Technical Guide

# Dynamic Host Configuration Protocol - DHCP

## Feature Overview and Configuration Guide

## Introduction

Dynamic Host Configuration Protocol (DHCP) is a standardized client/server network protocol that dynamically assigns IP addresses and other related configuration information to network devices. Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually.

DHCP is widely used in everyday life, for example when you:

- turn on your cell phone and connect to the Internet
- use a hotspot or wifi in a cafe
- connect to your home or office network

The key thing to understand about DHCP is that it **dynamically** assigns IP addresses. This is in contrast with its alternative, static addressing. With **static** addressing, IP addresses are assigned manually to specific devices, and do not change over time as the device is used. Static addressing is typically used where the source address of the device must not change, for example, to access a service such as a printer server. With this in mind, DHCP allows **reservations** - these are static IP addresses within the DHCP scope that can be assigned to specific servers or devices and never given out to other devices.

DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. A **DHCP server** provides this information to a **DHCP client** through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction. If the DHCP server and DHCP clients are located on different subnets, a **DHCP relay agent** is used to facilitate the conversation. DHCP is based on BOOTP, and is defined in RFC 2131.

AlliedWare Plus™ OPERATING SYSTEM

## Products and software version that apply to this guide

This guide applies to all AlliedWare Plus™ products, running version **5.4.4** or later.

For more information, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

From version **5.5.2-0.1** onwards, you can use commands to configure DHCP port based IP address assignment.

# Contents

# Benefits of DHCP

DHCP provides many benefits for network administrators, network users, and people using consumer gadgets such as mobile phones, tablets, and laptops to connect to the network. This section focuses on the benefits for network users and network administrators.

## Network users

DHCP provides network users with ‘plug and play’ networking. This means that network users can travel anywhere on the network and automatically receive an IP address when they reconnect to the network.

## Network administrators

DHCP provides network administrators with quicker and more reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Network administrators find DHCP useful when they want to change the IP addresses of a large number of systems. Instead of reconfiguring all the systems, they can just edit one DHCP configuration file on the server for the new set of IP addresses. If the DNS server for an organization changes, the changes are made on the DHCP server, not on the DHCP clients.

Because DHCP is easy to configure, it minimizes operational overhead and costs associated with configuration.

DHCP includes the following features to reduce network administration:

- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

DHCP also helps conserve limited IP address space, because IP addresses no longer need to be permanently assigned to hosts.

# How does DHCP work

When you access the Internet, your computer automatically requests an IP address from the network's DHCP server. The DHCP server contains a range (or scope) of IP addresses that it is allowed to give out. If there is an address available, the DHCP server will send your computer a response containing an IP address, the default gateway address, subnet mask, and the lease time that your computer can use the address for.

You might ask, "why is the IP address leased?" This is so that the range of IP addresses can be recycled and not used up, or left as 'used' by a device that has been disconnected. Leases times are configured to suit various requirements. For example, a cafe with free wifi may have leases that last/expire in **1** day, but in an Enterprise environment such as a call center with 1000 computers using the same IP addresses from a DHCP server 'permanently', they may use a lease of **100** days. This would make sure no undue network traffic was going on simply for renewing an IP address for hosts plugged in all the time.

Clients renew their leases (generally at 50% of the lease time), and when the lease is renewed it will usually be the same IP address.

Of course, not every device on the network needs to have a dynamic IP address. Using DHCP, you can reserve addresses for devices such as printers. As each network device has a MAC address, you can assign a static IP at the server to a specific MAC address. This allows devices such as the network printer to always get the same IP address even after it reboots and without assigning the IP address at the printer.

# DHCP architecture

The DHCP architecture is made up of DHCP clients, DHCP servers, and DHCP relay agents. The client interacts with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases.

Here is a brief description of the DHCP components:

## DHCP client

A DHCP client is any IP device connected on the network that has been configured to act as a host requesting configuration parameters such as an IP address from a DHCP server. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. DHCP uses the Options to pass additional IP settings to DHCP clients such as the default gateway IP address, DNS server address, and the DNS domain name.

For more detail about Options see "Configuring the DHCP client" on page 10.

## DHCP server

The DHCP server is a device on the network with a pool of IP addresses at its disposal to automatically assign to devices as they join the network.

The DHCP server assigns the network device its:

- IP address - **dynamically** configured
- subnet mask - **statically** configured
- default gateway for the network - **statically** configured
- Primary DNS server - to match a device NAME to an IP address
- Secondary DNS server - **statically** configured for redundancy and load balancing.

## DHCP relay agent

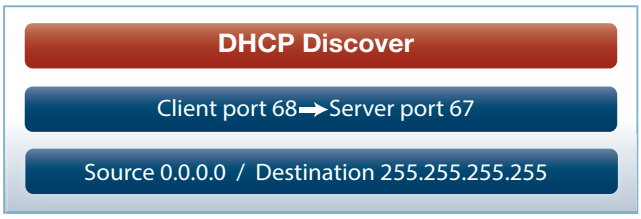
DHCP relay agents pass DHCP messages between servers and clients where the DHCP server does not reside on the same IP subnet as its clients.

For example, on large networks consisting of multiple subnets, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. You can configure a maximum number of 400 DHCP relay agents (one per interface) on AlliedWare Plus devices.

You can use DHCP relay agent information, Option 82, to protect your switch from spoofing attacks, where untrusted hosts send requests for IP addresses to access the network. For more information on Option 82 see, "DHCP relay agent information option (Option 82)" on page 18.

The following diagram shows the changing port numbers and the source and destination addresses used during the DHCP transaction. UDP port 68 is reserved for DHCP clients, and UDP port 67 is reserved for DHCP servers.

**Step 1** **DHCP Discover**

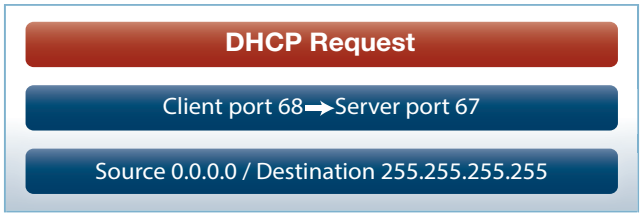



- Sent by the client looking for the IP address. The source IP is 0.0.0.0 because the client doesn't have an IP address. The destination is 255.255.255.255, which is the broadcast address, as the client doesn't know where the DHCP server is located, so it broadcasts to all devices on the network.

**Step 2** **DHCP Offer**

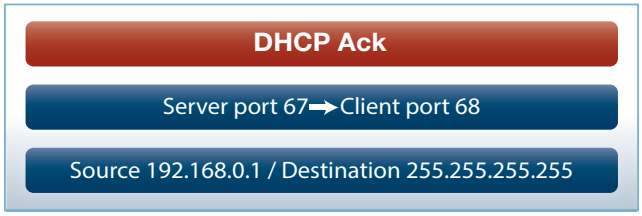

- Sent by the DHCP server offering an IP address to the client. The source address is the DHCP server address. The DHCP server doesn't know the client address yet, so it broadcasts the offer to all devices on the network.

