



# ADTRAN Switch Engine (ASE) Dynamic Host Configuration Protocol

Configuration Guide

6AMCCG0006-29B

May 2020



## To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

## Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

## Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.



Copyright © 2020 ADTRAN, Inc.  
All Rights Reserved.

## Revision History

Rev A	May 2019	Initial release
Rev B	May 2020	Updated format and revised supported hardware section.

# Table of Contents

<b>Overview</b> .....	<b>5</b>
Understanding DHCP .....	5
The DHCP Request Process .....	6
<b>Hardware and Software Requirements and Limitations</b> .....	<b>6</b>
<b>DHCP Configuration Overview</b> .....	<b>7</b>
Excluding IP Addresses from the DHCP Server Address Pool .....	7
DHCP Address Pool .....	7
IP Addresses to Exclude from the DHCP Server Address Pool .....	8
DHCP Relay .....	8
<b>Configuring DHCP Using the GUI</b> .....	<b>8</b>
Configure the DHCP VLAN and Enable the DHCP Server .....	8
Create a DHCP Server Address Pool for the Network .....	10
Specify an IP Address Range to Exclude from the DHCP Server Address Pool .....	11
DHCP Relay .....	12
<b>Configuring DHCP Using the CLI</b> .....	<b>13</b>
Enable the DHCP Server and Configure the Associated VLAN Interface .....	13
Associate Ports with the DHCP VLAN .....	13
Create a DHCP Server Address Pool for the Network .....	14
Specify an IP Address Range to Exclude from the DHCP Server Address Pool .....	14
DHCP Relay .....	15
<b>Troubleshooting</b> .....	<b>15</b>
Verify the DHCP Server is Configured Correctly .....	15
Verify that the VLAN Interface Status is UP .....	17
Verify that the DHCP Pool and Layer 3 VLAN Interface are in the Same Subnet .....	17
Verify the VLAN of the Port for the DHCP Device .....	18
Verify that the ASE Device is Seeing DHCP Messages .....	19
Verify that there is not an ACL blocking DHCP .....	20
Further Analysis Using Packet Capture .....	20
<b>Warranty and Contact Information</b> .....	<b>21</b>
Warranty .....	21
Contact Information .....	21

## 1. Overview

This document explains how to configure IPv4 Dynamic Host Configuration Protocol (DHCP) server IP address pools using the web-based Graphical User Interface (GUI) and the Command Line Interface (CLI). The examples used in this document pertain to ADTRAN Switch Engine (ASE) products.



### NOTE

*This document does not cover DHCP over IPv6.*

## Understanding DHCP

DHCP provides a framework for passing configuration information to hosts on IP networks. The protocol is based on the Bootstrap protocol (BOOTP), but also includes the capability to automatically allocate reusable network addresses and additional configuration options. DHCP is used to simplify network administration. Every computer that connects to the Internet or an IP network needs an IP address. It is not nearly as difficult to manually assign IP addressing information to every PC in a small network. However, as systems become larger and more complex, and mobile users are added to the mix, it becomes increasingly difficult to manage and keep track of IP assignments. DHCP allows you to assign a range or subnet of addresses to a DHCP server which it will dynamically distribute and maintain.

DHCP is a client-server model, where the DHCP client is the IP device that obtains configuration parameters (such as network addresses) and the DHCP server is the IP device that allocates network addresses and configuration parameters to the client. The DHCP server is responsible for providing network configuration information to the client, including the IP address to be used, the corresponding gateway address, the Domain Name Service (DNS) server address, and the Network Time Protocol (NTP) server address. [Figure 1](#) shows the usage of DHCP in a typical network deployment.

