

# Configure and Troubleshoot a DHCP Server on Cisco IOS XE SDWAN Router

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Network Diagram](#)

[Configurations](#)

[Configure DHCP Server on a Cisco IOS XE SD-WAN Router via vManage Template](#)

[Configure DHCP Server on a Cisco IOS XE SD-WAN Router via CLI](#)

### [Verify](#)

### [Troubleshoot](#)

[Capture DHCP Traffic using Embedded Packet Capture \(EPC\) and vManage Capture Tool](#)

### [Related Information](#)

---

## Introduction

This document describes how to configure and troubleshoot a DHCP Server on a Cisco SD-WAN IOS® XE Router.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Cisco SD-WAN IOS XE Command Line Interface (CLI)
- Packet analyzer
- Basic DHCP

### Components Used

This document is based on these software and hardware versions:

- Router c8000v 17.9.4
- vManage 20.9.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

This section contains an explanation of basic concepts and the process that Dynamic Host Configuration Protocol (DHCP) uses to assign a valid IP address to clients.

<b>Message</b>	<b>Description</b>
<b>DHCP Discover</b>	When a new device joins a network or needs to renew its IP address lease, it sends a DHCP Discover message. This message is typically broadcasted on the local network segment in order to discover the available DHCP servers.
<b>DHCP Offer</b>	DHCP servers on the network receive the DHCP Discover message and respond with a DHCP Offer. In this offer, they propose an available IP address and other network configuration settings to the requesting device.
<b>DHCP Request</b>	The requesting device chooses one of the offered IP addresses and sends a DHCP Request message to the chosen DHCP server. This message confirms the request of the device for the offered IP address and configuration settings.
<b>DHCP Acknowledge</b>	The DHCP server that obtains the DHCP Request message responds with a DHCP Acknowledge (ACK). This ACK acknowledges the request and confirms that the device can use the offered IP address and associated network configuration.
<b>IP Address Assignment</b>	When there is the DHCP ACK, the device configures its network interface with the provided IP address and other configuration parameters. It now has a valid IP address and can communicate on the network.
<b>Lease Duration</b>	The DHCP server assigns a lease duration to the IP address. This lease specifies how long the device can use the IP address. The device must renew the lease before it expires if it wants to keep the same IP address.

<p><b>Lease Renewal</b></p>	<p>Periodically, the device initiates a lease renewal, it sends a DHCP Request to the DHCP server that initially assigned the IP address. If the server approves the renewal, it sends a DHCP ACK, and the lease of the device is extended.</p>
<p><b>Default Lease Time</b></p>	<p>Is the default amount of time that a device is allowed to use its assigned IP address before it must renew it or request an extension to its IP address allocation, this value is 86400 seconds.</p>
<p><b>Lease Expiry</b></p>	<p>If the device does not renew its lease or disconnects from the network, the DHCP server eventually reclaims the leased IP address. This makes the address available for other devices to use.</p>

In summary, DHCP performs a process where a client device broadcasts a request. The DHCP servers respond with offers, the device selects an offer, and the DHCP server acknowledges the request. This is how the assignment of an IP address works. The lease duration ensures that IP addresses are efficiently managed and reclaims them when they are no longer in use.



**Note:** The configuration of Direct Internet Access (DIA) is out of the scope of this document. Refer to [Implement Direct Internet Access \(DIA\) for SD-WAN](#) for configuration guidance.

---



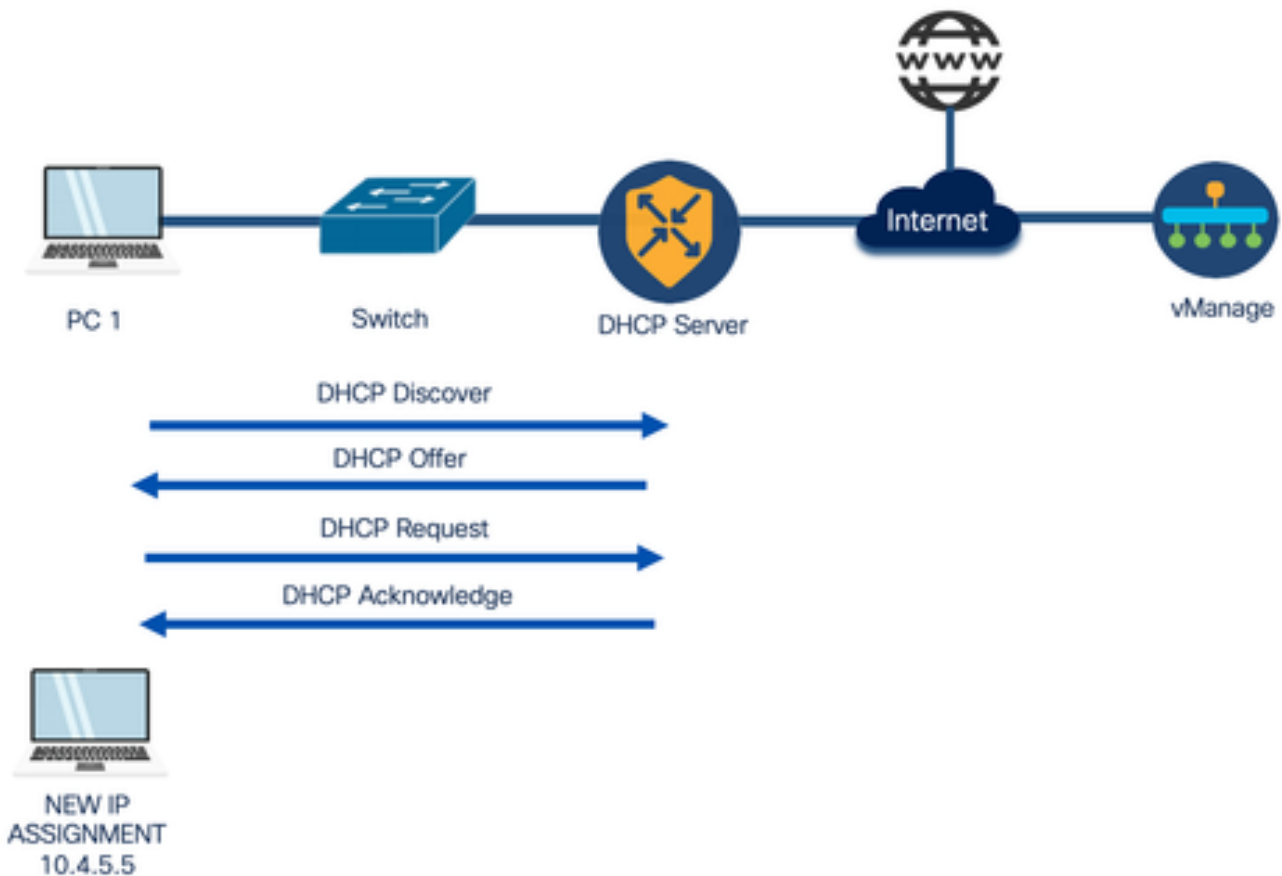
**Note:** If you have a Centralized Policy applied to verify that the DHCP ports are correctly allowed, refer to [DHCP Server Does Not Work on a Router That Runs Cisco IOS-XE SD-WAN with DIA](#).