**Step 3** **DHCP Request**




- Sent by the client to the DHCP server to say "I will take that IP address, thanks." The client IP address is still 0.0.0.0 and it is again broadcast to all so that any other servers on the network that may have offered an IP address will know to stop communicating with the client for now.

**Step 4** **DHCP Acknowledgment**



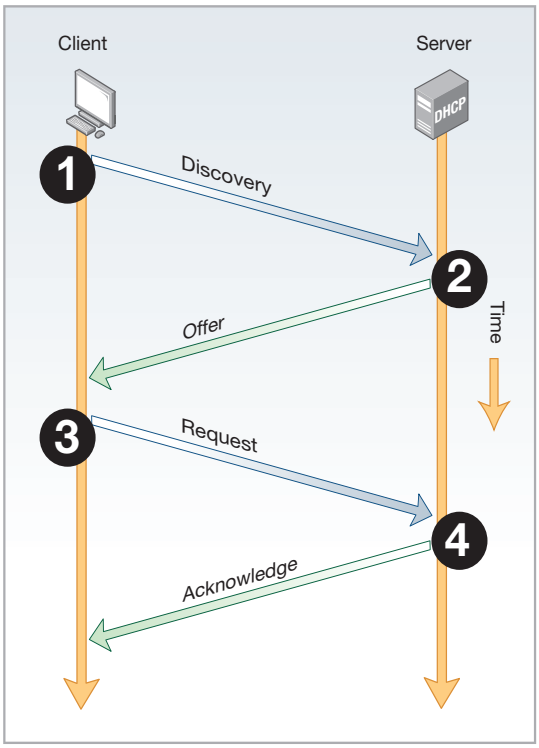

- Sent by the DHCP server to the client. It confirms the IP address and other details such as subnet mask, default gateway, and lease time with the client. The source address is the DHCP server and the destination is still the broadcast address.

## The DHCP process

There are four basic steps the DHCP process follows when a client connects to the network:

1. The client broadcasts a **DHCP Discover message** to say “I need an IP address, are there any DHCP servers out there?”
2. Multiple DHCP servers may respond (via broadcast) with an **OFFER** for a leased IP address back to the client.
3. The client will choose a DHCP server offer and then broadcast a DHCP **REQUEST** back to the DHCP server(s) to say “Thanks, I have selected an offer from this DHCP server.” All servers will see which offer the client selected.
4. Finally, the selected DHCP server will send (broadcast) an **ACKNOWLEDGEMENT** back to the client to confirm the IP address, lease time, and other details.

Figure 1: Basic DHCP transaction




### Lease renewal

If a clients wants to continue using its leased IP address it performs a renewal, generally at 50% of the lease time. This follows a simpler process than the initial lease acquisition. The client sends a DHCP REQUEST, requesting the address it is currently using. This time the message is unicast to the server it originally leased the address from. If the server can allow the client to continue using that address, it replies with a DHCP ACK.

### Releasing an IP address

If a client no longer wishes to continue using a leased address, it sends a DHCP RELEASE message to the server. This indicates to the server that the client is no longer using the address and it is free to be allocated to another client in the future.

## Port based DHCP address assignment

The DHCP Server Port-Based Address Allocation feature introduces the capability to ensure that the same IP address is always offered to a replacement device as the device being replaced.

This IP address is always offered to the same connected port even as the client identifier (client-id) or client hardware address (chaddr) changes in the DHCP messages received on that port.

This feature is enabled by substituting subscriber identifier (subscriber-id) for client-id in all DHCP server internal transactions (such as packet processing, lease management etc). And to allow port based address assignment, subscriber-id of a client needs to be associated with the physical port attachment.

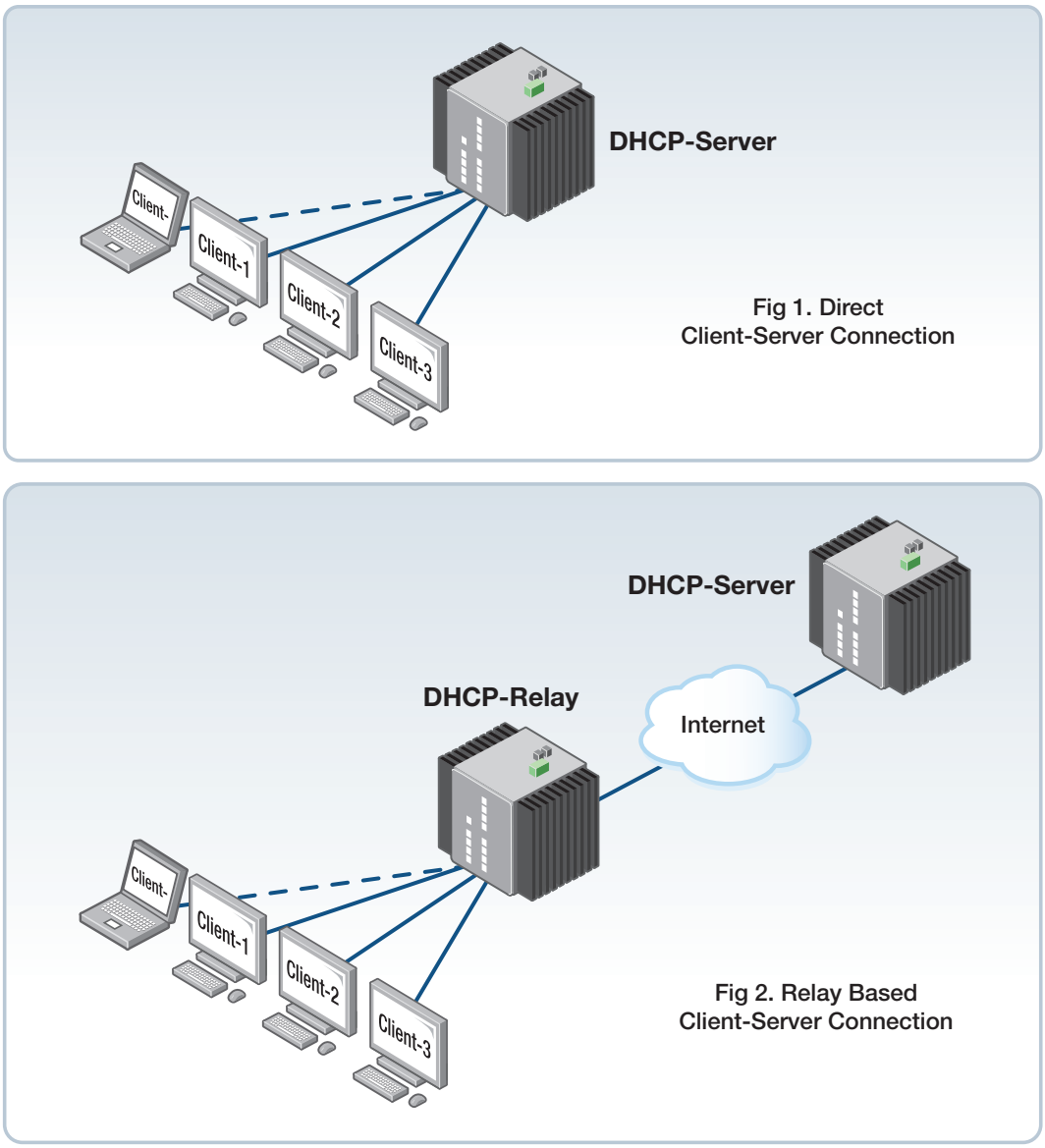
Subscriber-id for remote client is included in the relay-agent information option on DHCP client packets relayed via a relay-agent, and for locally attached client, its subscriber-id is internally generated based on and associated with port interface directly attached to the DHCP client. On wire, DHCP client-id on messages used between client and server are preserved to the original client-id used by the client, this will avoid issues with interoperability with the standard DHCP client and relay implementation.

