add a virtual IP to help the cloud route the packets appropriately to the edge router. To add a virtual or alias IP, see Add an IP address for an Azure interface.
- Each Cisco Catalyst 8000V instance must be configured with one external IP address. In this case, an IPsec tunnel is built either between the IP addresses of the two Cisco Catalyst 8000V instances, or between the Cisco Catalyst 8000V instance and the ASR1000 device. Ensure that the IPsec tunnel has a private address.
- Ensure that the IPsec tunnel is working between the IP address of the two Cisco Catalyst 8000V instances or between the Cisco Catalyst 8000V instance and the ASR1000 device.
- Depending on your solution, ensure that a ping is successful between: the two Cisco Catalyst 8000V instances, between a Cisco Catalyst 8000V and an ASR1000 device, and between the VMs and the hosts.

Restrictions for configuring LISP Layer 2 Extension

- If you move a host from the data center to the cloud or vice-versa, you must first add or remove the secondary address from the virtual IP table in the cloud.
- If you move a VM to the cloud, you must initiate packets to the Cisco Catalyst 8000V instance so that the Cisco Catalyst 8000V device realizes that the VM is now added from the data center to the cloud.
- High Availability does not work with the L2 Extension functionality.
- Azure supports a maximum of 256 IPs. The maximum number of hosts on the remote site or the data center is thus 256.

How to configure LISP Layer 2 Extension

To configure the L2 extension functionality, you must first deploy the Cisco Catalyst 8000V instance on Microsoft Azure and configure the instance as an xTR. You must then configure the mapping system to complete the deployment.

The LISP site uses the Cisco Catalyst 8000V instance configured as both an ITR and an ETR (also known as an xTR) with two connections to upstream providers. The LISP site then registers to the standalone device that you have configured as the map resolver/map server (MR/MS) in the network core. The mapping system performs LISP encapsulation and de-encapsulation of the packets that are going to the migrated public IPs within Azure. Optionally, for traffic that is leaving Azure, whenever a route to the destination is not found

on the C8000V routing table, the Cisco Catalyst 8000V instance routes that traffic through the PxTR at the enterprise data center.

Perform the following steps to enable and configure the LISP xTR functionality when using a LISP map server and map resolver for mapping services:

Deploy Cisco Catalyst 8000V with Multiple Interfaces

Perform the following steps to deploy Cisco Catalyst 8000V with multiple interfaces.

Procedure

Step 1 Select **Virtual machines** in the left hand side panel.

Step 2 Click **Add**.

Step 3 Enter "C8000V".

Finds the Cisco Catalyst 8000V VM deployments in the Azure Marketplace.

Step 4 Choose the deployment of your choice, with 2,4, or 8 NICs.

Step 5 Click **Create**.

Step 6 **Virtual Machine name** - Select the **Basics** sub-menu and enter a name for the virtual machine.

Name of the cloud-based network used by Microsoft Azure to represent a private network.

Step 7 **Username** - Select a user name.

The Username for the Cisco Catalyst 8000V virtual machine which you can use to log into the Cisco Catalyst 8000V instance.

Step 8 **Authentication type** - Enter a Password (default) or SSH public key.

Step 9 **Cisco IOS XE Image Version** - Select the Cisco IOS XE version.

Step 10 **Subscription** - (Optional) Change the subscription name.

A default subscription name is provided, based on the name of the virtual machine. You can change this default subscription name.

Step 11 **Resource Group** - Select either **Create new** or **Use existing**.

You can only create a Cisco Catalyst 8000V in a new Resource Group (or in a completely empty existing resource group). To remove a Resource Group, first delete the Cisco Catalyst 8000V VM and then delete the Resource Group.

Step 12 Click **OK**.

Step 13 Select the **Cisco C8000V Settings** sub-menu and then select **Number of Network Interfaces in C8000V**.

Step 14 Select the number of interfaces: 2, 4, or 8.

Step 15 **License Type** - Select either **BYOL** or **PAYG** as the license type.

Note
PAYG licensing type is not supported in SD Routing devices.

Step 16 **Managed Disk** - Select **Enabled**.

Step 17 **Storage Account** - Enter a name for the storage account.

For more information on storage accounts, see the Microsoft Azure Resources section in this guide.

Step 18 **Virtual machine size** - Select the appropriate virtual machine size.

