Setting Up VMware NSX-T for Photon Platform

Contents

1 Introduction

Here's how to set up VMware NSX-T 1.1 to work with Photon Controller 1.1.1. NSX-T must be in place before you install Photon Controller. After NSX-T is installed and configured to work with Photon Controller, you add the information about the NSX network to Photon Controller's YAML deployment file.

In this document, *NSX* refers to NSX-T version 1.1. Only minimal instructions are provided for installing and setting up NSX; if you need help, see the VMware documentation for NSX.

This document assumes that you have obtained valid licenses for NSX and have a VMware account with permission to access and download the NSX installers.

2 Requirements

- NSX-T 1.1.
- At least one ESXi host dedicated to NSX. The required version, update level, and patch number of ESXi appears in the NSX Installation Guide. The ESXi hosts that you use for NSX cannot be used for Photon Controller or Lightwave.
- An ESXi host dedicated as a DHCP server.
- An ESXi host dedicated to Photon Controller.
- An ESXi host dedicated to Lightwave.
- Each ESXi host must have at least 2 NIC cards.

Therefore, you need at least 4 ESXi hosts: one for NSX, one for DHCP, one for Photon Controller, and one for the Lightwave security system—and all of them must have at least 2 NIC cards. NSX itself might require more than 1 ESXi host; see the NSX documentation for memory and other requirements.

ESXi Patch Requirement

This guide assumes that the ESXi hosts are in place with the following attributes. The ESXi host can be either the licensed or the free version.

- It is running VMware ESXi 6.0.0 Patch 201611001 (ESXi600-201611001), which you can find by searching for patches for ESXi 6.0.0 on the My VMware Product Patches web site at https://my.vmware.com/group/vmware/patch. The patch's build number is 4600944.

This guide also assumes that you have root access to all the ESXi hosts, know how to manage them with the vSphere Web Client, and understand basic networking in a virtualized environment. Only minimal instructions are provided for working with ESXi and its web client, which is also known as the VMware ESXi Host Client; if you need help, see the VMware documentation for vSphere and ESXi.

3 NSX Overview

NSX is a software-defined network that runs on a hypervisor to reproduce such networking services as switches, routers, and firewalls. NSX has three planes: management, control, and data. As a system administrator, you manage all the nodes in the NSX system by connecting to the management plane through the API or the user interface. The control plane computes state and disseminates information about the system's configuration and topology. The data plane processes packets according to tables populated by the control plane.

The planes run as software on three kinds of nodes or clusters of nodes: manager, controller, and Edge transport nodes. The manager hosts the API and other services. The controller deploys virtual networks across the NSX architecture. And the *NSX Edge transport node* connects virtual machines to logical switches by routing IP addresses and performing other IP services. On a transport node, NSX creates a hostswitch that binds logical router uplinks and downlinks to physical NICs.

A collection of transport nodes forms a *transport zone*—a fabric of logical switches that connects VMs to hypervisors. In NSX, a transport zone determines the extent of a Layer 2 network. An NSX Edge transport node can belong to one overlay transport zone and one or more VLAN transport zones. The overlay transport zone is for internal NSX tunneling between transport nodes. The VLAN transport zones are for the VLAN uplinks to the external physical network.

3.1 Understanding Fabric Topology

Understanding the relationship between NSX, DHCP, and Photon Controller will help you configure NSX and DHCP.

For Photon Controller, a single overlay transport zone is shared by all Photon Controller cloud hosts as well as the Edge node. The overlay transport zone provides L2 connectivity between VMs through a logical switch.

A single VLAN transport zone is also created. The purpose of this VLAN transport zone is to provide connectivity between the logical network and the external, physical network. The Edge node joins both the overlay transport zone and VLAN transport zone.