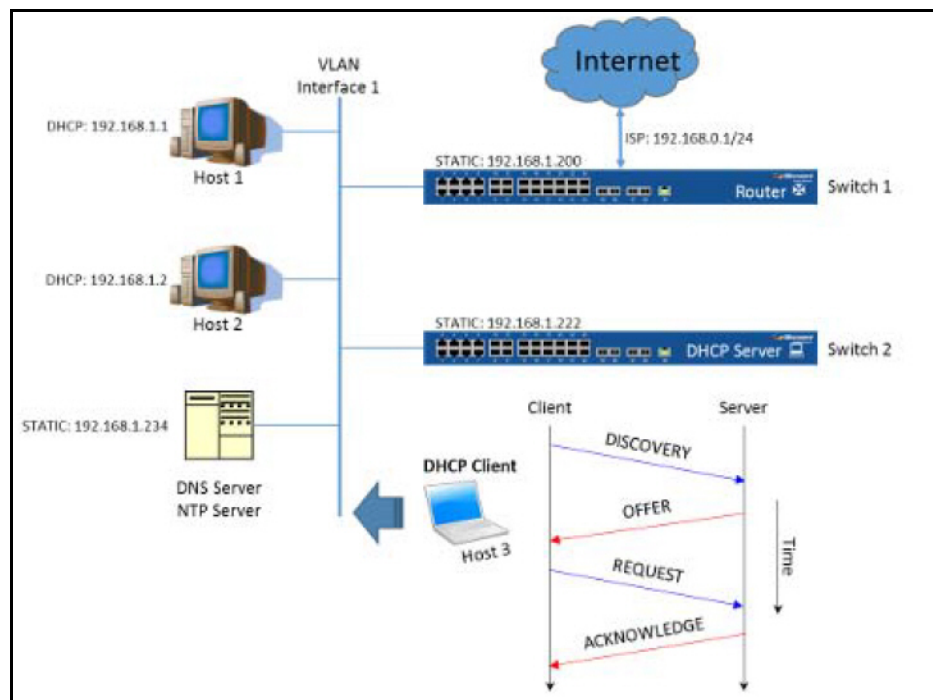


Figure 1. DHCP Deployment in a Typical Network

As shown in [Figure 1](#), IP subnet 192.168.1.0/24 is running on the virtual local area network (VLAN) named VLAN 1, and the switch devices are configured to be both routers and DHCP servers. To provide additional services, such as name resolution and time synchronization, another desktop server is configured to support DNS and NTP services simultaneously. DHCP is used to complete the rest of the configuration for the connected IP hosts. For example, when Host 1 is online, the network administrator only needs to connect it with the VLAN Interface 1 on either Switch 1 or Switch 2. The IP address (192.168.1.1/24), the default router address (192.168.1.200), DNS server address (192.168.1.234), and even NTP server address (192.168.1.234) are automatically assigned simultaneously.

## The DHCP Request Process

Referring to [Figure 1](#), when a new DHCP Client (Host 3) connects to this network, the DHCP Server (Switch 2) responds with the pre-configured network parameters that the host should apply. The DHCP process can be broken down into four steps:

1. Host 3 broadcasts a DISCOVERY packet, requesting an IP address and other configurations.
2. Switch 2 responds with an OFFER, which includes an available network address.
3. Host 3 sends a REQUEST, accepting the offer and requesting the complete configuration from Switch 2.
4. Switch 2 responds with a ACKNOWLEDGE, which includes the following:
  - The agreed-upon network address
  - A default gateway
  - A lease time
  - The address of one or more DNS servers (optional)
  - The address of one or more Window Internet Name Service (WINS) servers (optional)

When DHCP message exchanges are complete, the client is able to access the Internet, and is also aware of available network services (for example, DNS and NTP).

## 2. Hardware and Software Requirements and Limitations

DHCP and its related options are supported on ASE products outlined in [Table 1](#) that are running ASE firmware 4.4-49 or later.

**Table 1. Supported Products**

Product	P/N
NetVanta 1560-08-150W Switch	17108108PF2
NetVanta 1560-24-740W Switch	17108124PF2
NetVanta 1560-48-740W Switch	17108148PF2
NetVanta 1560-08-65W Switch	17101561PF2
NetVanta 1560-24-370W Switch	17101564PF2
NetVanta 1560-48-370W Switch	17101568PF2

### 3. DHCP Configuration Overview

The DHCP server is disabled by default on ASE products. Therefore, to provide IP address allocation services, you must enable the DHCP server and associate it with the applicable VLAN interface. Next, specify any static IP addresses that should be excluded from the DHCP pool. Finally, configure a DHCP address pool for providing connected hosts with the needed IP network settings.

DHCP Relay is an option that can be configured on an ASE device that allows DHCP clients to receive dynamic addresses from a server on a remote network.

#### Excluding IP Addresses from the DHCP Server Address Pool

Often, there are servers or routers that must be configured with a static IP address. The IP addresses of these devices must not conflict with any other IP addresses in the same subnet. Therefore, these addresses must be excluded from the DHCP pool so that they are not assigned to other devices.

#### DHCP Address Pool

There are two types of DHCP address pools:

- **Network Pool:** Defined to provide IP addresses for more than one DHCP client. The allocated addresses are network addresses (for example, **1.2.3.0/24**).
- **Host Pool:** Used to provide an address to a specific DHCP client identified by either a client identifier (a specific string) or a hardware address (a specific media access control (MAC) address). The allocated addresses are host addresses (for example, **1.2.3.4/32**).

Regardless of the type of DHCP address pool that is used, an expiration time for each allocated address (lease time) is supplied.

Additional configurable DHCP address pool attributes are listed below.