Based on the number of interfaces that you are using, select the appropriate virtual machine size. Microsoft Azure supports different image types with different performance expectations. To view the supported instance types and the virtual machine sizes, see the following links:

- Dv2 and DSv2 series
- Fsv2 series

Step 19 **Custom Data** - Select **Yes** if you want to provide a bootstrap configuration file.

For further information about providing a bootstrap configuration file for the Cisco Catalyst 8000V instance, see *Deploying a Cisco Catalyst 8000V VM Using a Day 0 Bootstrap File* section and the *Customdata-examples* section.

Step 20 **Availability Set** - Select **Yes**.

Step 21 **Availability Set name** - Enter a name for the availability set.

Step 22 **Availability Set fault domain count** - Enter the availability set fault domain count.

Fault domains define the group of VMs that share a common power source and network switch. Availability sets arrange virtual machines across fault domains.

Step 23 **Availability Set update domain count** - Enter the availability set update domain count.

An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

Step 24 **Boot diagnostics** - Enter the boot diagnostics.

For more information on boot diagnostics, see the *Information About Deploying Cisco Catalyst 8000V in Microsoft Azure* section.

Step 25 **Diagnostics Storage account** - Enter the storage account name.

Step 26 **Public IP Address** - Enter the public IP address name.

For more information on the public IP address, see the *Microsoft Azure Resources* section.

Step 27 **DNS label** - (Optional) Change the name of the DNS label.

The DNS label is the name of the public IP address to be assigned to the Cisco Catalyst 8000V. A default value for the DNS label is shown in the text box, which is the VM name followed by "`-dns`".

Step 28 **Virtual network** - Choose one of the following: **Create New** or **Use existing**.

For a new virtual network, enter the name and the IP address.

Step 29 Click **Subnets** - Enter the subnet names and the IP addresses.

Step 30 Check that all the Cisco Catalyst 8000V Settings are acceptable, and then click **OK**.

The **3 Summary** sub-menu is highlighted.

Step 31 Click **OK**.

The **4 Buy** sub-menu is highlighted.

Step 32 Click **Create**

The VM is created and the purchase is confirmed.

Step 33 Click **Virtual machines** on the left hand panel.

After a few minutes, the status of the recently created VM changes from Creating to Running. Make a note of the Public IP address name.

Configure a tunnel between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the enterprise system

The communication between the Cisco Catalyst 8000V instance deployed within the enterprise data center and the Cisco Catalyst 8000V instance deployed within the public cloud is secured by an IP Security (IPsec) tunnel established between them. The LISP-encapsulated traffic is protected with the IPsec tunnel that provides data origin authentication, integrity protection, anti-reply protection, and confidentiality between the public cloud and the enterprise.

Procedure

Step 1 Configure a Cisco Catalyst 8000V instance on Microsoft Azure.

Run the **interface Loopback** command. Loopback is used as the LISP RLOC which identifies where the migrated customer IP space is located.

Run the **interface Tunnel** command to connect to the Cisco Catalyst 8000V instance on the cloud.

```
interface Loopback1
 ip address 33.33.33.33 255.255.255.255
!
interface Tunnel2
 ip address 30.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 173.39.145.79
 tunnel protection ipsec profile p2p_pf1
!
interface GigabitEthernet2
 ip address 10.10.10.140 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Step 2 Configure a second Cisco Catalyst 8000V instance on the enterprise site.

```
interface Loopback1
 ip address 11.11.11.11 255.255.255.255

interface Tunnel2
 ip address 30.0.0.1 255.255.255.0
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 52.14.116.161
 tunnel protection ipsec profile p2p_pf1
!
!
interface GigabitEthernet3
```

```
 ip address 10.10.10.2 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Configure LISP xTR on the Cisco Catalyst 8000V Instance Running on Azure

Procedure

To configure LISP xTR on the Cisco Catalyst 8000V instance running on the service provider, follow the configuration steps in the Configuring LISP (Location ID Separation Protocol) section.

The Cisco Catalyst 8000V instance on Azure uses the enterprise LISP router as the proxy ETR. Whenever the routing table points to the default route, it sends the traffic to the PETR.

Run the router **lisp command** to enable LISP. Execute the **itr map resolver** and the **itr map server** commands, to configure the Cisco Catalyst 8000V instance on the enterprise as the map server/map resolver.