---

## Configure

One of the most common use cases is when the router acts as a gateway in order to provide internet service to the users in a branch using the DIA feature and then needs to obtain an IP address from a specific network segment given.

## Network Diagram

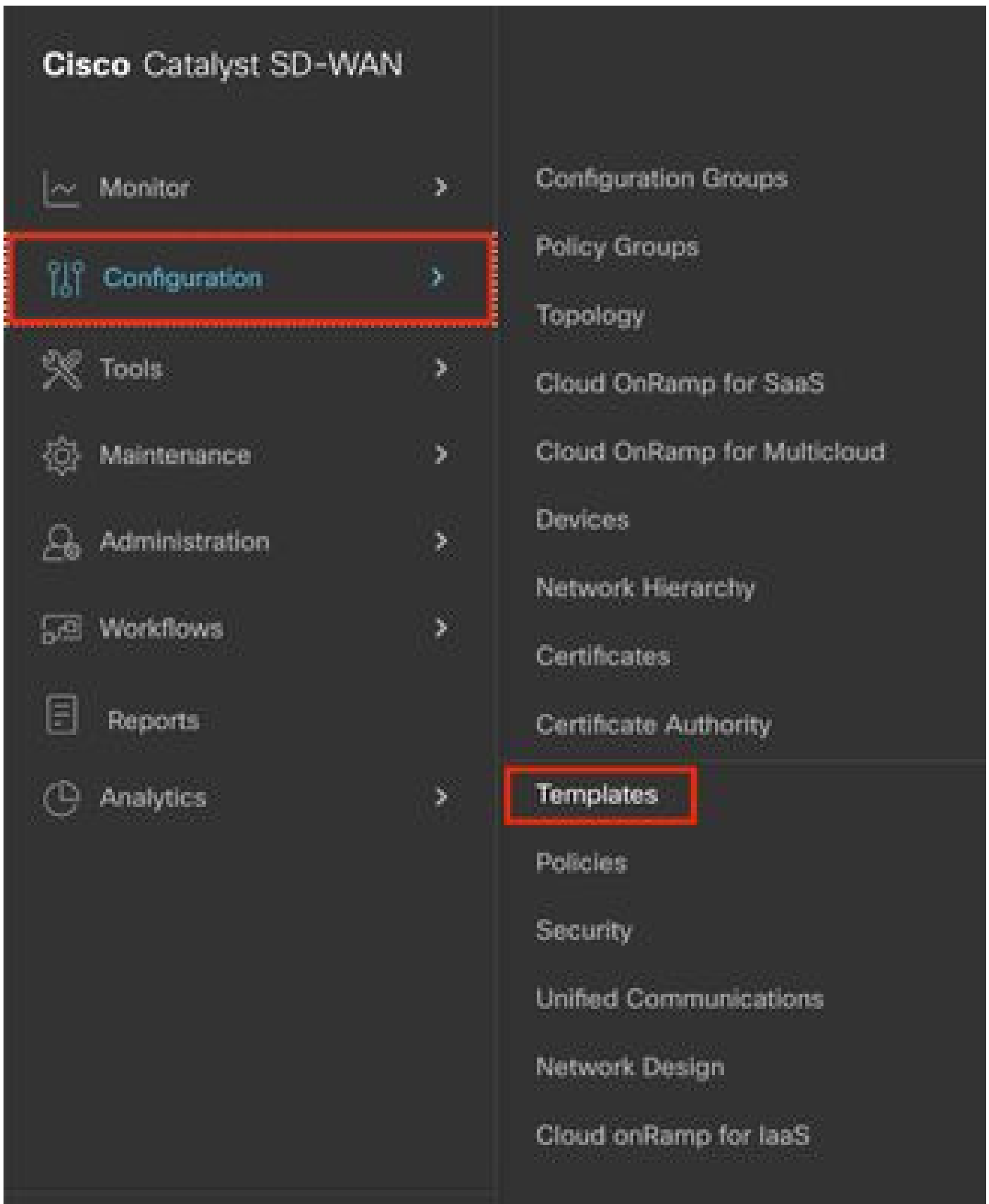


## Configurations

This guide considers that the router has already the onboard configuration on a Cisco vManage with Control Connections formed and already has a device template attached with a service VPN configured. The scope of this document covers the addition of the DHCP configuration in order to provide the dynamic IP assignment.

### Configure DHCP Server on a Cisco IOS XE SD-WAN Router via vManage Template

Step 1. On your vManage, navigate to Configuration > Templates.



Step 2. Navigate to Feature Templates > Add Template and choose the correct model; **C8000v** for this example.

Configuration Groups

Feature Profiles

Device Templates

Feature Templates

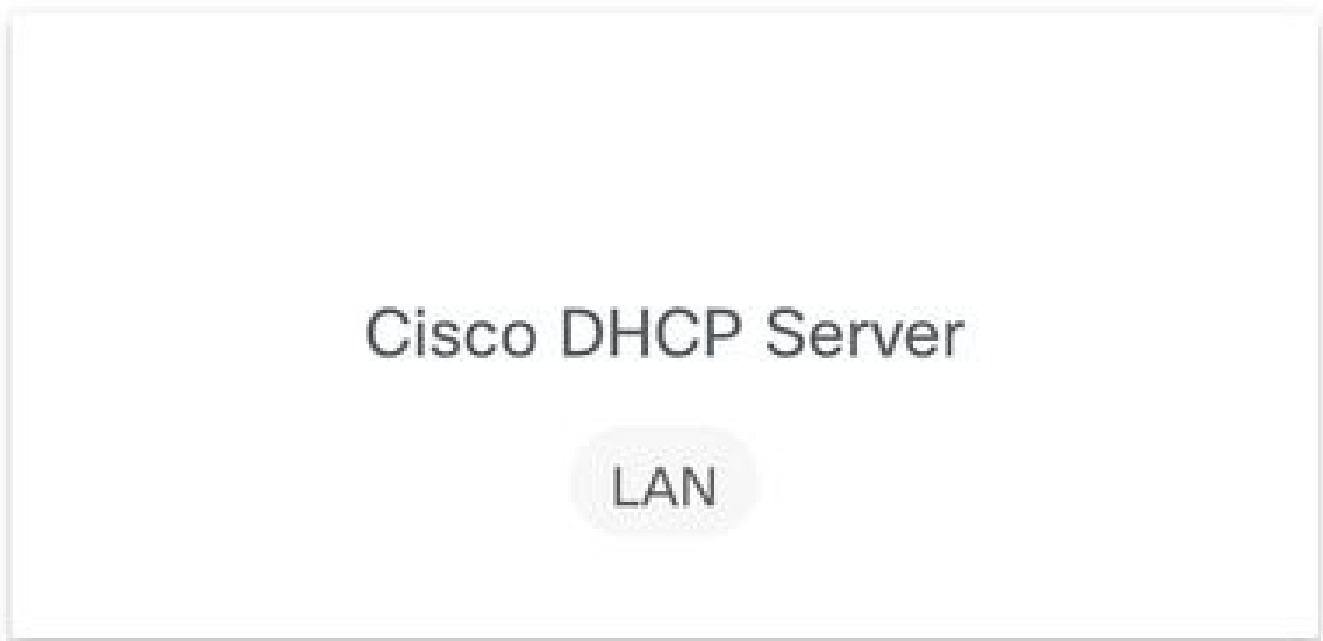
Feature Template &gt; Add Template

Select Devices

C8000v

 C8000v

Step 3. In the other templates, choose Cisco DHCP Server.



Step 4. Add a **Name** and **Description**.

Feature Template &gt; Add Template &gt; Cisco DHCP Server

Device Type C8000v

Template Name\* DHCP\_Server

Description\* DHCP\_Server

Step 5. Configure the DHCP server parameters such as the ones listed here and save changes.



- Address Pool: Pool of assignable addresses.
- Exclude Addresses: Addresses that you do not want to be assigned.
- Lease Time (seconds): Amount of time that this IP address can be leased.
- Default Gateway: The IP address that the DHCP clients perceive as the Default Gateway.

▼ BASIC CONFIGURATION

Address Pool	<input type="text" value="10.4.5.0/24"/>
Exclude Addresses	<input type="text" value="10.4.5.1"/>
Lease Time (seconds)	<input type="text" value="86400"/>

▼ ADVANCED

Interface MTU	<input type="text"/>
Domain Name	<input type="text"/>
Default Gateway	<input type="text" value="10.4.5.1"/>
DNS Servers	<input type="text" value="8.8.8.8"/>
TFTP Servers	<input type="text"/>

Step 6. Navigate to Device Templates, **Edit** the existing Device Template or create a new one and navigate to the Service VPN option.