**Table 2. Configurable DHCP Address Pool Attributes**

DHCP Option	Description
<b>broadcast</b>	Broadcast address in use on the client's subnet
<b>client-identifier</b>	Client identifier used in DHCP message exchange
<b>client-name</b>	Host name to be assigned for a client
<b>default-router</b>	Default routers
<b>dns-server</b>	DNS servers
<b>domain-name</b>	Domain name to be used as a DNS search suffix
<b>hardware-address</b>	Client's hardware address
<b>netbios-name-server</b>	NetBIOS (WINS) name servers
<b>netbios-node-type</b>	NetBIOS node type
<b>netbios-scope</b>	NetBIOS scope
<b>nis-domain-name</b>	Network Information System (NIS) domain name
<b>nis-server</b>	NIS servers
<b>vendor</b>	Vendor configurations

**NOTE**

The **default-router** option should be configured for every host as a gateway to access the Internet.

## IP Addresses to Exclude from the DHCP Server Address Pool

In any IP subnet, there will be IP servers or routers configured manually to provide services. Their IP addresses are not allowed to conflict with any other IP addresses in the same IP subnet, in order to guarantee IP connectivity and service. For this purpose, the DHCP server has to exclude these static IP addresses from its address pool.

IP addresses that should be excluded from the DHCP server address pool include IP addresses of the local interfaces of a device and any known gateway addresses.

## DHCP Relay

DHCP relies on clients being able to reach a server by broadcasting a request. The DHCP request is limited by being broadcast to the application port for DHCP (the BOOTPS port, 67). Limited broadcasts propagate only throughout the local subnet. If the client is not on the same subnet as the server, the broadcast will not reach the server.

If you want clients to receive dynamic addresses from a server on a remote network, you must configure DHCP relay on the ASE device. To enable DHCP relay, you configure the switch to forward packets received on the DHCP application port to a helper address.

## 4. Configuring DHCP Using the GUI

To configure DHCP, connect to the ASE GUI and complete the following tasks:

- [Configure the DHCP VLAN and Enable the DHCP Server on page 8](#)
- [Create a DHCP Server Address Pool for the Network on page 10](#)
- [Specify an IP Address Range to Exclude from the DHCP Server Address Pool on page 11](#)

Optionally, you can configure DHCP Relay and Option 82:

- [DHCP Relay on page 12](#)

### Configure the DHCP VLAN and Enable the DHCP Server

Begin configuring DHCP in the ASE device by creating the DHCP VLAN and assigning it to the ports that will be using it. Then, enable the DHCP server and VLAN.



1. Navigate to **Configuration > VLANs > Configuration** to create the VLAN as shown below. Enter the VLAN number beside **Allowed Access VLANs**. Assign the DCHP VLAN to ports by entering the VLAN number in the **Port VLAN** field beside each of the port numbers that will use this VLAN. Select **Save**.

Global VLAN Configuration

Allowed Access VLANs: 1, 10  
 Ethertype for Custom S-ports: 88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	10	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	10	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

2. Configure the Layer 3 VLAN Interface. The IP address assigned to this interface should be in the same subnet as the DHCP Pool. Navigate to **Configuration > System > IP** and select **Add Interface** under IP Interfaces as shown below. Enter the VLAN number, the IPv4 IP Address and Mask Length. Select **Save**.

IP Interfaces

Delete	VLAN	Enable	DHCPv4				Hostname	Fallback	Current Lease	IPv4	
			Type	IfMac	ASCII	HEX				Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	Auto	Port 1				0		10.19.14.66	24
<input type="checkbox"/>	10	<input type="checkbox"/>	Auto	Port 1				0		192.168.1.1	24

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Distance(IPv4) / Next Hop VLAN(IPv6)
<input type="checkbox"/>	0.0.0.0	0	10.19.14.254	1

Add Route

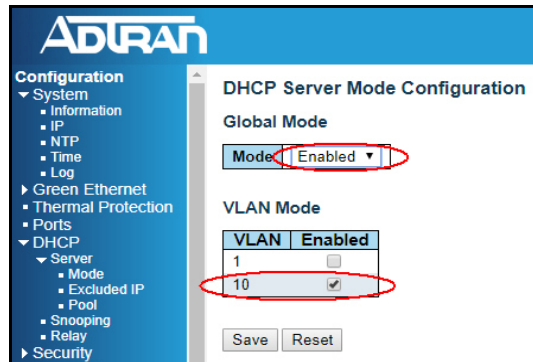
Save Reset



**NOTE**

*If this switch is the default route of the new VLAN, ensure this default route has been added to the route table.*