Example:

```
router lisp
 locator-set azure
  33.33.33.33 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  itr
  etr map-server 11.11.11.11 key cisco
  etr
  use-petr 11.11.11.11
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set azure
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 exit-router-lisp
!
router ospf 11
 network 30.0.0.2 0.0.0.0 area 11
 network 33.33.33.33 0.0.0.0 area 11
!

router lisp
 locator-set dmz
  11.11.11.11 priority 1 weight 100
```

```
 exit-locator-set
!
service ipv4
 itr map-resolver 11.11.11.11
 etr map-server 11.11.11.11 key cisco
 etr
 proxy-etr
 proxy-itr 11.11.11.11
 map-server
 map-resolver
 exit-service-ipv4
!
instance-id 0
 dynamic-eid subnet1
  database-mapping 10.10.10.0/24 locator-set dmz
  map-notify-group 239.0.0.1
  exit-dynamic-eid
 !
 service ipv4
  eid-table default
  exit-service-ipv4
 !
 exit-instance-id
!
site DATA_CENTER
 authentication-key cisco
 eid-record 10.10.10.0/24 accept-more-specifics
 exit-site
!
exit-router-lisp
!
router ospf 11
 network 11.11.11.11 0.0.0.0 area 11
 network 30.0.0.1 0.0.0.0 area 11
!

!
!
```

Verify the LISP Layer 2 Traffic Between Cisco Catalyst 8000V on Azure and Cisco Catalyst 8000V on the Enterprise System

Procedure

Run the following show lisp commands to verify the LISP Layer 2 traffic:

Example:

```
Router#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 2, no-route 0, inactive 0

10.0.1.1/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
```

```
10.0.1.20/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
Router-azure#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 4 entries

0.0.0.0/0, uptime: 00:09:49, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
10.0.1.0/24, uptime: 00:09:49, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.4/30, uptime: 00:00:55, expires: 00:00:57, via map-reply, forward-native
  Encapsulating to proxy ETR
10.0.1.100/32, uptime: 00:01:34, expires: 23:58:26, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
11.11.11.11  00:01:34  up           1/100       -
Router-azure#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 2
  Last dynamic-EID discovered: 10.0.1.20, 00:01:37 ago
    10.0.1.1, GigabitEthernet2, uptime: 00:09:23
      last activity: 00:00:42, discovered by: Packet Reception
    10.0.1.20, GigabitEthernet2, uptime: 00:01:37
      last activity: 00:00:40, discovered by: Packet Reception

Router-DC#show ip lisp
Router-DC#show ip lisp data
Router-DC#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

10.0.1.100/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
11.11.11.11    1/100  cfg-addr   site-self, reachable
Router-DC#show ip lisp
Router-DC#show ip lisp map
Router-DC#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 2 entries

10.0.1.0/24, uptime: 1d08h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.20/32, uptime: 00:00:35, expires: 23:59:24, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
33.33.33.33  00:00:35  up           1/100

Router-DC#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 1
  Last dynamic-EID discovered: 10.0.1.100, 1d08h ago
    10.0.1.100, GigabitEthernet2, uptime: 1d08h
```

```
      last activity: 00:00:47, discovered by: Packet Reception

Router-DC#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
dc             never     no     --                            10.0.1.0/24
               00:08:41  yes#   33.33.33.33                   10.0.1.1/32
               00:01:00  yes#   33.33.33.33                   10.0.1.20/32
               1d08h     yes#   11.11.11.11                   10.0.1.100/32
Router-DC#show ip cef 10.0.1.20
10.0.1.20/32
  nexthop 33.33.33.33 LISP0
Router-DC#

Router#show lisp instance-id 0 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 7, no-route 0, inactive 4

10.20.20.1/32, locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.5/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.6/32, Inactive, expires: 01:20:16
10.230.1.7/32, Inactive, expires: 01:20:16
10.230.1.8/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.31/32, Inactive, expires: 01:21:52
10.230.1.32/32, Inactive, expires: 01:20:16
Router-OnPrem#show lisp instance-id 0 ipv4 map
Router#show lisp instance-id 0 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 6 entries

10.20.0.0/16, uptime: 22:39:53, expires: never, via static-send-map-request
Negative cache entry, action: send-map-request
10.230.1.0/24, uptime: 22:39:53, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.230.1.6/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.7/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.31/32, uptime: 22:38:14, expires: 01:21:45, via map-reply, complete
Locator Uptime State Pri/Wgt Encap-IID
11.11.11.11 22:38:14 up 1/100 -
10.230.1.32/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
```