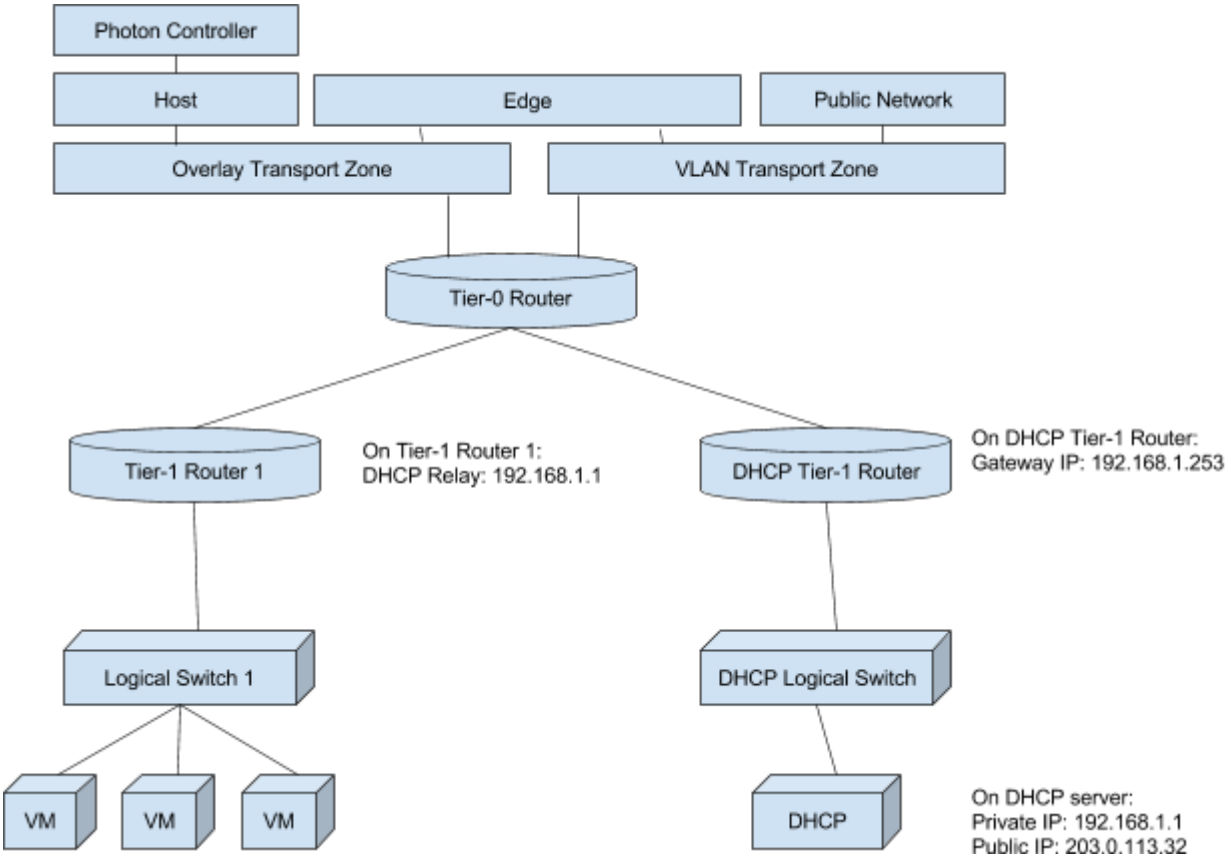
3.2 Virtual Network Topology

You create a single top-tier Tier-0 logical router to provide northbound connectivity with the external network and sounthbound connectivity to Tier-1 routers. It also provides interconnectivity among Tier-1 routers.

For each virtual network, a Tier-1 logical router is created to provide L3 connectivity. In NSX, a Tier-1 router is the second-tier router that, if the network type is ROUTED, connects to the Tier-0 router for northbound connectivity. A logical switch is created for each virtual network as well to provide L2 connectivity. All VMs belonging to the same virtual network are attached to the corresponding logical switch.

A single DHCP server resides in a separate virtual network, which you must set up manually. The DHCP server handles DHCP requests from every virtual network through the DHCP relay service configured on each Tier-1 router of the corresponding network. The DHCP server needs a private IP address as well as a public IP address.

Here's an example of an NSX setup with a virtual network:



A single Tier-0 router is created. It sits between the physical network and the virtual networks. For each *virtual network* created by Photon Controller, a single Tier-1 router and a single logical switch are created, as shown on the left side of the diagram. The Tier-1 router is configured with a private gateway IP address that is facing the VMs. A DHCP relay service is also attached to the gateway port, which points to the private IP address of the DHCP server.

You set up the *dedicated virtual network for DHCP*, shown on the right side of the diagram, manually before deploying Photon Controller.

The DHCP server must have a static private IP address, such as `192.168.1.1`. The private IP address is used by the DHCP relay service attached to the other Tier-1 routers. On the DHCP Tier-1 router, the gateway IP address is, for example, `192.168.1.253` on the gateway port.