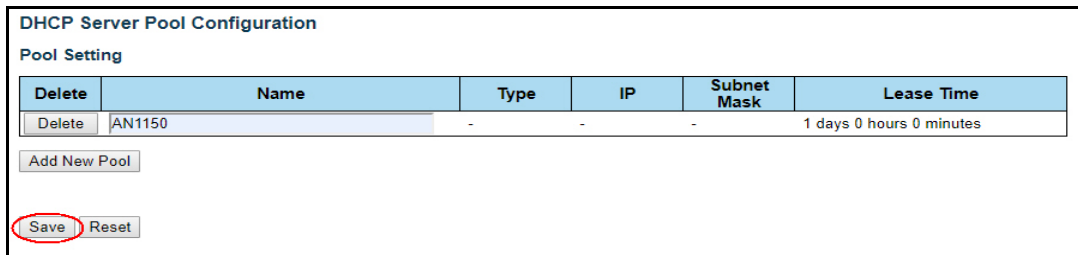
3. Activate the DHCP server and configure its associated IP VLAN interface. Navigate to **Configuration > DHCP > Server > Mode**, and select **Enabled** next to Mode to globally enable the DHCP server. Select the check box under Enabled next to the DHCP VLAN you created in Step 2 and select **Save**.



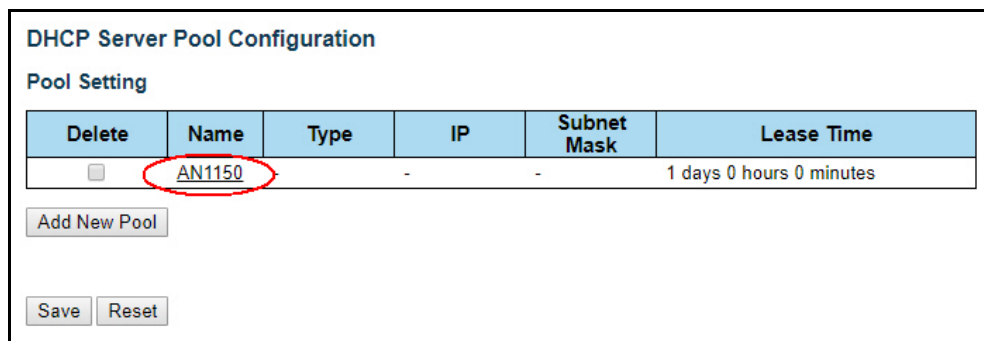
### Create a DHCP Server Address Pool for the Network

Create a DHCP server address pool on the device, and then specify the IP address(es) to be allocated in order to provide the IP hosts connected to the VLAN interface with automatic network configuration parameters. For example, to create the DHCP address pool **AN1150** to allocate the IP address **192.168.1.0/24**, perform the following steps:

1. Navigate to **Configuration > DHCP > Server > Pool**, and select **Add New Pool**. Enter the DHCP address pool name in the **Name** field.



2. Select **Save**.
3. Enter the pool setting configuration menu by selecting the hyper-linked name **AN1150** in the **Name** field as shown below.



4. Enter the DHCP address pool parameters as shown below.

### DHCP Pool Configuration

**Pool**

Name

**Setting**

Pool Name	AN1150
Type	Network
IP	192.168.1.0
Subnet Mask	255.255.255.0
Lease Time	<input type="text" value="1"/> days (0-365) <input type="text" value="0"/> hours (0-23) <input type="text" value="0"/> minutes (0-59)
Domain Name	my.net
Broadcast Address	192.168.1.255
Default Router	192.168.1.200 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	192.168.1.234 8.8.8.8 0.0.0.0 0.0.0.0
NTP Server	192.168.1.235 0.0.0.0 0.0.0.0 0.0.0.0

**NOTE**

---

*It is usually practical to assign multiple (DNS/NTP) servers for reference.*

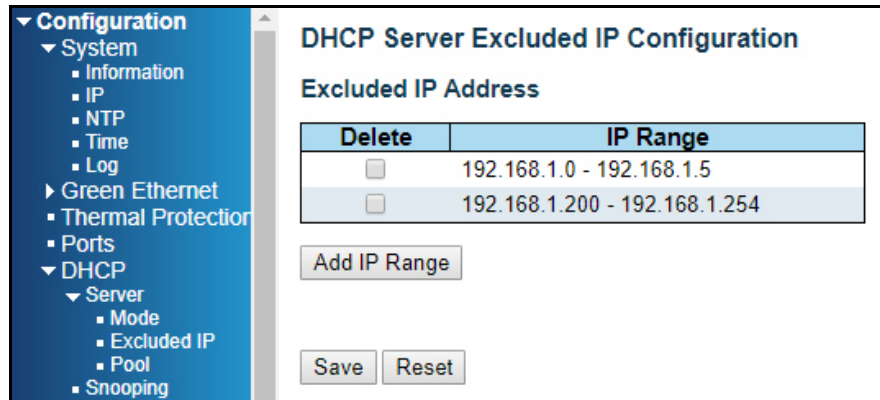
5. Select **Save**.