Another feature that is introduced with this enhancement is the ability for the server to make IP address reservation based on the subscriber-id.

This feature is designed to work with the following deployment scenarios:

- Direct client-server connection
  In this deployment scenario, host devices (DHCP clients) are directly attached to the switch acting as a DHCP server. The DHCP client sends DHCP messages without relay agent information option - thus without subscriber-id sub-option. Therefore we have to internally generate the subscriber-id for the client based port interface attached to the client. In this deployment scenario, only automatically generated port names can be used as subscriber-id, thus client connected to port1.0.1 of the switch acting as the server will be automatically assigned with internal subscriber-id of ‘port1.0.1’, and so on.
- Relay based client-server connection
  When host devices are connected to a switch acting either as a DHCP relay agent or running the DHCP snooping feature, the relay agent or the DHCP snooper has to be able to insert relay agent information option (option 82) with the subscriber-id sub-option (sub-option 6). The subscriber-id sub-option carried in the messages transmitted by the client will be used internally by the server as substitute for client-id for the purpose of address assignment and lease management. And to make port based assignment possible, users need to associate subscriber-id with port where the client host device is attached to.

Figure 2: Deployment scenarios for port-based IP assignment



# Configuring DHCP

This section describes how to configure the DHCP:

- Client
- Server
- Relay agent
- Short lease threshold
- Port based IP assignment

## Configuring the DHCP client

You can configure an interface on your device with a static IP address, or with a dynamic IP address assigned using your device's DHCP client. When you use the DHCP client, it obtains the IP address for the interface, and other IP configuration parameters, from a DHCP server. To configure an interface and gain its IP configuration using the DHCP client, use the commands:

```
awplus(config)# interface <ifname>
awplus(config-if)# ip address dhcp [client-id <interface>] [hostname
<hostname>}
```

The DHCP client supports the following IP configuration options:

Table 1: DHCP client options

| OPTION CODE | DESCRIPTION |
|---|---|
| 1 | The subnet mask for your device. |
| 3 | A list of default routers. |
| 6 | A list of DNS servers. This list appends the DNS servers set on your device with the **ip name-server** command. |
| 15 | A domain name used to resolve host names. This option replaces the domain name set with the **ip domain-name** command.<br>Your device ignores this domain name if it has a domain list set using the **ip domain-list** command. |
| 51 | Lease expiration time. |

Options are defined when you configure the DHCP server. For information on how to configure the Options, see "Set the options" on page 14.

If an IP interface is configured to get its IP address and subnet mask from DHCP, the interface does not take part in IP routing until the IP address and subnet mask have been set by DHCP.

To configure a static IP address on an interface, use the **ip address** command.

## Configuring the DHCP server

The DHCP server uses **address pools** when responding to DHCP client requests. Address pools contains specific IP configuration details that the DHCP server can allocate to a client. You can configure multiple address pools on the device for different networks.

To configure an address pool, you must:

1. **Create the pool** and enter its configuration mode.
2. **Define the network** the pool applies to.
3. **Define the range** of IP addresses that the server can allocate to clients. You can specify multiple address ranges for each pool.
4. **Set the lease** for the clients. This defines whether the clients receive a dynamic, permanent, or static IP address.
5. **Set the options** (standard and user-defined) that the clients of a pool require when configuring their IP details.
6. After configuring the address pools, **enable the DHCP server** by using the command:

```
awplus(config)# service dhcp-server
```

- For networks where you do not want the server to respond to BOOTP requests, you can configure the DHCP server so that it ignores them by using the command:

```
awplus(config)# ip dhcp bootp ignore
```

### Create the pool

A DHCP pool is identified by a name. To create a DHCP pool and enter the DHCP Configuration mode for the pool, use the command:

```
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)#
```

### Define the network

Define the network that the DHCP clients are in. You can define one network per address pool. Use the following command to define the network after defining the DHCP pool first:

```
awplus(dhcp-config)# network {<ip-subnet-addr/prefix-length>|<ip-subnet-addr/mask>
```

- For remote clients, set the network address to the network of the remote clients. The **network** command does not need to match a specific interface's network, because the DHCP server listens on all IP interfaces for DHCP requests.
- For locally connected clients, ensure that the desired interface has an IP address and subnet mask defined; use the **ip address *<ip-addr/prefix-length>*** command (in interface configuration mode ) to set a static address. Enter the configuration mode for the pool, and set the DHCP address pool's network to match the interface's network. Pools that span multiple interfaces are possible only if the interface networks are contiguous.

### Define the range

Configure an IP address range for the pool. This range must be in the same subnet as the pool's network setting. Use the command:

```
awplus(dhcp-config)# range <ip-address> [<ip-address>]
```

The first IPv4 address specifies the low end of the range, while the second IP address is the high end. You can set the range to a single IP address by specifying only one IP address.

### Set the lease

The DHCP server assigns IP settings to hosts for specific times (the lease time). Each DCHP pool has one lease time setting. You can use DHCP to allocate the following types of addresses:

- A **dynamic** IP address
  These are available to a host for a limited amount of time. When the lease expires, the server can reallocate the IP address to another device. To set the lease time for the DHCP pool so that it assigns dynamic IP addresses, use the command:

```
awplus(dhcp-config)# lease <days> <hours> <minutes> [<seconds>]
```

- A **permanent** IP address
  These are available to a host for an unlimited amount of time. To set the lease time to assign permanent IP addresses, use the command:

```
awplus(dhcp-config)# lease infinite
```

- A **static** IP address
  These are allocated to a particular client. The DHCP server recognizes the client by its MAC address. This lets you use DHCP to manage most of your network automatically, while having unchanging IP addresses on key devices such as servers. To assign a static IP address to a device, use the command:

```
awplus(dhcp-config)# host <ip-address> <mac-address>
```

BOOTP requests can be satisfied by pools with leases set to infinity.