The DHCP server must also have a static public IP address, such as 203.0.113.32, as the diagram above illustrates. To obtain a public IP address for the DHCP server, see your network administrator. Photon Controller uses the public IP address to dynamically configure the DHCP server when Photon Controller creates the virtual network.

3.3 IP Addressing and Routing Requirements for Photon Controller

The virtual network topology for Photon Controller carries the following requirements for the NSX virtual network:

Physical router: You must be able to add a static route to a physical router outside the NSX virtual network so that if you choose to set up your Tier-0 router on a different subnet, you and others can access the virtual network. The physical router uses the static route to communicate with the virtual networks created by Photon Controller.

The gateway IP address of the physical network will be used to route all traffic to and from the NSX virtual networks.

The NSX Tier-0 router: You must use a static IP address accessible by the physical network written in CIDR format–for example, 198.51.100.9/24.

The public IP address of the DHCP server should be accessible by Photon Controller.

The private IP address of the DHCP server must not overlap with the IP address pool of Photon Controller; for example, 192.168.1.1 would be a correct IP address.

The IP address pool for Photon Controller must contain only private IP addresses specified in CIDR format. The IP addresses in the pool must not overlap with the private IP address of the DHCP server. For example, because 192.168.1.1 is used by the private IP address of the DHCP server, the private IP address must be something in another range, such as 192.168.2.0/24.

The floating IP address pool for Photon Controller contains public IP addresses. The floating IP addresses will be assigned to VMs so that each VM is publicly accessible.

4 Installation Prerequisites

- Read the NSX Release Notes.
- Read the NSX Installation Guide to understand basic NSX concepts.
- Follow chapter 5 of the NSX Installation Guide to deploy NSX Manager on an ESXi host.
- Follow chapter 6 of the NSX Installation Guide to deploy NSX Controller on an ESXi host.
- Follow chapter 7 of the NSX Installation Guide to deploy NSX Edge on an ESXi host.

Do not proceed with the installation of NSX and its configuration for Photon Platform until you have read the NSX documentation.

5 Download and Install the NSX OVAs

- Download the NSX Manager OVA.
- Download the NSX Controller OVA
- Download the NSX Edge OVA

For help, see the requirements and the instructions in the NSX Installation Guide. If you need additional instructions on how to deploy an OVA on ESXi, see the vSphere documentation.

6 NSX Configuration

After installing the NSX components, you must configure NSX for Photon Controller before deploying Photon Controller. The following steps are required:

- Create a VLAN transport zone.
- Create an overlay transport zone.
- Create an uplink profile.
- Create an IP address pool.
- Configure an Edge transport node.
- Create an Edge cluster.
- Create a Tier-0 router.
- Connect the Tier-0 router to the external network.

You can complete these steps by logging in to your NSX Manager at the following URL:

`https://<ip-address-of-nsx-manager>`

After you complete these steps, you must create a dedicated virtual network in NSX to host the DHCP server, to register the ESXi host running the DHCP server with the NSX fabric, and configure the DHCP server.

6.1 Create a VLAN Transport Zone

Select `Fabric` > `Transport Zones` and click `Add`.

The `Name` can be something like `tz-vlan` and the `Host Switch Name` can be something like `vlan-host-switch`. For `Traffic Type`, select `VLAN`.

See Chapter 9 of the NSX Installation Guide for more on information creating a VLAN transport zone.

6.2 Create an Overlay Transport Zone

Select `Fabric` > `Transport Zones` and click `Add`.

The `Name` can be something like `tz-overlay` and the `Host Switch Name` can be something like `overlay-host-switch`. For `Traffic Type`, select `Overlay`.

See chapter 9 of the NSX Installation Guide for more information creating an overlay transport zone.

6.3 Create an Uplink Profile

The default uplink profile created by NSX defines a stand-by uplink, which is not supported by transport zone uplinks.

To create a new uplink profile, click `Fabric` > `Profiles` > `Uplink Profiles` and click `Add`.

The name can be, for example, `tz-uplink-profile`. For Teaming Policy, select `Failover Order`. For `Active Uplinks`, enter `uplink-1`. For `Transport VLAN`, enter `0`.