## Specify an IP Address Range to Exclude from the DHCP Server Address Pool

Specifying an IP address range to exclude from the DHCP server address pool allows the DHCP server to refrain from allocating the IP addresses in this range to DHCP client(s). Router and server IP addresses should typically be excluded from the DHCP server address pool.

To exclude IP addresses in a range from the DHCP server address pool, for example, from **192.168.1.0** to **192.168.1.5** and **192.168.1.200** to **192.168.1.254**, perform the following steps:

1. Navigate to **Configuration > DHCP > Server > Excluded IP**, and select **Add IP Range**. Specify the IP address range parameters as shown below.



2. Select **Save** to add the listed IP address range to those addresses excluded from the DHCP server address pool.

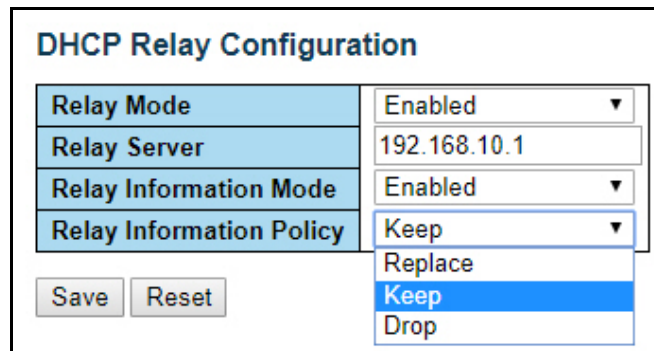
**i** **NOTE**

*The first address in the range must be a lower IP address than (or equal to) the second IP address in the range.*

## DHCP Relay

To configure DHCP relay via the GUI, you must enable relay mode and specify the IP Helper Address. The IP Helper address is the unicast address of the DHCP relay server or a device on the same subnet as the server.

For example, to configure DHCP relay with an IP Helper address of 192.168.10.1, navigate to **Configuration > DHCP > Relay** and select **Enabled** next to *Relay Mode*. Enter **192.168.10.1** next to *Relay Server*.



## Option 82

If DHCP Relay is enabled, you can also choose to enable DHCP Relay Information mode (Option 82). Option 82 adds a layer of security to DHCP by preventing DHCP client requests from untrusted devices. To enable DHCP Option 82, select **Enabled** next to *Relay Information Mode*. Then select **Replace**, **Keep**, or **Drop** to choose the policy of Option 82 when a received packet already contains DHCP relay information. Select **Save**.

## 5. Configuring DHCP Using the CLI

To configure DHCP, connect to the ASE GUI and complete the following tasks:

- [Enable the DHCP Server and Configure the Associated VLAN Interface on page 13](#)
- [Associate Ports with the DHCP VLAN on page 13](#)
- [Create a DHCP Server Address Pool for the Network on page 14](#)
- [Specify an IP Address Range to Exclude from the DHCP Server Address Pool on page 14](#)

Optionally, you can configure DHCP Relay and Option 82:

- [DHCP Relay on page 15](#)

### Enable the DHCP Server and Configure the Associated VLAN Interface

Begin configuring DHCP in the ASE device by activating the DHCP server and configuring its associated IP VLAN interface.

```
#configure terminal
```

! Enable DHCP Server.

```
(config)#ip dhcp server
```

! Create the DHCP VLAN

```
(config)#vlan 10
```

! Associate VLAN Interface 10 with the DHCP Server.

```
(config)#interface vlan 10  
(config-if-vlan)#ip dhcp server
```

! Configure the VLAN IP Address

```
(config-if-vlan)#ip address 192.168.1.1 255.255.255.0  
(config-if-vlan)#end
```



#### NOTE

*The Layer 3 interface on the VLAN must be in the same subnet as the DHCP Pool.*

### Associate Ports with the DHCP VLAN

Ports that will be using the DHCP VLAN must be associated with the VLAN number you created for DHCP. The following example associates Port 2 with VLAN 10. Repeat this step for each individual interface you want to assign to the DHCP VLAN.