### Enable DHCP Leasequery

The DHCP Leasequery protocol (RFC 4388) allows a device or process, for example a DHCP relay agent, to obtain IP address information directly from the DHCP server using DHCPLEASEQUERY messages.

DHCPLEASEQUERY messages support three query regimes:

**IP address**

- Only an IP address is supplied in the DHCPLEASEQUERY message. The DHCP server will return any information that it has on the most recent client to have been assigned that IP address.

**MAC address**

- Only a MAC address is supplied in the DHCPLEASEQUERY message. The DHCP server will return any information that it has on the IP address most recently accessed by a client with that MAC address. Also, the DHCP server may supply additional IP addresses that have been associated with that MAC address in different subnets.

**Client identifier option**

- Only a client identifier option is supplied in the DHCPLEASEQUERY message. The DHCP server will return any information that it has on the IP address most recently accessed by a client with that client identifier. Also, the DHCP server may supply additional IP addresses that have been associated with the client identifier in different subnets.

An AlliedWare Plus DHCP server implementing DHCP Leasequery supports all three query regimes.

If the DHCP Leasequery feature is enabled, when a DHCP relay agent needs to know the location of an IP endpoint and sends a DHCPLEASEQUERY message, the DHCP server will reply with either a DHCPLEASEACTIVE, DHCPLEASEUNASSIGNED, or DHCPLEASEUNKNOWN message.

When the DHCP server replies to a DHCPLEASEQUERY message:

- a DHCPLEASEACTIVE message allows the DHCP relay agent to determine the IP endpoint location and the remaining duration of the IP address lease.
- a DHCPLEASEUNASSIGNED message indicates that there is no current active lease for the IP address, but the DHCP server does manage that IP address.
- a DHCPLEASEUNKNOWN message indicates that the DHCP server supports DHCP Leasequery but has no knowledge of the query information specified in the DHCPLEASEQUERY message (e.g., IP address, MAC address, or client identifier option).

To enable the DHCP Leasequery feature, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp leasequery enable
```

To disable the DHCP Leasequery feature, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp leasequery enable
```

To display information about DHCP Leasequery messages, use either of the commands:

```
awplus# show counter dhcp-server
awplus# show ip dhcp server statistics
```

To display information about the current configuration of the DHCP server, including whether the DHCP server is configured to support DHCP Leasequery, use the command:

```
awplus# show ip dhcp server summary
```

### Set the options

DHCP allows clients to receive options from the DHCP server. Options describe the network configuration, and various services that are available on the network. Options are configured separately on each DHCP pool. You can configure both standard predefined options and user-defined options for a DHCP pool.

To create a user-defined option, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option <1-254> [name <option-name>
[<option-type>]]
```

To add a user-defined option to a DHCP address pool, use the commands:

```
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)# option [<1-254>|<option-name>] <option-value>
```

It is possible to add a user-defined option with the same number as an existing pre-defined option. If this situation occurs, the user-defined option takes precedence—that is, it overrides but does not eliminate the standard option.

You can set some pre-defined options using the following commands:

- To set a subnet mask (option 1) for the address pool, use the command:

```
awplus(dhcp-config)# subnet-mask <mask>
```

- To add a domain name (option 15) for the address pool, use the command:

```
awplus(dhcp-config)# domain-name <domain-name>
```

- To add a default router (option 3) for the address pool, use the command:

```
awplus(dhcp-config)# default-router <ip-address>
```

- To add a DNS server (option 6) for the address pool, use the command:

```
awplus(dhcp-config)# dns-server <ip-address>
```

### DHCP lease probing

Probing is used by the DHCP server to check whether an IP address it wants to lease to a client is already being used by another host. Probing is configured on a per-DHCP pool basis. You can specify probing either by ICMP Echo Request (ping) or by ARPing. ARP probing is useful in networks where ICMP may be blocked on some devices, whereas ARP is always supported. ARP and ping probing are mutually exclusive and cannot operate concurrently within a DHCP pool.

Probing is enabled by default when a DHCP pool is created.

To enable probing if probing has previously been disabled for a DHCP pool, enter the configuration mode for the pool with the **ip dhcp pool** command and then use the command:

```
awplus(dhcp-config)# probe enable
```

The default probe type is ping. To specify the probe type as ARP, enter the configuration mode for the pool and then use the command:

```
awplus(dhcp-config)# probe type arp
```

To set the timeout value in milliseconds to wait for a response after each probe packet is sent, use the command:

```
awplus(dhcp-config)# probe timeout <50-5000>
```

To specify the number of packets sent for each lease probe, use the command:

```
awplus(dhcp-config)# probe packets <0-10>
```

To disable probing for a DHCP pool, enter the configuration mode for the pool and then use the command:

```
awplus(dhcp-config)# no probe enable
```

To display the lease probe configuration settings for a specific DHCP pool or for all DHCP pools configured on the device, use the command:

```
awplus# show ip dhcp pool [<address-pool>]
```

## Configuring a DHCP server to be VRF aware

From version 5.5.1-1.1 onwards, you can configure a DHCP server to be VRF aware. This means you can associate a VRF with a DHCP address pool and (optionally) use the same DHCP lease across multiple isolated networks. You can configure DHCP pools with same or different network and address ranges associated with each.

The command: `vrf <name>` which allows you to add a VRF name to a DHCP server's address pool. For example, to add the VRF named 'red' to the DHCP address pool named 'red_pool', use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool red_pool
awplus(dhcp-config)# vrf red
```

To remove the VRF named ‘red’ from ‘red_pool’ use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool red_pool
```

## Example configuration

Here is a simple configuration for a DHCP VRF-aware server.  This example shows how to configure VRF aware DHCP server address pools.

The **vrf** command must be added to the DHCP server pool before the **network** and **range** address commands. The VRF instance must exist before the VRF command is configured.

Note: When a new DHCP Lease Request is received by the server it will look up the VRF domain the request was learned on and assign a lease based off of valid pool(s) for the VRF. This also means the same pool address range can be used by multiple VRF instances.

.