6.4 Create an IP Address Pool for Tunnel Endpoints

The IP address pool provides internal IP addresses for NSX tunnel endpoints, that is, the ESXi hosts and the Edge node. Choose an internal IP address range that does not conflict with the IP addresses on the physical network; for example, 192.168.150.100-192.168.150.200.

Select `Inventory` > `Groups` > `IP Pools` and click `Add`.

See Chapter 9 of the NSX Installation Guide for more information about creating an IP address pool.

6.5 Configure an Edge Transport Node

During NSX installation, an Edge entity automatically appears in the NSX Manager web interface after the Edge is joined to the management plain. You can find the Edge entity under `Fabric` > `Nodes` > `Edges`.

To configure the Edge entity as a transport node, select the Edge entity, and then click `Actions` > `Configure as Transport Node`.

For the overlay host switch only, you need to choose the IP address pool that you created for the tunnel endpoints.

You must choose the corresponding vNICs for each virtual NIC. See the NSX Installation Guide on how to choose and set up NSX Edge vNICs.

6.6 Create an Edge Cluster

To create an Edge cluster, click `Fabric` > `Nodes` > `Edge Clusters` > `Add`.

To add the Edge transport node to the cluster, click `Edit`. For `Type`, select `Virtual Machine`, and then move the Edge Transport Node from `Available` to `Selected`.

6.7 Create a Tier-0 Router

To create a Tier-0 router, click `Routing` > `Add` > `Tier-0 Router`. For `High Availability Mode`, select `Active-Active`.

6.8 Connect the Tier-0 Router to the External Network

First, to connect the Tier-0 router to the external network, create a VLAN logical switch that connects to the Tier-0 router.

Click `Switching` > `Switches` > `Add`.

Set the `Admin State` to `Up`, select `None` for the `Switching Profiles Type`, and set the `VLAN` to `0`.

Second, create a new router port on the Tier-0 router that connects to the VLAN logical switch.

Click `Routing` > `Routers`, and then click the Tier-0 router. Click `Configuration` > `Router Ports` > `Add`.

For `Type`, select `Uplink`. For `Transport Node`, select the Edge transport node that you created earlier. For `Logical Switch Port`, select `Attach to new switch port`. For `Switch Port Name`, you can name it something like `vlan-switch-to-tier0-router`. For `IP Address/mask`, the IP address that you enter must be in CIDR notation and must be accessible on the physical network.

Third, create a static route for the IP assigned to the port. Click the Tier-0 router, and then click `Routing` > `Static Routes` > `Add`. Use `0.0.0.0/0` in the network field, and click Insert Row to add the gateway for the next hop.

For information about setting the public IP address and the gateway, see the section above on IP Addressing and Routing Requirements for Photon Controller.

7 DHCP Configuration

To configure the DHCP server, you create a dedicated virtual network in NSX to host the server. You also register the ESXi host running the DHCP server with the NSX fabric.

This section describes how to set up such a network as well as how to configure the DHCP server. Remember from the requirements that the ESXi host containing the DHCP must be dedicated to DHCP; it cannot be reused as a Photon Controller host or as a host for other NSX components.

To set up DHCP, you must do the following:

- Create the DHCP server virtual network.
- Register the ESXi host with the NSX fabric.
- Deploy the DHCP server.