! Associate Port 2 with VLAN 10.

```
(config)#interface gigabitethernet 1/2  
(config-if)#switchport access vlan 10  
(config-if)#end
```

## Create a DHCP Server Address Pool for the Network

Create a DHCP server address pool on the device, and then specify the IP address(es) to be allocated in order to provide the IP hosts connected to the VLAN interface with automatic network configuration parameters. For example, to create the DHCP address pool **AN1150** to allocate the IP address **192.168.1.0/24**, perform the following steps:

```
#configure terminal
```

! Create and enter the pool configuration sub mode.

```
(config)#ip dhcp pool AN1150
```

! Set up 'Network' type and its network address allocation.

```
(config-dhcp-pool)#network 192.168.1.0 255.255.255.0
```

! Set up the lease time.

```
(config-dhcp-pool)#lease 1 0 0
```

! Set up the default gateway.

```
(config-dhcp-pool)#default-router 192.168.1.200
```

! Set up additional options.

```
(config-dhcp-pool)#broadcast 192.168.1.255
```

```
(config-dhcp-pool)#domain-name my.net
```

```
(config-dhcp-pool)#dns-server 192.168.1.234 8.8.8.8
```

```
(config-dhcp-pool)#ntp-server 192.168.1.234 129.6.15.28
```

```
(config-dhcp-pool)#end
```

## Specify an IP Address Range to Exclude from the DHCP Server Address Pool

Specifying an IP address range to exclude from the DHCP server address pool allows the DHCP server to refrain from allocating the IP addresses in this range to DHCP client(s). Router and server IP addresses should typically be excluded from the DHCP server address pool.

To exclude IP addresses in a range from the DHCP server address pool, for example, from **192.168.1.0** to **192.168.1.5** and **192.168.1.200** to **192.168.1.254**, perform the following steps:

```
#configure terminal
```

! Set up excluded IP range 192.168.1.0 ~ 192.168.1.5 and 192.168.1.200 ~ 192.168.1.254.

```
(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.5
```

```
(config)#ip dhcp excluded-address 192.168.1.200 192.168.1.254
```

```
(config)#end
```



### NOTE

*The first address in the range must be a lower IP address than (or equal to) the second IP address in the range.*

## DHCP Relay

To configure DHCP relay in an ASE device, you must specify the IP Helper Address. The IP Helper address is the unicast address of the DHCP relay server or a device on the same subnet as the server. For example, to configure the IP Helper address 192.168.10.1, enter the following command from Global Configuration mode:

```
(config)#ip helper 192.168.10.1
```

### Option 82

If DHCP Relay is enabled, you can also choose to enable DHCP Relay Information mode (Option 82). Option 82 adds a layer of security to DHCP by preventing DHCP client requests from untrusted devices. To enable DHCP Option 82, enter the following command from Global Configuration mode:

```
(config)#ip dhcp relay information option
```

Choose the policy for handling DHCP messages received that already contain DHCP relay information.

```
(config)#ip dhcp relay information policy [drop|keep|replace]
```

**drop**      drop the packet  
**keep**      keep the original DHCP relay information  
**replace**    replace the original DHCP relay information

## 6. Troubleshooting

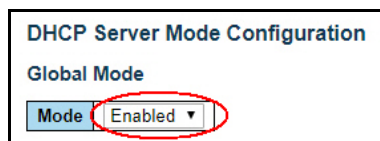
The ASE device can display information that aids in troubleshooting DHCP configurations. The following steps are recommended when trying to troubleshoot a problem with the DHCP server:

1. [Verify the DHCP Server is Configured Correctly:](#)
  - DHCP Server Globally Enabled
  - DHCP Server Enabled on VLAN
  - Excluded IP Address Ranges
  - DHCP Address Pool
2. [Verify that the VLAN Interface Status is UP](#)
3. [Verify that the DHCP Pool and Layer 3 VLAN Interface are in the Same Subnet](#)
4. [Verify the VLAN of the Port for the DHCP Device](#)
5. [Verify that the ASE Device is Seeing DHCP Messages](#)
6. [Verify that there is not an ACL blocking DHCP](#)
7. [Further Analysis Using Packet Capture](#)

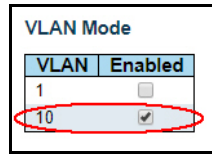
### Verify the DHCP Server is Configured Correctly

To verify the DHCP server configuration in the GUI, follow these steps:

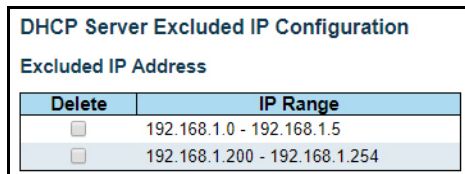
1. Navigate to **Configuration > DHCP > Server > Mode**, and ensure that the DHCP server is **Enabled**.