```
...
ip dhcp pool blue_pool
 vrf blue
 network 192.168.4.0 255.255.255.0
 range 192.168.4.10 192.168.4.20
 host 192.168.4.3 aaaa.bbbb.cccc
!
ip dhcp pool green_pool
 vrf green
 network 192.168.4.0 255.255.255.0
 range 192.168.4.10 192.168.4.20
 host 192.168.4.3 aaaa.bbbb.cccc
 dns-server 192.168.2.1
 dns-server 192.168.3.1
!
server dhcp-server
!
ip vrf blue 1
!
ip vrf green 2
....
....
interface vlan6
 ip vrf forwarding green
 ip address 192.168.4.1/24
!
interface vlan7
 ip vrf forwarding blue
 ip address 192.168.4.1/24
!
```

## Limitations

We would recommend a max limit of 32 DHCP Server instances on the AR2050 due to memory limitations.

## Configuring the DHCP relay agent

DHCP relay agents pass BOOTP messages between servers and clients. Networks where the DHCP or BOOTP server does not reside on the same IP subnet as its clients need the routers attached to the subnet to act as DHCP relay agents.

Note that both BOOTP and DHCP use BOOTP messages, allowing DHCP relay agents to relay all their packets.

Your device's DHCP relay agent relays these message types:

- BOOTREQUEST messages originating from any of the device's interfaces to a user-defined destination.
- BOOTREPLY messages addressed to BOOTP clients on networks directly connected to the device.

The DHCP relay agent ignores BOOTREPLY messages addressed to clients on networks not directly connected to the device. The device treats these as ordinary IP packets for forwarding.

A BOOTREQUEST message is relayed via unicast.

The hops field in a BOOTP message records the number of DHCP relay agents the message has been through. If the value of the hops field exceeds a predefined threshold, the DHCP relay agent discards the message.

### Enabling the DHCP relay agent

To enable the DHCP relay agent on your device, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

Note DHCP relay agent is enabled by default on your switch. You only need to enter a **service dhcp-relay** command if DHCP relay agent is disabled on your switch.

You must define a relay destination on one of the device's interfaces before the relay agent can relay packets. This is the path to the DHCP server. To define a relay destination on the currently specified interface, use the commands:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay server-address {<ipv4-address>| <ipv6-address> <server-interface>}
```

You can define more than one relay destination on your device. The following table describes how the DHCP relay agent forwards the packets.

| If an interface has... | Then the relay agent relays BOOTP packets it receives on that interface to... |
|---|---|
| One relay destination defined | The relay destination |
| Multiple relay destinations defined | Each defined relay destination |

To delete a DHCP relay destination, use the command:

```
awplus(config-if)# no ip dhcp-relay server-address {<ip-address>| <ipv6-address> <server-interface>}
```

See the **ip dhcp-relay server-address** command and the **service dhcp-relay** command for command description and command examples. You can use the **ip dhcp-relay server-address** command to configure an IPv4 or IPv6 server address to relay to.

When the 'hops' field in a BOOTP message exceeds a predefined threshold the BOOTP message is discarded. The default of the threshold is 10. To set the threshold, use the command:

```
awplus(config-if)# ip dhcp-relay maxhops <1-255>
```

To display the current configuration of the DHCP relay agent, use the command:

```
awplus# show ip dhcp-relay [interface <interface-name>]
```

## DHCP relay agent information option (Option 82)

You can use DHCP relay agent information option (Option 82) to protect your switch from spoofing attacks, where untrusted hosts send requests for IP addresses to access the network. The switch relays these requests to DHCP servers and the servers send IP address leases in response. Untrusted hosts then use these IP addresses for spoofing attacks. Option 82 provides information about the location of a DHCP client for the DHCP server.

Enabling the DCHP relay agent information option feature on the switch allows the switch to insert extra information into the DHCP packets that it is relaying. This information enables accurate identification of a subscriber, as it states which interface on which relay switch the subscriber is connected to. The information is stored in an optional field in the DHCP packet header, the relay agent information option field, with the option ID 82.

The DHCP relay agent inserts the Option 82 information into the DHCP packets that it is relaying to a DHCP server. DHCP servers that are configured to recognize Option 82 may use the information to implement IP addresses, or other parameter assignment policies, based on the network location of the client device.

Alternatively, the server can simply log this information to create a detailed audit trail of the locations of the clients to which given addresses were allocated at given times. For more information, see the DHCP Snooping Feature Overview and Configuration Guide.

If Option 82 insertion is enabled, then the DHCP packet flow is as follows:

- The DHCP client generates a DHCP request and broadcasts it on the network.
- The DHCP relay agent intercepts the broadcast DHCP request packet and inserts the Option 82 field in the packet.
- The DHCP relay agent unicasts the DHCP request that includes the Option 82 field to the DHCP server.
- The DHCP server receives the packet.
- If the DHCP server supports Option 82, then it echoes the Option 82 field in the DHCP reply. If the server does not support Option 82, it ignores the option and does not echo it in the reply.
- The DHCP server unicasts the reply to the relay agent.
- The relay agent removes the Option 82 field and forwards the packet to the switch port connected to the DHCP client that sent the DHCP request.

For information about DHCP relay agent information Option 82, see RFC 3046.

To enable the relay agent to insert its details into the Option 82 field in requests received from clients on a particular interface, use the command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option
```

The Option 82 field contains sub-options. You can specify a value for the Remote ID sub-option, which contains information that identifies the host. To specify a value for the Remote ID, use the command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option <remote-id>
```

If a Remote ID value is not specified, the Remote ID sub-option is set to the switch's MAC address. You can also configure the Remote ID value as an alphanumeric string.

Note: Option 82 agent information added by DHCP Relay differs from the information inserted by DHCP snooping. If you configure both DHCP Snooping and DHCP Relay on the switch, you cannot use DHCP Relay to insert Option 82 information. You must use DHCP snooping to insert it instead.

### Dealing with client-originated packets that already contain Option 82 information

It is possible that the requests arriving from the clients to the relay agent could already contain Option 82 data. There are two main circumstances in which this can occur:

1. A client is maliciously inserting bogus information into the packet in an attempt to subvert the process of identifying the client's location. In this case, you would want to drop the packets that contain the bogus information (or remove bogus information).
2. A Layer 2 DHCP snooping switch, that sits between the clients and the DCHP relay, is validly inserting the Option 82 information into the packets. The DHCP snooping switch is not acting as a relay agent, but is inserting the Option 82 information. In this case, you would want to forward the valid information to the DHCP server.

The action taken on packets with an Option 82 field is configurable. The command to configure this action is shown below:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay information policy [append|drop|keep|
replace]
```

This command sets the action that the DHCP relay should take when a received DHCP client request contains Option 82 information.

This command takes parameters that can configure the switch to:

- Leave the existing Option 82 field untouched (**keep** parameter).
- Append its own Option 82 field after the existing field (**append** parameter - use this when there is a trusted DHCP Snooping switch or another relay device between the clients and the DHCP Relay).
- Drop the packet (**drop** parameter).
- Replace the existing Option 82 information with its own (the default - **replace** parameter).

See the **ip dhcp-relay information policy** command for a command description and command examples.

### Checking Option 82 information in DHCP server responses

To configure the switch to check for Option 82 information in DHCP packets from servers, configure DHCP-relay agent-option checking with the Interface Configuration command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option checking
```

This command enables the DHCP relay agent to check Option 82 information in response packets returned from DHCP servers. If the information does not match the information it has configured for its own client (downstream) interface then the DHCP relay agent drops the packet.