7.1 Create the DHCP Server Virtual Network

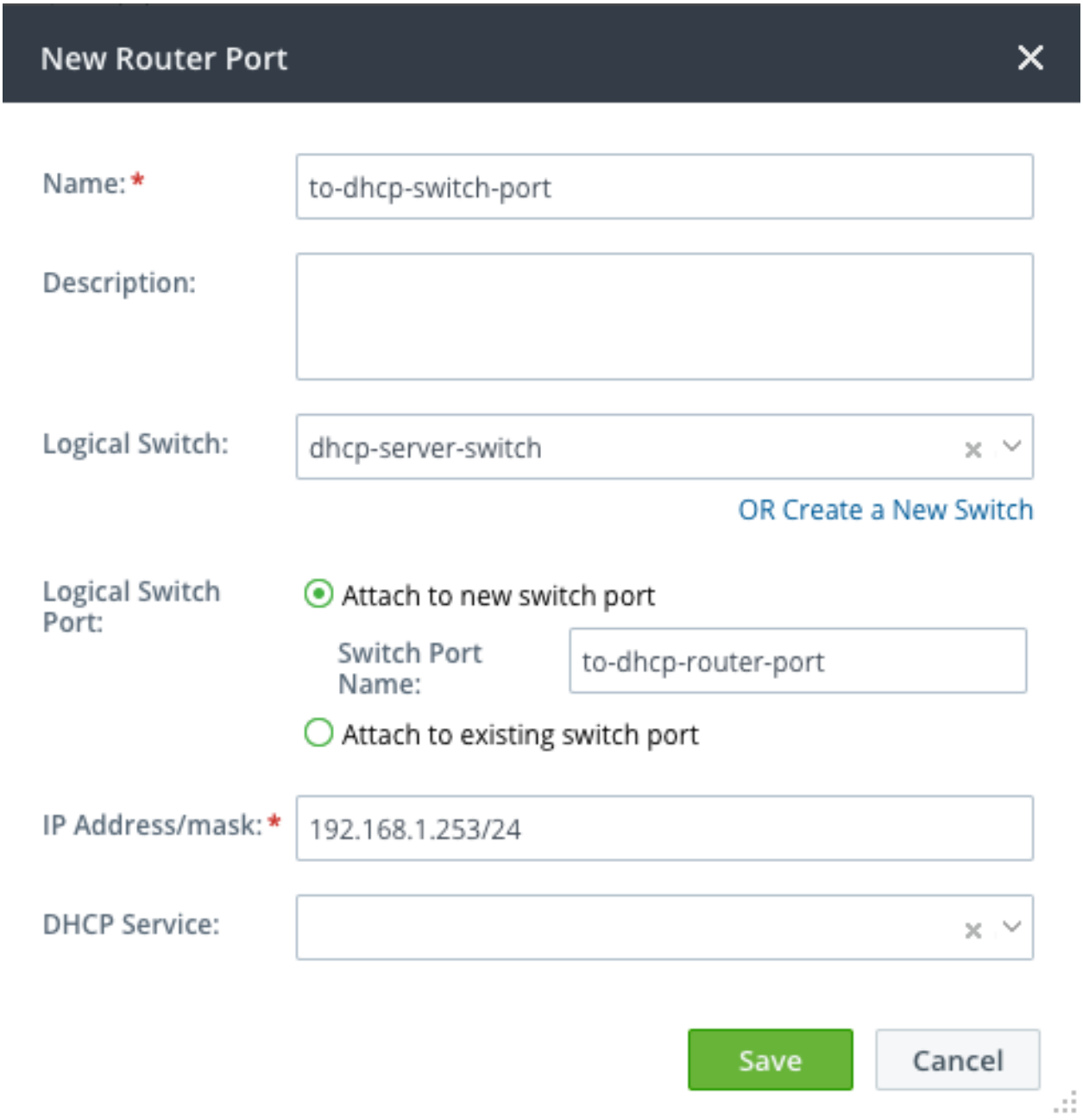
As illustrated in the diagram in the section on virtual network topology, the DHCP server has a dedicated virtual network composed of a Tier-1 router and a logical switch. You must now create these components and connect them with a logical router port.

First, to create a logical switch, click `Switching` > `Switches` > `Add`. For the `Transport Zone`, select the overlay transport zone that you created earlier. For `Admin State`, select `UP`. For `Replication Mode`, select `Hierarchical Two-Tier replication`. Under `Switching Profiles`, use the default profile for each setting.

Second, after creating the logical switch, create a Tier-1 router that connects to the logical switch you created for the DHCP virtual network as well as the Tier-0 router.

Click `Routing` > `Routers` > `Add` > `Tier-1 Router`. You can name it something like `dhcp-server-router` and for the `Edge Cluster`, select the edge cluster that you created earlier.

Third, create a logical router port that connects the Tier-1 router with the logical switch. To do so, click the Tier-1 router, click `Configuration` > `Router Ports` > `Add`. In this example, 192.168.1.253/24 is set as the gateway IP address because the example private IP address of the DHCP server was set to 192.168.1.1. Change the gateway IP address to match your environment. Here's an example:



Finally, enable route advertisement so that other Tier-1 routers can reach the DHCP server:

Click `Routing`, click the Tier-1 router, click `Route Advertisement`, click `Edit`, and enable all settings.