Device Templates

Feature Templates

Device Model*	CB000v
Device Role*	SDWAN Edge
Template Name*	CB000v_DHCP_Server
Description*	CB000v DHCP Server

Basic Information

Transport &amp; Management VPN

Service VPN

Cellular

Additional Templates

Step 7. Navigate to Add VPN, click Create VPN Template, and add the VPN Service Values.

Configuration Groups

Feature Profiles

Device Templates

Feature Templates

Feature Template &gt; Add Template &gt; Cisco VPN

Device Type	CB000v
Template Name*	CB000v_VPN10
Description*	CB000v_VPN10

Basic Configuration

DNS

Advertise OMP

IPv4 Route

IPv6 Route

Service

Service Route

GRE Route

BASIC CONFIGURATION

VPN	10
Name	
Enhance ECMP Keying	<input type="radio"/> On <input checked="" type="radio"/> Off
OMP Admin Distance IPv4	
OMP Admin Distance IPv6	

Step 8. Add a Cisco VPN Interface Ethernet, from the drop-down list choose Create Template, add the basic values such as the ones listed here, and save the changes.

- Shutdown: Place it in no to turn on the interface.
- Interface Name: Choose the interface to choose as the Default Gateway of the DHCP Clients.
- Description: Description of that interface.
- Dynamic/Static IPv4 Address: Choose the IP address of the Interface.
- IPv4 Address/prefix-length: Choose the IP address and the prefix length.

✓ BASIC CONFIGURATION

Shutdown  Yes  No

Interface Name

Description

IPv4  IPv6

Dynamic  Static

IPv4 Address/ prefix-length

Secondary IP Address (Maximum: 4) [Add](#)

DHCP Helper

Block Non Source IP  Yes  No

Bandwidth Upstream

[Cancel](#) [Save](#)

Step 9. Choose **Sub-Templates** and **Cisco DHCP Server**; from the drop-down list choose the previous template created and click **Add**.

Cisco VPN Interface Ethernet   + Sub-Templates -

Cisco DHCP Server   Cisco DHCP Server

Step 10. Create the template or save the changes and from Device Templates, choose the correct Device Template and choose **Attach Devices**.

Edit

View

Delete

Copy

Enable Draft Mode

Attach Devices

Change Resource Group

Export CSV

Step 11. Choose the correct device and click **Attach**.

## Attach Devices

X

Attach device from the list below

1 Item Selected

Available Devices

All

Name	Device IP
------	-----------



Selected Devices  Select All

All

Name	Device IP
Router	10.10.10.1

Attach

Cancel

Step 12. Add the information requested and click **Next**.

Status	chassis Number	System IP	Hostname	Hostname	System IP	Site ID
	21111-8P88-FGL21889JAB	10.10.10.1	Router	Router	10.10.10.1	10

Next

Cancel

Step 13. Click the device and **Config diff**.

# ☰ Cisco SD-WAN

Device Template  
**C8000V\_DT**

**Total**  
**1**

Device list (Total: 1 devices)

Filter/Search

**C8000V\_DT -FGL214991A9**

Router|10.10.10.1

Config Preview

Config Diff

Step 14. Verify the configuration.

143	<code>ip dhcp excluded-address vrf 10 10.4.5.1</code>
144	<code>ip dhcp pool vrf-10-Vlan10</code>
145	<code>vrf 10</code>
146	<code>lease 1 0 0</code>
147	<code>default-router 10.4.5.1</code>
148	<code>dns-server 8.8.8.8</code>
149	<code>network 10.4.5.0 255.255.255.0</code>
150	<code>exit</code>
151	<code>ip dhcp use hardware-address client-id</code>
152	<code>no ip dhcp use class</code>
153	<code>ip dhcp use vrf remote</code>

Step 15. Click **Configure Devices** and wait for the task to finish.

## Configure Devices

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Template successfully attach...	C1111-8PWE-FGL214991A9	C1111-8PW*	Router	10.10.10.1	10	1.1.1.7

```

[5-Oct-2023 4:03:32 UTC] Configuring device with feature template: C1111-8PW_07
[5-Oct-2023 4:03:32 UTC] Checking and creating device in vManage
[5-Oct-2023 4:03:35 UTC] Generating configuration from template
[5-Oct-2023 4:03:39 UTC] Device is online
[5-Oct-2023 4:03:39 UTC] Updating device configuration in vManage
[5-Oct-2023 4:03:40 UTC] Sending configuration to device

```

## Configure DHCP Server on a Cisco IOS XE SD-WAN Router via CLI

Step 1. Navigate to the configuration mode.

```
<#root>
```

```
cEdge#
```

```
config-transaction
```

```
admin connected from 127.0.0.1 using console on Router
```

```
cEdge(config)#
```

Step 2. Configure the DHCP Pool, assign the values listed here, and save changes.