## DHCP Relay client side IP source address

In most cases, there are filters placed between the DHCP relay and DHCP server which only allow DHCP packets from the client subnet to the server and back.

From software version 5.4.9-0.7 onwards, there is a command that allows you to configure the DHCP relay so that the relay will use the IP address of the interface receiving clients DHCP requests to be used as the source IP address of the relayed DHCP packets. This means that the relay will always use the client-side interface IP address as the source IP address of the DHCP relayed packets.

To configure the client side IP address as the source IP address of DHCP relayed packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-client-side-address
```

To show the status of the DHCP-Relay service, use the command:

```
awplus# show ip dhcp-relay
```

Notice that the second line of the display shows the status of the client-side address being used as the source IP address.

```
awplus#sh ip dhcp-relay

DHCP Relay Service is enabled
Use of client side address as source address is enabled

vlan10 is down, line protocol is down
Maximum hop count is 10
Maximum DHCP message length is 1400
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
Insertion of Subscriber-ID auto-MAC is disabled
The Remote Id string for Relay Agent Option is 0000.0000.0000
Relay Information policy is to replace existing relay agent information

List of servers :   10.1.1.1
```

## Configuring a DHCP short lease threshold

As mentioned in the section: "How does DHCP work" on page 4, lease times are configured to suit various requirements. A cafe with free wifi may have leases that last/expire in 1 hour, but an enterprise environment lease might expire in a number of days or even weeks.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few minutes before their existing lease expires. This can happen for example, when mobile devices move in and out of a Wi-Fi zone or when Wi-Fi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

DHCP leases need to be backed up in NVS so that when the DHCP server reboots or goes through a power cycle, it won't lose all the knowledge of these leases.

If there is no benefit in backing up DHCP requests into the NVS lease file (because the device will simply make another DHCP request if it needs to), you can use the **short-lease-threshold** command.

The **short-lease-threshold** command allows you to configure the threshold for a short lease, from 1 minute to 24 hours. Any lease **less** then the threshold is deemed to be a short lease and will NOT be backed up to NVS.

This is useful if you have limited backup file space, and you don't need to restore leases after a device reboot or power cycle.

For example, to set the short lease threshold for address pool P1 to 40 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P1
awplus(dhcp-config)# short-lease-threshold 0 40
```

To set the short lease threshold for address pool Office_wifi to 1 hour and 35 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Office_wifi
awplus(dhcp-config)# short-lease-threshold 1 35
```

To set the short lease threshold to the default of one minute, use the following commands:

```
awplus# configure terminal
awplus(config)# no short-lease-threshold
```

## Port based IP assignment

From version **5.5.2-0.1** onwards, you can use the following commands to configure DHCP port based IP address assignment.

By default DHCP port based IP assignment is disabled. When you configure DHCP port-based assignment consider the following rules:

- You can configure only one IP address assigned per port.
- You cannot clear preassigned addresses using the **clear ip dhcp binding** command.
- Dynamic IP address assignment excludes preassigned addresses automatically. These addresses cannot be used in host pools, but you can use multiple preassigned addresses per DHCP address pool.

The DHCP server port-based address allocation feature gives you the capability to ensure that the same IP address is always offered to a replacement device as it is being replaced. This IP address is always offered to the same connected port even as the client-identifier or client hardware address changes in the DHCP messages received on that port.

This feature is enabled by substituting a subscriber identifier (subscriber-id) for client identifier (client-id) in all DHCP server internal transactions. To allow port based address assignment, the subscriber-id of a client needs to be associated with the physical port attachment. Subscriber-id for a remote client is included in the relay-agent information option on DHCP client packets relayed via a relay-agent. For a locally attached client, its subscriber-id is internally generated based on and associated with a port interface directly attached to the DHCP clients.

The commands allow you to substitute a client-id with the subscriber-id associated to a client. This is either internally generated, by the ingress port receiving messages for a particular client, or an explicit subscriber-id obtained from a relay agent information option included in the messages from relayed client messages. You have the capability to add a subscriber-id sub-option to the relay agent information option it adds/replaces on client messages. Additionally, the DHCP server enables you to make an IP address reservation for a given client-id.

**Commands**

The **host** command:

To add a static host address reservation to the DHCP address pool you are configuring for the DHCP client with the given client identifier use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)# host <ip-address> client-id <identifier-id>
```

The **use-subscriber-id** command:

To configure the DHCP server to use subscriber identifier substitution for a client identifier on all DHCP packets for a given remote address, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)# use-subscriber-id
```

The **ip dhcp use-subscriber-id (conf)** command:

To configure the DHCP server to use subscriber identifier substitution on all DHCP packets coming from all switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp use-subscriber-id
```

The **ip dhcp use-subscriber-id (if)** command:

To configure the DHCP server to use subscriber identifier substitution for the client identifier on all DHCP packets coming from the DHCP client directly connected to an interface, use the commands:

```
awplus(config)# int port<port-name>
awplus(config-if)# ip dhcp use-subscriber-id
```

The **ip dhcp-relay agent-option subscriber-id** command:

To set an ASCII string as a subscriber identifier for a port used by the relay agent, use the commands:

```
awplus# configure terminal
awplus(config)# interface <port-number>
awplus(config-if)# ip dhcp-relay agent-option subscriber-id <subscriber-id>
```