7.2 Register the ESXi Host with the NSX Fabric

To register the ESXi host running the DHCP server with NSX, in the NSX web interface, click `Fabric`, click `Nodes`, and then under the `Hosts` tab, click `Add`. Enter the IP address and the credentials of the ESXi host running the DHCP server.

After you add the host, make sure its deployment status is successful and its LCP connectivity and MPA connectivity are up. Then select the host in the list, click `Actions`, and click `Configure as Transport`

`Node`. For `Transport Zones`, select the overlay transport zone you created earlier. For `Host Switch Name`, select the overlay hostswitch that you created with your overlay transport zone. For the `Uplink Profile`, use the default. For `IP Assignment`, select the IP address pool you created earlier. For the `Physical NICs`, you must select one that is not in use.

7.3 Deploy the DHCP Server

Download the `dhcp-ova.ova` image file from the Photon Controller GitHub downloads page to deploy the DHCP server. By using the vSphere Web Client, deploy the OVA file to the ESXi host that you have set aside for DHCP.

As you deploy the OVA by using the web client, you must make modifications on the `Deployment options` screen and on the `Additional settings` screen.

On the `Deployment options` screen, in the `Network mappings` section, for `PrivateNetwork`, select the name you set for the logical switch for the DHCP server (`dhcp-server-switch` in the example). For `PublicNetwork`, select `dhcp-public-network`. View an example.

On the `Additional settings` screen, under `Options`, add the IP addresses for use by the DHCP server:

- For `Private IP Address`, enter the private IP address that you want to assign to the DHCP server—192.168.1.1 in the examples.
- For `Private Interface Netmask`, enter the netmask for the private IP addressed you are assigning to the DHCP server.
- For `Private Interface Default Gateway`, enter the IP address for the default gateway for the private IP addressed you are assigning to the DHCP server.
- For `Public IP Address`, enter the static public IP address that you want to assign to the DHCP server, such as 203.0.113.32.
- For `Public Interface Netmask`, enter the netmask for the public interface.
- For `Public Interface Default Gateway`, enter the default gateway IP address that the external, physical network is to use to
- For `Root user password`, enter the password that you want to set.
- For the `CIDR of the private IP addresses used by Photon Controller`, enter the IP address pool that you want to assign to Photon Controller. Keep in mind that this IP address pool must contain only private IP addresses specified in CIDR format. The IP addresses in the pool must not overlap with the private IP address of the DHCP server. For example, because 192.168.1.1 is used by the private IP address of the DHCP server, the private IP address must be something in another range, such as 192.168.2.0/24.

View an example.

After the VM powers on, open its console and log in with the root account. The password is the password that you set when you deployed the OVA. Check that the private and public IP addresses by running `ifconfig` on the DHCP server. Then check the gateway IP addresses are set correctly by running `ip route`.

Next, make sure you can ping the gateway IP address of the Tier-0 router. In the example setup in this document, it is 192.168.1.253. If you cannot, go back to the step where you set up the virtual network for your DHCP server and make sure you did it correctly. For instance, make sure that you connected the Tier-1 router to the Tier-0 router and that you enabled route advertisement on the Tier-1 router.

8 Deploy Photon Controller

You need to supply the NSX metadata to the Photon Controller deployment YAML file when the virtual network is enabled. For instructions on how to deploy Photon Controller, see the Photon Controller Quick Start Guide.

Here's an example of the YAML code block for NSX. The value for the `ipaddress` key in the `nsxconfig` section is the IP address of your NSX Network Manager.

```
nsxconfig:
  ipaddress: "203.0.113.220"
  credential:
    username: "admin"
    password: "secret$1"
  privateDHCPIp: "192.168.1.1"
  publicDHCPIp: "203.0.113.223"
  privateIpRootCidr: "192.168.2.0/24"
  floatingIpRootRange: "203.0.113.160-203.0.113.170"
  t0RouterId: "d3b1a8gr-6c58-2062-2562-2drc8977e414"
  edgeClusterId: "55338b48-4r72-38b0-8d4r-65b29084c99a"
  overlayTransportZoneId: "dg821bea-c5r3-34b2-a32g-b02d44726d24"
  tunnelIpPoolId: "b4h8c34d-7714-507c-78g2-ef93b6b2db2a"
  hostUplinkPnic: "vmnic4"
```