- Name: Name your DHCP Pool.
- VRF: Add the Service VRF.
- Network: Configure a network with the addresses to be assigned.
- Default-Router: Define the Default Gateway for the DHCP clients.
- DNS-Server: Specify the DNS Server.

```
<#root>
```

```
cEdge(config)#
```

```
ip dhcp pool CISCO
```

```
cEdge(dhcp-config)#
```

```
vrf 40
```

```
cEdge(dhcp-config)#
```

```
network 10.4.5.0 255.255.255.0
```

```
cEdge(dhcp-config)#
```

```
default-router 10.4.5.1
```

```
cEdge(dhcp-config)#
```

```
dns-server 8.8.8.8
```

```
cEdge(dhcp-config)#
```

```
commit
```

Step 3. Configure the Default Gateway IP address of the DHCP clients on the Interface and save changes.

```
<#root>
```

```
cEdge(config)#
```

```
interface GigabitEthernet2
```

```
cEdge(config-if)#
```

```
ip address 10.4.5.1 255.255.255.0
```

```
cEdge(config-if)#
```

```
no shut
```



```
cEdge(config-if)#
```

```
commit
```

## Verify

Verify the information related to the configured pool with the `show ip dhcp pool` command.

```
<#root>
```

```
cEdge#
```

```
show ip dhcp pool CISCO
```

```
Pool CISCO :
```

```
Utilization mark (high/low) : 100 / 0
```

```
Subnet size (first/next) : 0 / 0
```

```
Total addresses : 254
```

```
Leased addresses : 77
```

```
Excluded addresses : 86
```

```
Pending event : none
```

```
1 subnet is currently in the pool :
```

```
Current index IP address range Leased/Excluded/Total
```

```
10.4.5.1 10.4.5.1 - 10.4.5.254 77 / 86 / 254
```

```
cEdge#
```

Verify all the assigned addresses with `show ip dhcp binding` command.

```
<#root>
```

```
cEdge#
```

```
show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
```

```
IP address Client-ID/ Lease expiration Type State Interface
```

```
Hardware address/
```

```
User name
```

```
--- Output omitted ---
```

10.4.5.5 c08f.2073.8a83 Oct 3 2023 06:39 PM Automatic Active GigabitEthernet1

--- Output omitted ---

Verify all the statistics such as counters of messages received and sent, expired leased addresses, and so on with `show ip dhcp server statistics`.

<#root>

cEdge#

`show ip dhcp server statistics`

Memory usage 60892

Address pools 1

Database agents 0

Automatic bindings 78

Manual bindings 0

Expired bindings 0

Malformed messages 0

Secure arp entries 0

Renew messages 0

Workspace timeouts 0

Static routes 0

Relay bindings 0

Relay bindings active 0

Relay bindings terminated 0

Relay bindings selecting 0

Message Received

BOOTREQUEST 0

DHCPDISCOVER 120

DHCPREQUEST 78

DHCPDECLINE 0

DHCPRELEASE 0

DHCPINFORM 0

DHCPVENDOR 0

BOOTREPLY 0

DHCPOFFER 0

DHCPACK 0

DHCPNAK 0

Message Sent

BOOTREPLY 0

DHCPOFFER 78

DHCPACK 78

DHCPNAK 0

Message Forwarded

BOOTREQUEST 0

DHCPDISCOVER 0

DHCPREQUEST 0

DHCPDECLINE 0

DHCPRELEASE 0

DHCPINFORM 0

DHCPVENDOR 0

BOOTREPLY 0

DHCPOFFER 0

DHCPACK 0

DHCPNAK 0

DHCP-DPM Statistics

Offer notifications sent 0

Offer callbacks received 0

Classname requests sent 0

Classname callbacks received 0

cEdge#

Verify the possible conflicts with `show ip dhcp conflicts`.

<#root>

cEdge#

`show ip dhcp conflict`

IP address Detection method Detection time VRF

```
10.4.5.3 Ping Oct 03 2023 06:39 PM
10.4.5.5 Ping Oct 03 2023 06:39 PM
10.4.5.4 Ping Oct 03 2023 06:39 PM
10.4.5.6 Ping Oct 03 2023 06:39 PM
10.4.5.8 Ping Oct 03 2023 06:39 PM
10.4.5.7 Ping Oct 03 2023 06:39 PM
10.4.5.9 Ping Oct 03 2023 06:39 PM
10.4.5.13 Ping Oct 03 2023 06:39 PM
10.4.5.14 Ping Oct 03 2023 06:39 PM
10.4.5.16 Ping Oct 03 2023 06:39 PM
10.4.5.15 Ping Oct 03 2023 06:39 PM
10.4.5.17 Ping Oct 03 2023 06:39 PM
10.4.5.18 Ping Oct 03 2023 06:39 PM
10.4.5.19 Ping Oct 03 2023 06:39 PM
10.4.5.21 Ping Oct 03 2023 06:39 PM
10.4.5.22 Ping Oct 03 2023 06:39 PM
10.4.5.23 Ping Oct 03 2023 06:39 PM
10.4.5.24 Ping Oct 03 2023 06:39 PM
10.4.5.25 Ping Oct 03 2023 06:39 PM
10.4.5.26 Ping Oct 03 2023 06:39 PM
10.4.5.31 Ping Oct 03 2023 06:39 PM
10.4.5.32 Ping Oct 03 2023 06:39 PM
10.4.5.36 Ping Oct 03 2023 06:39 PM
10.4.5.35 Ping Oct 03 2023 06:39 PM
10.4.5.40 Ping Oct 03 2023 06:39 PM
10.4.5.39 Ping Oct 03 2023 06:39 PM
```

Verify the DHCP configuration with `show running-config | section dhcp`.

```
<#root>
```

```
cEdge#
```

```
show running-config | section dhcp
```

```
no ip dhcp use class
ip dhcp pool CISCO
network 10.4.5.0 255.255.255.0
default-router 10.4.5.1
dns-server 8.8.8.8
lease 100
ip route 0.0.0.0 0.0.0.0 dhcp 20
cEdge
```