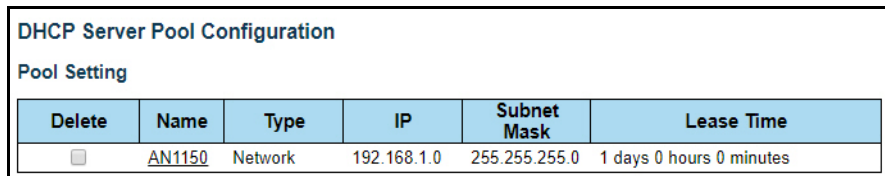
- Verify that the DHCP server is enabled on the VLAN that you are troubleshooting (in this example, DHCP is enabled on VLAN 10).



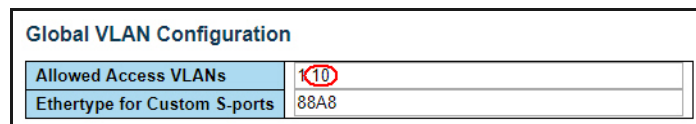
- Verify that excluded IP addresses and ranges have been configured correctly.



- Verify that the DHCP Pool is configured correctly in the same subnet as the excluded addresses.



- Verify that the VLAN on which the DHCP server resides is enabled globally. Navigate to **Configuration > VLANs > Configuration** and check to see that the DHCP server VLAN number is listed in the Allowed Access VLANs.



To verify the DHCP server configuration in the CLI, issue the **show run feature dhcp\_server** command:

```
#show run feature dhcp_server
Building configuration...
ip dhcp server
ip dhcp excluded-address 192.168.1.0 192.168.1.5
ip dhcp excluded-address 192.168.1.200 192.168.1.254
!
.....
!
!
interface vlan 1
!
interface vlan 10
ip dhcp server
!
.....

line vty 15
!
```

Indicates DHCP server is enabled globally. All excluded IP address ranges are displayed.

DHCP Server is enabled on VLAN 10.



```

ip dhcp pool AN1150
 network 192.168.1.0 255.255.255.0
 broadcast 192.168.1.255
 default-router 192.168.1.200
 lease 1 0 0
 domain-name my.net
 dns-server 192.168.1.234 8.8.8.8
 ntp-server 192.168.1.234 192.168.1.5
!
ip dhcp server
ip dhcp excluded-address 192.168.1.0 192.168.1.5
ip dhcp excluded-address 192.168.1.200 192.168.1.254
!
end
    
```

Verify the DHCP Pool Configuration.

### Verify that the VLAN Interface Status is UP

To verify the VLAN interface status in the GUI, navigate to **Monitor > System > Routing Info. Base** and verify the State is **Active** for the VLAN of interest.

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
S *	0.0.0.0/0	10.19.14.254	1	0	VLAN 1	-	Active
C *	10.19.14.0/24	-	-	-	VLAN 1	-	Active
C *	192.168.1.0/24	-	-	-	VLAN 10	-	Active

To verify the VLAN interface status in the CLI, issue the **show ip interface** command to display the status of the VLAN interfaces and verify the VLAN of interest is UP:

```

#show ip interface
Interface Address Method Status
-----
VLAN 1 10.19.14.66/24 Manual UP
VLAN 10 192.168.1.1/24 Manual UP
    
```

### Verify that the DHCP Pool and Layer 3 VLAN Interface are in the Same Subnet

Typically, the DHCP Pool IP address and the Layer 3 VLAN interface address should be in the same subnet. To verify the subnet of the DHCP pool and Layer 3 VLAN interface in the GUI, follow these steps:

1. First, verify the DHCP Pool IP address. Navigate to **Configuration > DHCP > Server > Pool** and check the IP address.

Delete	Name	Type	IP	Subnet Mask	Lease Time
<input type="checkbox"/>	AN1150	Network	192.168.1.0	255.255.255.0	1 days 0 hours 0 minutes

- Next, compare the DHCP Pool IP address to the IP address assigned to the VLAN interface for the DHCP server. Navigate to **Configuration > System > IP** and examine the IP address assignment. Ensure that this IP address is in the same subnet as the DHCP Pool IP address.

Delete		VLAN	Enable	Type	Client ID			Hostname	Fallback	Current Lease	IPv4	
					IfMac	ASCII	HEX				Address	Mask Length
<input type="checkbox"/>	<input type="checkbox"/>	1	<input type="checkbox"/>	Auto	Port 1				0		10.19.14.66	24
<input type="checkbox"/>	<input type="checkbox"/>	10	<input type="checkbox"/>	Auto	Port 1				0		192.168.1.1	24

You can verify the DHCP Pool and Layer 3 VLAN Interface IP addresses in the CLI by issuing the **show run** command:

```
#show run
Building configuration...
!
interface vlan 1
ip address 10.19.14.66 255.255.255.0
!
interface vlan 10
ip address 192.168.77.1 255.255.255.0
ip dhcp server
!
ip dhcp pool AN1150
network 192.168.77.0 255.255.255.0
broadcast 192.168.77.255
default-router 192.168.77.200
lease 1 0 0
domain-name my.net
dns-server 192.168.77.234
ntp-server 192.168.77.234
!
ip dhcp server
ip dhcp excluded-address 192.168.77.0 192.168.77.5
ip dhcp excluded-address 192.168.77.200 192.168.77.254
!
end
```

Notice that the IP address on which the DHCP server is running, 192.168.77.1, is on the same subnet as the DHCP Pool, which is 192.168.77.0.