8.1 Additional Items to Check Before Installing Photon Platform with NSX

- If ESXi hosts don't use a shared datastore for Photon Controller's image repository, make sure their datastore names are unique.
- Make sure that the hostname of each ESXi host is set and is unique. Check `/etc/hosts` to verify this requirement. If you need to set a hostname, see the documentation for ESXi.
- Make sure each ESXi host has NTP enabled, configured correctly, and working properly. To check, connect to the ESXi host by using SSH and then run the following command: `ntpq -p`

8.2 Example YAML File

Here's a complete example YAML file that installs Photon Platform on an NSX network:

```
compute:
  hypervisors:
    esxi-1:
      hostname: "pc-1"
      ipaddress: "198.51.100.1"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-2:
      hostname: "pc-2"
      ipaddress: "198.51.100.12"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
```

```
    esxi-3:
      hostname: "pc-3"
      ipaddress: "198.51.100.3"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-4:
      hostname: "pc-4"
      ipaddress: "198.51.100.4"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-5:
      hostname: "pc-5"
      ipaddress: "198.51.100.8"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
lightwave:
  domain: "example.com"
  credential:
    username: "administrator"
    password: "Secret123$"
  controllers:
    lightwave-1:
      site: "new york"
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "lightwave-1.example.com"
          ipaddress: "198.51.100.12"
          network: "NAT=VM Network"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          netmask: "255.255.252.0"
          gateway: "198.51.100.253"
    lightwave-2:
      site: "cambridge"
      partner: "198.51.100.13"
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
```

```
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "lightwave-2.example.com"
          ipaddress: "198.51.100.13"
          network: "NAT=VM Network"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          netmask: "255.255.252.0"
          gateway: "198.51.100.253"
photon:
  imagestore:
    img-store-1:
      datastore: "datastore1, datastore2"
      enableimagestoreforvms: "true"
  cloud:
    hostref-1: "esxi-5"
    hostref-2: "esxi-3"
  administrator-group: "example.com\\Administrators"
  syslog:
    ipaddress: "198.51.100.23"
  controllers:
    pc-1:
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "pc-1.example.com"
          ipaddress: "198.51.100.14"
          network: "NAT=VM Network"
          netmask: "255.255.252.0"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          gateway: "198.51.100.253"
    pc-2:
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "pc-2.example.com"
```

```
          ipaddress: "198.51.100.15"
          network: "NAT=VM Network"
          netmask: "255.255.252.0"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          gateway: "198.51.100.253"
dhcp:
  dhcp-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
      credential:
        username: "root"
        password: "Secret1!"
      network-config-private:
        type: "static"
        ipaddress: "198.51.100.16"
        network: "PrivateNetwork=VM Network"
        netmask: "255.255.252.0"
        gateway: "198.51.100.253"
      network-config-public:
        type: "static"
        ipaddress: "198.51.100.16"
        network: "PublicNetwork=Management VLAN"
        netmask: "255.255.252.0"
        gateway: "198.51.100.253"
vsan:
  vsan-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
      credential:
        username: "root"
        password: "Secret1!"
      network-config:
        type: "static"
        hostname: "vsan-1.example.com"
        ipaddress: "198.51.100.20"
        network: "NAT=VM Network"
        netmask: "255.255.252.0"
        dns: "198.51.100.12,198.51.100.13"
        ntp: "203.0.113.1"
        gateway: "198.51.100.253"
loadBalancer:
  load-balancer-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
```

```
      credential:
        username: "root"
        password: "Secret1!"
      network-config:
        type: "static"
        hostname: "lb-1.example.com"
        ipaddress: "198.51.100.21"
        network: "NAT=VM Network"
        netmask: "255.255.252.0"
        dns: "198.51.100.12,198.51.100.13"
        ntp: "203.0.113.1"
        gateway: "198.51.100.253"
nsxconfig:
  ipaddress: "203.0.0.1"
  credential:
    username: "root"
    password: "Secret1!"
  privateDHCPIp: "192.168.1.1"
  publicDHCPIp: "203.0.113.223"
  privateIpRootCidr: "192.168.2.0/24"
  floatingIpRootRange: "203.0.113.160-203.0.113.170"
  t0RouterId: "123"
  edgeCLusterId: "456"
  overlayTransportZoneId: "123"
  tunnelIpPoolId: "123"
  hostUplinkPnic: "vmnic4"
```

After NSX is installed, see the NSX Admin Guide for instructions on how to manage the virtual network.