Verify the state of the interface that acts as a Default Gateway of the DHCP clients with the `show interfaces GigabitEthernet1` command.

```
<#root>
```

```
cEdge#
```

```
show interfaces GigabitEthernet1
```

GigabitEthernet1 is up, line protocol is up

Hardware is vNIC, address is 0050.56b3.6fbb (bia 0050.56b3.6fbb)

Internet address is 10.4.5.1/24

MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Encapsulation ARPA, loopback not set  
Keepalive set (10 sec)  
Full Duplex, 1000Mbps, link type is auto, media type is Virtual  
output flow-control is unsupported, input flow-control is unsupported  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 00:00:00, output 00:00:00, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/375/51623/140000 (size/max/drops/flushes); Total output drops: 1322  
Queueing strategy: fifo  
Output queue: 0/40 (size/max)  
5 minute input rate 1628000 bits/sec, 855 packets/sec  
5 minute output rate 21000 bits/sec, 13 packets/sec  
2868354905 packets input, 657207872035 bytes, 0 no buffer  
Received 0 broadcasts (0 IP multicasts)  
0 runts, 0 giants, 0 throttles  
  
588 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
  
0 watchdog, 0 multicast, 0 pause input  
  
66586780 packets output, 23880813581 bytes, 0 underruns  
  
Output 0 broadcasts (0 IP multicasts)  
0 output errors, 0 collisions, 4 interface resets  
  
1102044 unknown protocol drops  
0 babbles, 0 late collision, 0 deferred  
0 lost carrier, 0 no carrier, 0 pause output  
0 output buffer failures, 0 output buffers swapped out  
cEdge#

## Troubleshoot

Here you can find the messages that must be exchanged between the DHCP server and the DHCP client in order to complete the IP address assignment:

<#root>

\*Oct 3 20:35:48.042:

DHCPD: DHCPDISCOVER received from client c08f.2073.8a83 on interface GigabitEthernet1.

```
*Oct 3 20:35:48.042: DHCPD: Option 125 not present in the msg.
*Oct 3 20:35:48.042: Option 82 not present
*Oct 3 20:35:48.042: Option 82 not present
*Oct 3 20:35:48.042: DHCPD: Option 125 not present in the msg.
*Oct 3 20:35:48.042:
```

DHCPD: Sending notification of DISCOVER:

```
*Oct 3 20:35:48.042: DHCPD: htype 1 chaddr c08f.2073.8a83
*Oct 3 20:35:48.042: DHCPD: remote id 020a0000ac0c025f01000000
*Oct 3 20:35:48.042: DHCPD: interface = GigabitEthernet1
*Oct 3 20:35:48.042:
```

DHCPD: Sending DHCP OFFER to client c08f.2073.8a83 (10.4.5.5).DHCPD: Setting only r

Requested parameters

```
*Oct 3 20:35:48.042: DHCPD: classname not set in msg
*Oct 3 20:35:48.042: DHCPD: Selecting relay q from pool
*Oct 3 20:35:48.042:
```

DHCPD: DHCPREQUEST received from client c08f.2073.8a83.

```
*Oct 3 20:35:48.042:
```

DHCPD: DHCPREQUEST received on interface GigabitEthernet1.

```
*Oct 3 20:35:48.042: DHCPD: Found previous binding
*Oct 3 20:35:48.042: DHCPD: Allocated binding 7F6C1C366788
*Oct 3 20:35:48.042: DHCPD: Adding binding to radix tree (10.4.5.5)
*Oct 3 20:35:48.042: DHCPD: Adding binding to hash tree 7F6C1C366788
*Oct 3 20:35:48.042: DHCPD:dhcpd_binding_add_to_mac_hash: index- 461 add binding 7F6C1C366788
*Oct 3 20:35:48.042: DHCPD: 7F6C1C366788 inserting in mac hash next to 7F6C1C368FC8
*Oct 3 20:35:48.043:
```

DHCPD: assigned IP address 10.4.5.5 to client c08f.2073.8a83.

```
*Oct 3 20:35:48.043: DHCPD: Saving workspace (ID=0xB200004F)
*Oct 3 20:35:48.043: DHCPD: New packet workspace 0x7F6C9CBE0FB8 (ID=0xAE000050)
*Oct 3 20:35:50.043: DHCPD: Reprocessing saved workspace (ID=0xB200004F)
*Oct 3 20:35:50.054:
```

DHCPD: Sending DHCPACK to client c08f.2073.8a83 (10.4.5.5).DHCPD: Setting only req

Requested parameters

These are the debugs that you can activate on the router in order to troubleshoot DHCP issues:

Debug	Description
<b>Debug ip dhcp server events</b>	This command displays DHCP server-related events, such as DHCP client requests, IP address assignments, and other important server activities. It

	is useful to view a summary of DHCP events.
<b>Debug ip dhcp server packet</b>	This command displays detailed information about DHCP packets entering and leaving the server. You can view DHCP requests, offers, requests, and confirmations to debug communication problems.
<b>Debug ip dhcp conflict</b>	If you are having IP address conflict issues on your network, you can use this command to debug and display information about DHCP conflicts.
<b>Debug ip dhcp binding</b>	This command displays information about the IP address assignments made by the DHCP server, including the assigned IP address, the MAC address of the client, and the lease duration.
<b>Debug ip dhcp server statistics</b>	This command displays statistics related to the operation of the DHCP server, such as the number of DHCP requests received, IP address leases, and lease time, among others.
<b>Undebug all</b>	In order to stop all debugging commands, you can use the <code>undebug all</code> command to disable all ongoing debugging.