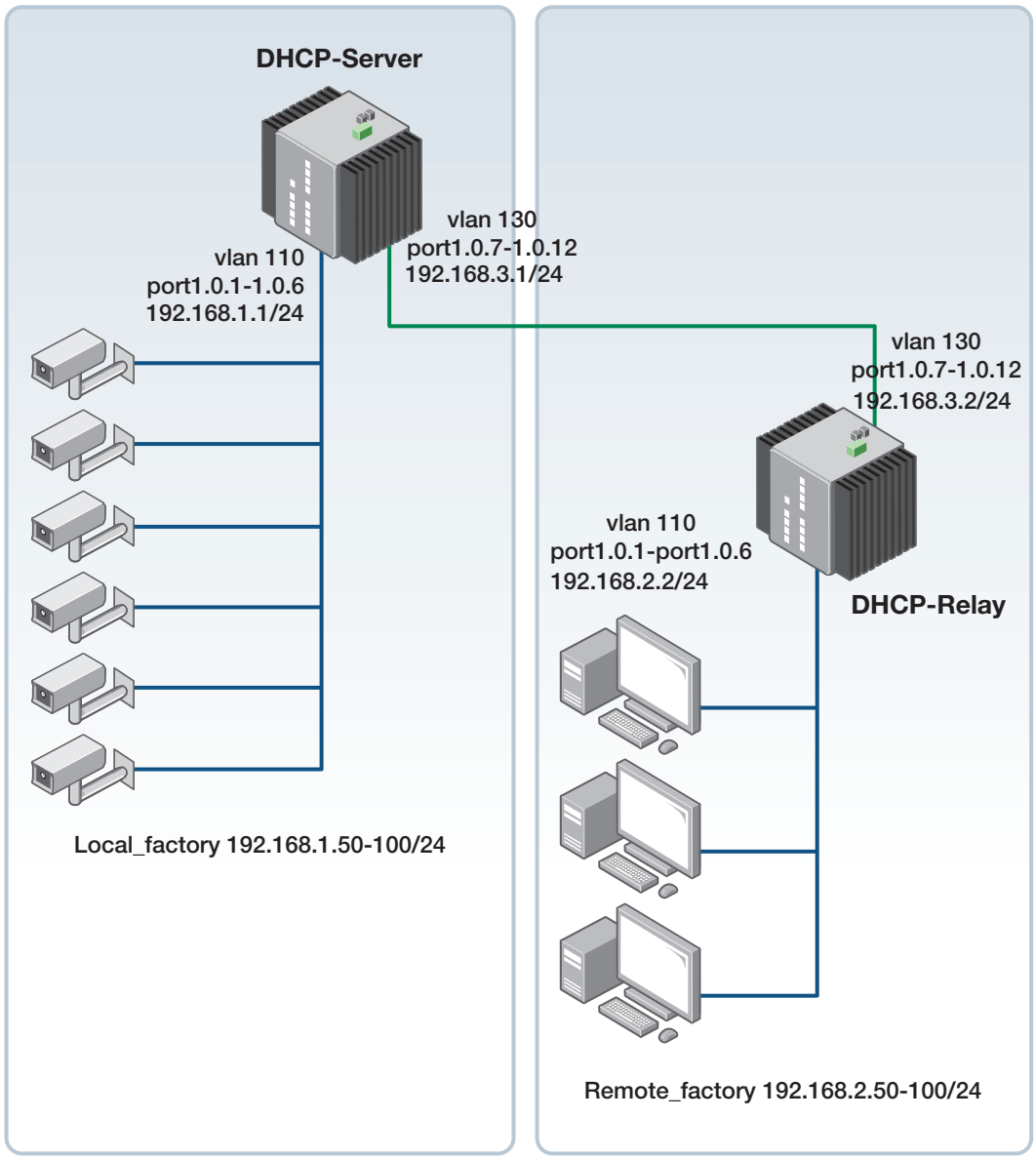
See the following configuration examples showing configuration of a DHCP server, DHCP relay server, and show commands to verify your configuration:


- "Configuration scenario example diagram" on page 25
- "Configuration example for the DHCP server" on page 26
- "Configuration example for the DHCP relay server" on page 27
- "Show commands to monitor your configuration" on page 28

## Configuration scenario example diagram

The following configuration example diagram shows DHCP port-based IP assignment for a DHCP server and a DHCP relay server. The DHCP server is located at a local factory and the DHCP relay server is located at a remote destination:

Figure 3: Configuration example for port-based IP assignment



### Configuration example for the DHCP server

This example shows how to configure the local DHCP server based on the example scenario diagram above:

```
!
hostname DHCP-Server
!
ip dhcp pool Local_factory
network 192.168.1.0 255.255.255.0
range 192.168.1.50 192.168.1.100
! port1.0.1-1.0.3 have static IP address reservations
host 192.168.1.75 client-id port1.0.1
host 192.168.1.76 client-id port1.0.2
host 192.168.1.77 client-id port1.0.3
! port1.0.4-1.0.6 will be allocated IP address automatically
dns-server 192.168.1.1
default-router 192.168.1.1
!
ip dhcp pool Remote_factory
! use subscriber-id for client-id substitution for this pool
use-subscriber-id
network 192.168.2.0 255.255.255.0
range 192.168.2.50 192.168.2.100
! static IP address reservations for remote_pc_1, 2 and 3
host 192.168.2.80 client-id remote_pc_1
host 192.168.2.81 client-id remote_pc_2
host 192.168.2.82 client-id remote_pc_3
! all other devices will be allocated IP address automatically
dns-server 192.168.1.1
default-router 192.168.2.2
!
service dhcp-server
!
vlan database
vlan 110,130 state enable
!
interface port1.0.1-1.0.6
! subscriber-id for client-id substitution
ip dhcp use-subscriber-id
switchport
switchport mode access
switchport access vlan 110
!
interface port1.0.7-1.0.12
switchport
switchport mode access
switchport access vlan 130
!
interface vlan110
ip address 192.168.1.1/24
!
interface vlan130
ip address 192.168.3.1/24
!
ip route 192.168.2.0/24 192.168.3.2
!
```

### Configuration example for the DHCP relay server

This example shows how to configure the remote DHCP relay server based on the example scenario diagram above:

```
!
hostname DHCP-Relay
!
no service dhcp-server
!
vlan database
vlan 120,130 state enable
!
interface port1.0.1
! device attached to port1.0.1 to be assigned with 192.168.2.80
ip dhcp-relay agent-option subscriber-id remote_pc_1
switchport
switchport mode access
switchport access vlan 120
!
interface port1.0.2
! device attached to port1.0.2 to be assigned with 192.168.2.81
ip dhcp-relay agent-option subscriber-id remote_pc_2
switchport
switchport mode access
switchport access vlan 120
!
interface port1.0.3
! device attached to port1.0.3 to be assigned with 192.168.2.82
ip dhcp-relay agent-option subscriber-id remote_pc_3
switchport
switchport mode access
switchport access vlan 120
!
interface port1.0.4-1.0.6
switchport
switchport mode access
switchport access vlan 120
!
interface port1.0.7-1.0.12
switchport
switchport mode access
switchport access vlan 130
!
interface vlan120
ip address 192.168.2.2/24
ip dhcp-relay agent-option
ip dhcp-relay information policy append
ip dhcp-relay server-address 192.168.3.1
!
interface vlan130
ip address 192.168.3.2/24
!
```

### Show commands to monitor your configuration

The following show commands are used to check and verify your configuration:

Use the command **show interface *<interface>*** to display the status and configuration of a specific interface, for example:

```
awplus#show interface port1.0.11
Interface port1.0.11
  Scope: both
  Link is DOWN, administrative state is UP
  Thrash-limiting
    Status Not Detected, Action learn-disable, Timeout 1(s)
  Hardware is Ethernet, address is e01a.ea60.087f
  index 5010 metric 1 mru 1500
  configured duplex auto, configured speed auto, configured polarity auto
<UP,BROADCAST,MULTICAST>
SNMP link-status traps: Disabled
 DHCP subscriber-id substitution for client-id is not enabled
  DHCP subscriber-id is office-1
   input packets 0, bytes 0, dropped 0, multicast packets 0
   output packets 0, bytes 0, multicast packets 0, broadcast packets 0
   input average rate : 30 seconds 0 bps, 5 minutes 0 bps
   output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 17:51:00
DHCP-server#
```