### Verify the VLAN of the Port for the DHCP Device

To verify the VLAN of the port for the DHCP device in the GUI, navigate to **Monitor > VLANs > Membership** and verify that the port used by the device to the DHCP Server is on the correct VLAN.

VLAN Membership Status for Combined users										
Start from VLAN		1	with		20	entries per page.		<<	>>	
Port Members										
VLAN ID	1	2	3	4	5	6	7	8	9	10
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To verify the DHCP device port's VLAN in the CLI, issue the **show vlan** command to display a list of VLANs and their associated interfaces (port members):

```
#show vlan
VLAN  Name                               Interfaces
-----
1     default                               Gi 1/1-3,5-10
10    VLAN0010                              Gi 1/4
```

## Verify that the ASE Device is Seeing DHCP Messages

View the DHCP server statistics to see a snapshot of the number of DHCP DISCOVER messages received and the number of OFFER and ACK messages the ASE devices has sent. If any of these counters have a value of zero, you can identify where the DHCP process is failing. Refer to [The DHCP Request Process on page 6](#) for detailed information on DHCP negotiation messages.

To verify the switch is seeing DHCP messages in the GUI, navigate to **Monitor > DHCP > Server > Statistics** and examine the DISCOVER, OFFER, and ACK counters.

DHCP Server Statistics				
Database Counters				
Pool	Excluded IP Address	Declined IP Address		
1	2	0		
Binding Counters				
Automatic Binding	Manual Binding	Expired Binding		
1	0	0		
DHCP Message Received Counters				
DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
3441	2	0	0	202
DHCP Message Sent Counters				
OFFER	ACK	NAK		
17	204	0		

To verify the switch is seeing DHCP messages in the CLI, issue the **show ip dhcp server statistics** command:

```
#show ip dhcp server statistics
```

```
Database Counters
```

```
=====
POOL                1
Excluded IP        2
Declined IP        0
=====
```

```
Binding Counters
```

```
=====
Automatic          1
Manual             0
Expired            0
=====
```

```
Message Received Counters
```

```
=====
DISCOVER           3441
=====
```

```

REQUEST          2
DECLINE          0
RELEASE          0
INFORM           210
=====
    
```

Message Sent Counters

```

=====
OFFER            17
ACK              212
NAK              0
=====
    
```

## Verify that there is not an ACL blocking DHCP

Ensure that an ACL is not blocking the DHCP server or host.

To verify the ACL configuration in the GUI, navigate to **Monitor > Security > Network > ACL Status** to view details for configured ACLs on the ASE device. If you do not have any ACLs configured, the web interface will display two VLANs.

ACL Status									
User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict	
dhcp	1	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Yes	14	No	
dhcp	2	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Yes	5332	No	
IP	1	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No	
IP	2	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No	

To verify ACL configuration in the CLI, issue the **show access-list ace statistics** command to display a list of configured ACLs on the ASE device. In the following example, the command was issued on a device that did not have any configured ACLs:

```

#show access-list ace statistics
Switch access-list ace number: 0
    
```

## Further Analysis Using Packet Capture

Using a third party packet capture program, you can capture packets on the VLAN or on the DHCP client. You can then analyze the captured DHCP packets and compare them to the DHCP statistics information gathered earlier. See [Verify that the ASE Device is Seeing DHCP Messages on page 19](#) for information on statistics and comparing the information against the DHCP request process.

## 7. Warranty and Contact Information

### Warranty

Warranty information can be found at:

[www.adtran.com/warranty](http://www.adtran.com/warranty).

### Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. <b>Technical Support:</b> <ul style="list-style-type: none"> <li>• Web:</li> </ul> <b>Training:</b> <ul style="list-style-type: none"> <li>• Email:</li> <li>• Web:</li> </ul>	1-888-4ADTRAN (1-888-423-8726) + 1 (256) 963-8716  <a href="http://www.adtran.com/support">www.adtran.com/support</a>  training@adtran.com <a href="http://www.adtran.com/training">www.adtran.com/training</a> <a href="http://www.adtranuniversity.com">www.adtranuniversity.com</a>
Sales	Pricing and Availability	1-800-827-0807