## Capture DHCP Traffic using Embedded Packet Capture (EPC) and vManage Capture Tool

```
<#root>
```

```
cEdge#
```

```
monitor capture DHCP interface GigabitEthernet 1 both match any buffer circular limit pps 2000
```

```
Interface GigabitEthernet1 direction BOTH is already attached to the capture  
Packets per second limit is already set, replace?[confirm]
```

```
cEdge#
```

```
monitor capture DHCP start
```

```
Started capture point : DHCP
```

```
cEdge#
```

```
--- Wait some time to let DHCP negotiation proceed ---
```

```
cEdge#
```

```
monitor capture DHCP stop
```

```
Stopped capture point : DHCP  
cEdge#
```

Then you can export the capture with this command:

```
<#root>
```

```
cEdge#
```

```
monitor capture DHCP export bootflash:DHCP.pcap
```

```
Exported Successfully  
cEdge#
```

In order to clear the capture, issue this command:

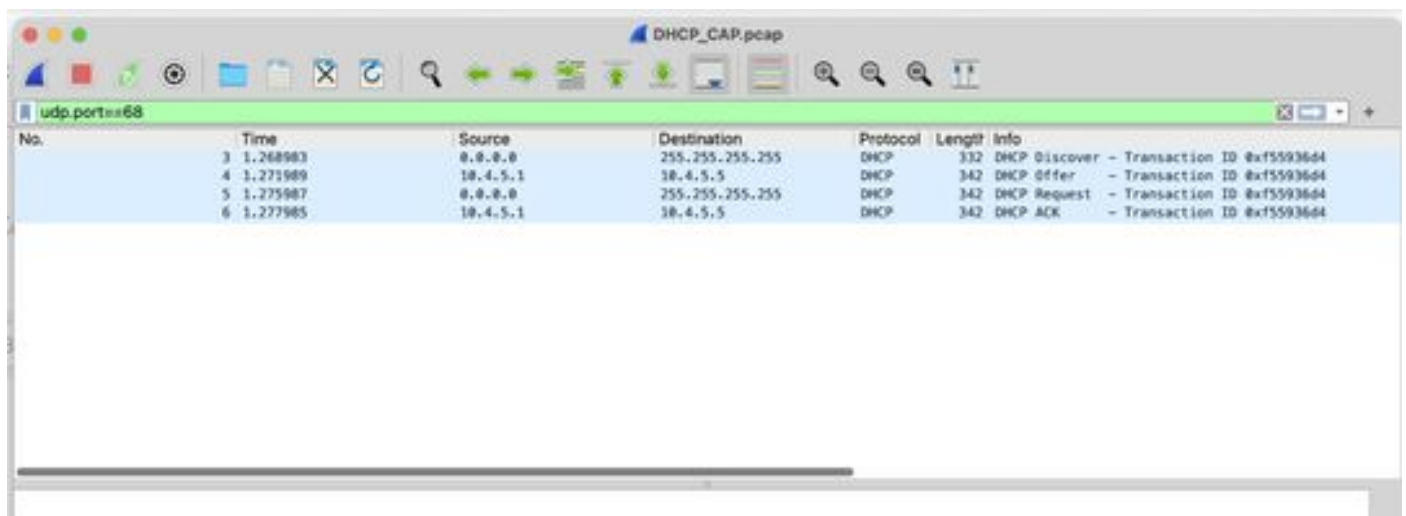
```
<#root>
```

```
cEdge#
```

```
monitor capture DHCP clear
```

```
Captured data is deleted [clear]?[confirm]  
cleared buffer : DHCP  
cEdge#
```

Then with WireShark, verify that you see these packets involved in the negotiation:



The screenshot shows the Wireshark interface with a capture filter of 'udp.port==68'. The packet list pane displays four DHCP packets:

No.	Time	Source	Destination	Protocol	Length	Info
3	1.268983	0.0.0.0	255.255.255.255	DHCP	332	DHCP Discover - Transaction ID 8xf55936d4
4	1.271989	10.4.5.1	10.4.5.5	DHCP	342	DHCP Offer - Transaction ID 8xf55936d4
5	1.275987	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 8xf55936d4
6	1.277985	10.4.5.1	10.4.5.5	DHCP	342	DHCP ACK - Transaction ID 8xf55936d4

You must see this information when you open the packets:

**Discover packet**



- The most important information that you must verify is the source MAC Address; this must match with the MAC of the DHCP Client.
- The destination is ff:ff:ff:ff:ff:ff because it is a broadcast address; the DHCP client sends this message to discover the DHCP Server.
- The source IP Address is set as 0.0.0.0.
- The ports used for this negotiation are the UDP 67 and 68.
- You can see the options that the packet contains; this is about the information requested by the DHCP Server on the packet.

```

Frame 3: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 4, 2023 01:09:27.284973000 (ST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1696403367.284973000 seconds
  [Time delta from previous captured frame: 0.289038000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 1.260903000 seconds]
  Frame Number: 3
  Frame Length: 332 bytes (2656 bits)
  Capture Length: 332 bytes (2656 bits)
  [Frame is marked: false]
  [Frame is ignored: false]
  [Protocols in frame: eth:ethertype:ip:udp:dhcp]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
  Ethernet II, Src: Shenzhen 73:8a:83 (c0:8f:20:73:8a:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: Shenzhen 73:8a:83 (c0:8f:20:73:8a:83)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 298
    Checksum: 0xb5b8 (unverified)

```

## Dynamic Host Configuration Protocol (Discover)

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xf55936d4
Seconds elapsed: 3
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Shenzhen_73:8a:83 (c0:8f:20:73:8a:83)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (61) Client identifier
> Option: (57) Maximum DHCP Message Size
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (80) Rapid commit
> Option: (255) End
```

## Offer packet

- Now you can see that the Source Address is different as the DHCP Server is known with the IP address 10.4.5.1.
- The Destination IP Address is known as 10.4.5.5 because this address is one of the available addresses on the pool.