Use the command **show ip dhcp binding** to show the address bindings on the DHCP server.

```
DHCP-Server#show ip dhcp binding

rPool Local_factory Network 192.168.1.0/24
rDHCP Client Entries
rIP Address      ClientId                          Type    Expiry
-------------------------------------------------------------------------------
r192.168.1.75    port1.0.1                         Static  Infinite
r192.168.1.76    port1.0.2                         Static  Infinite
r192.168.1.77    port1.0.3                         Static  Infinite

rPool Remote_factory Network 192.168.2.0/24
rDHCP Client Entries
rIP Address      ClientId                          Type    Expiry
-------------------------------------------------------------------------------
r192.168.2.80    remote_pc_1                       Static  Infinite
r192.168.2.81    remote_pc_2                       Static  Infinite
r192.168.2.82    remote_pc_3                       Static  Infinite

DHCP-Server#
```

Use the command **show ip dhcp pool** to show the DHCP address pools:

```
DHCP-Server#show ip dhcp pool

Pool Local_factory :
  subscriber-id substition for client-id is not enabled
  network: 192.168.1.0/24
  address ranges:
    addr: 192.168.1.50 to 192.168.1.100
            (static host addr 192.168.1.75 excluded)
            (static host addr 192.168.1.76 excluded)
            (static host addr 192.168.1.77 excluded)
  static host addresses:
    addr: 192.168.1.75     Client-id: port1.0.1
    addr: 192.168.1.76     Client-id: port1.0.2
    addr: 192.168.1.77     Client-id: port1.0.3
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  dns servers:  192.168.1.1
  default-router(s):  192.168.1.1
  Probe:                        Default Values
    Status:       Enabled      [Enabled]
    Type:         Ping         [Ping]
    Packets:      5            [5]
    Timeout:      200 msecs    [200]
  Dynamic addresses:
    Total:        48
    Leased:       0
    Utilization:  0.0 %
  Static host addresses:
    Total:        3
    Leased:       3

Pool Remote_factory :
  subscriber-id substition for client-id is enabled
  network: 192.168.2.0/24
  address ranges:
    addr: 192.168.2.50 to 192.168.2.100
            (static host addr 192.168.2.80 excluded)
            (static host addr 192.168.2.81 excluded)
            (static host addr 192.168.2.82 excluded)
  static host addresses:
    addr: 192.168.2.80     Client-id: remote_pc_1
    addr: 192.168.2.81     Client-id: remote_pc_2
    addr: 192.168.2.82     Client-id: remote_pc_3
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  dns servers:  192.168.1.1
  default-router(s):  192.168.2.2
  Probe:                        Default Values
    Status:       Enabled      [Enabled]
    Type:         Ping         [Ping]
    Packets:      5            [5]
    Timeout:      200 msecs    [200]
  Dynamic addresses:
    Total:        48
    Leased:       0
    Utilization:  0.0 %
  Static host addresses:
    Total:        3
    Leased:       3
DHCP-Server#
```

Use the command **show ip dhcp server summary** to display information about the DHCP server:

```
DHCP-Server#show ip dhcp server summary
DHCP Server service is enabled
DHCP Server is running
BOOTP ignore is disabled
DHCP leasequery support is disabled
DHCP subscriber-id substitution for client-id is not enabled
Pool list: Local_factory Remote_factory
DHCP-Server#

DHCP-Server#show ip dhcp server summary
DHCP Server service is enabled
DHCP Server is running
BOOTP ignore is disabled
DHCP leasequery support is disabled
DHCP subscriber-id substitution for client-id is enabled
Pool list: Local_factory Remote_factory
DHCP-Server
```

Use the command **show running-config** to verify your configuration for the DHCP server:

```
DHCP-Server#show running-config
!
service password-encryption
!
hostname DHCP-Server
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
ip domain-lookup
!
ip dhcp pool Local_factory
 network 192.168.1.0 255.255.255.0
 range 192.168.1.50 192.168.1.100
 host 192.168.1.75 client-id port1.0.1
 host 192.168.1.76 client-id port1.0.2
 host 192.168.1.77 client-id port1.0.3
 dns-server 192.168.1.1
 default-router 192.168.1.1
!
```

**show running-config** (cont'd) for the DHCP server:

```
ip dhcp pool Remote_factory
 use-subscriber-id
 network 192.168.2.0 255.255.255.0
 range 192.168.2.50 192.168.2.100
 host 192.168.2.80 client-id remote_pc_1
 host 192.168.2.81 client-id remote_pc_2
 host 192.168.2.82 client-id remote_pc_3
 dns-server 192.168.1.1
 default-router 192.168.2.2
!
!
!
service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
no lacp global-passive-mode enable
!
switch 1 provision x950-28
switch 1 bay 1 provision xem2-12
!
vlan database
 vlan 110,130 state enable
!
interface port1.0.1-1.0.6
 ip dhcp use-subscriber-id
 switchport
 switchport mode access
 switchport access vlan 110
!
interface port1.0.7-1.0.12
 switchport
 switchport mode access
 switchport access vlan 130
!
interface port1.0.13-1.0.37
 switchport
 switchport mode access
!
interface port1.1.1-1.1.12
 switchport
 switchport mode access
!
interface vlan110
 ip address 192.168.1.1/24
!
interface vlan130
 ip address 192.168.3.1/24
!
ip route 192.168.2.0/24 192.168.3.2
!
line con 0
line vty 0 4
!
end
```

Use the **show running-config** to verify your configuration for the DHCP relay server:

```
DHCP-Relay#show running-config
!
service password-encryption
!
hostname DHCP-Relay
!
no banner motd
!
username manager privilege 15 password 8
$1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
ip domain-lookup
!
!
!
no service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
no lacp global-passive-mode enable
!
switch 1 provision x950-52
!
vlan database
 vlan 120,130 state enable
!
```

**show running-config** for the DHCP relay server (cont'd):

```
interface port1.0.1
 ip dhcp-relay agent-option subscriber-id remote_pc_1
 switchport
 switchport mode access
 switchport access vlan 120
!
interface port1.0.2
 ip dhcp-relay agent-option subscriber-id remote_pc_2
 switchport
 switchport mode access
 switchport access vlan 120
!
interface port1.0.3
 ip dhcp-relay agent-option subscriber-id remote_pc_3
 switchport
 switchport mode access
 switchport access vlan 120
!
interface port1.0.4-1.0.6
 switchport
 switchport mode access
 switchport access vlan 120
!
interface port1.0.7-1.0.12
 switchport
 switchport mode access
 switchport access vlan 130
!
interface port1.0.13-1.0.61
 switchport
 switchport mode access
!
interface vlan120
 ip address 192.168.2.2/24
 ip dhcp-relay agent-option
 ip dhcp-relay information policy append
 ip dhcp-relay server-address 192.168.3.1
!
interface vlan130
 ip address 192.168.3.2/24
!
line con 0
line vty 0 4
!
end
```



Allied Telesis NETWORK SMARTER

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com