```

Internet Protocol Version 4, Src: 10.4.5.1, Dst: 10.4.5.5
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 328
  Identification: 0x004b (75)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x9c4c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.4.5.1
  Destination Address: 10.4.5.5
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0x9c76 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  UDP payload (308 bytes)
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf55936d4
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.4.5.5
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Shenzhen_73:8a:83 (c0:8f:20:73:8a:83)
  Client hardware address padding: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DMCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (61) Client Identifier
  > Option: (54) DHCP Server Identifier (10.4.5.1)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (255) End
  Padding: 0000000000

```

## Request packet

On the request packet, the source address is seen as 0.0.0.0 and now the 10.4.5.5 address is the new request.

```
our payload (300 bytes)
  Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x81)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf55936d4
    Seconds elapsed: 3
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Shenzhen_73:8a:83 (c0:8f:20:73:8a:83)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.4.5.5)
    Length: 4
    Requested IP Address: 10.4.5.5
  > Option: (54) DHCP Server Identifier (10.4.5.1)
  > Option: (57) Maximum DHCP Message Size
  > Option: (60) Vendor class identifier
```

## ACK packet

- The source address is set as 10.4.5.1.
- The destination address is set as 10.4.5.5 because this is now the new IP address of the DHCP client.

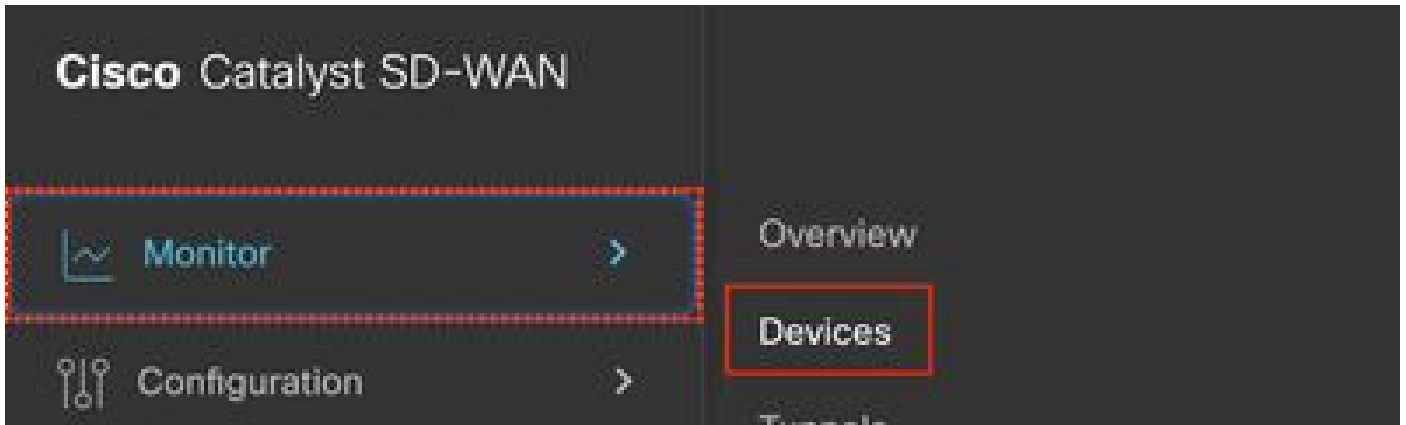
```

Internet Protocol Version 4, Src: 10.4.5.1, Dst: 10.4.5.5
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 328
  Identification: 0x004c (76)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x9c4b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.4.5.1
  Destination Address: 10.4.5.5
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0x96bb [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  UDP payload (308 bytes)
Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf55936d4
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.4.5.5
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Shenzhen_73:8a:83 (c0:8f:20:73:8a:83)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
  > Option: (61) Client identifier

```

The Packet Capture can be taken on the vManage GUI with these steps:

Step 1. Navigate to Monitor > Devices.



Step 2. Click the DHCP server device.

A screenshot of the Cisco Catalyst SD-WAN interface showing a search bar with "cEdge-02" entered. Below the search bar, there is a table of devices. The table has columns for Hostname, Device Model, Site Name, System IP, Health, Reachability, vSmart Control, BFD, TLDC, Up Since, CPU Load, and Actions. The first row of data shows a device named "cEdge-02" with a model of "CSR1000v", site name "SITE\_102", system IP "1.1.30.20", and a CPU load of 13.44%.

Step 3. On Security Monitoring, click Troubleshooting.

## **SECURITY MONITORING**

**Firewall**

**Intrusion Prevention**

**URL Filtering**

**Advanced Malware Protection**

**TLS/SSL Decryption**

**Umbrella DNS Re-direct**

---

**Control Connections**

---

**System Status**

---

**Events**

---